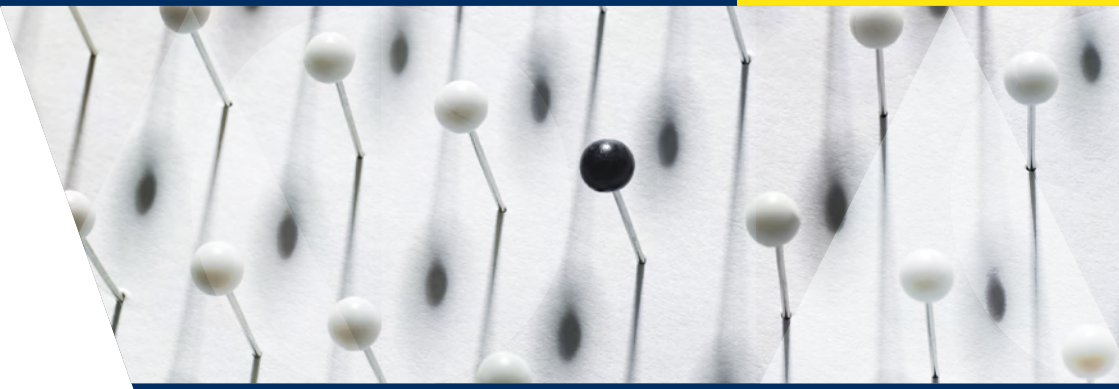
ROKASGRĀMATA



Rokasgrāmata par Eiropas tiesību aktiem datu aizsardzības jomā

2018. gada izdevums

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

Šīs rokasgrāmatas manuskripts pabeigts 2018. gada aprīlī.

Atjauninājumi nākotnē būs pieejami *FRA* tīmekļa vietnē fra.europa.eu, Eiropas Padomes tīmekļa vietnē coe.int/dataprotection, Eiropas Cilvēktiesību tiesas tīmekļa vietnē echr.coe.int *Case-Law* izvēlnē, kā arī Eiropas datu aizsardzības uzraudzītāja tīmekļa vietnē edps.europa.eu.

Fotoattēli (uz vāka un iekšlapās): © *iStockphoto*

Luksemburga: Eiropas Savienības Publikāciju birojs, 2022

Eiropas Padome:	ISBN 978-92-871-9828-0		
FRA – Print:	ISBN 978-92-9461-556-5	doi:10.2811/095074	TK-05-17-225-LV-C
FRA – PDF:	ISBN 978-92-9461-557-2	doi:10.2811/828873	TK-05-17-225-LV-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

Rokasgrāmata par Eiropas tiesību aktiem datu aizsardzības jomā

2018. gada izdevums

Priekšvārds

Mūsu sabiedrība kļūst arvien digitalizētāka. Ņemot vērā šīs izmaiņas, tehnoloģiju attīstības tempi un tas, kā tiek apstrādāti personas dati, katru dienu un visdažādākajos veidos ietekmē ikvienu no mums. Nesen tika pārskatīti Eiropas Savienības (ES) un Eiropas Padomes tiesiskie regulējumi, kas aizsargā privātumu un nodrošina personas datu aizsardzību.

Datu aizsardzības jomā Eiropai pasaulē ir vadošā funkcija. ES datu aizsardzības standarti ir balstīti uz Eiropas Padomes Konvenciju Nr. 108, ES instrumentiem, tostarp Vispārīgo datu aizsardzības regulu un Datu aizsardzības direktīvu policijas un krimināltiesību jomā, kā arī uz Eiropas Cilvēktiesību tiesas un Eiropas Savienības Tiesas attiecīgo judikatūru.

ES un Eiropas Padomes veiktās datu aizsardzības reformas ir visaptverošas un nereti sarežģītas, nodrošinot plašu ieguvumu klāstu un ietekmējot gan indivīdus, gan uzņēmumus. Šīs rokasgrāmatas mērķis ir celt informētības līmeni un uzlabot zināšanas par datu aizsardzības noteikumiem, jo īpaši to praktizējošo juristu vidū, kuri nav specializējušies šajā jomā un kuri savā darbā saskaras ar datu aizsardzības jautājumiem.

Rokasgrāmatu ir sagatavojusi ES Pamattiesību aģentūra (*FRA*) sadarbībā ar Eiropas Padomi (kopā ar Eiropas Cilvēktiesību tiesas kanceleju) un Eiropas Datu aizsardzības uzraudzītāju. Ar šo rokasgrāmatu tiek atjaunināts 2014. gada izdevums, un tā ir daļa no juridisko rokasgrāmatu sērijas, ko kopīgi sagatavojušas *FRA* un Eiropas Padome.

Mēs pateicamies Apvienotās Karalistes, Beļģijas, Francijas, Gruzijas, Igaunijas, Itālijas, Īrijas, Monako, Šveices un Ungārijas datu aizsardzības iestādēm par sniegtajām noderīgajām atsauksmēm attiecībā uz rokasgrāmatas projektu. Turklāt mēs izsakām pateicību Eiropas Komisijas Datu aizsardzības nodaļai un tās Starptautiskās datu plūsmas un aizsardzības nodaļai. Mēs pateicamies Eiropas Savienības Tiesai par šīs rokasgrāmatas sagatavošanas darbu laikā sniegto dokumentālo atbalstu. Visbeidzot, mēs vēlamies izteikt pateicību Datu valsts inspekcijai par atbalstu šīs rokasgrāmatas latviešu valodas versijas pārbaudē.

Christos Giakoumopoulos

Eiropas Padomes Cilvēktiesību un juridisko lietu ģenerāldirektorāta ģenerāldirektors

Giovanni Buttarelli

Eiropas Datu aizsardzības uzraudzītājs

Michael O'Flaherty

Eiropas Savienības Pamattiesību aģentūras direktors

Saturs

Saīsinājumi un akronīmi

ANO	Apvienoto Nāciju Organizācija
AUI	Apvienotā uzraudzības iestāde
BCR	Saistošs uzņēmuma noteikums
CCTV	Videonovērošanas sistēma
CETS	Eiropas Padomes līgumu sērija
CRM	Klientu attiecību pārvaldība
C-SIS	Centrālā Šengenas informācijas sistēma
DAI	Datu aizsardzības iestāde
DAS	Datu aizsardzības speciālists
EAO	Eiropas apcietināšanas orderis
EBTA	Eiropas Brīvās tirdzniecības asociācija
ECT	Eiropas Cilvēktiesību tiesa
ECTK	Eiropas Cilvēktiesību konvencija
EDAK	Eiropas Datu aizsardzības kolēģija
EDAU	Eiropas Datu aizsardzības uzraudzītājs
EEZ	Eiropas Ekonomikas zona
EFSA	Eiropas Pārtikas nekaitīguma iestāde
EK	Eiropas Kopiena
ENISA	Eiropas Tīklu un informācijas drošības aģentūra
ENU	Eiropola valsts vienība
EP	Eiropas Padome
EPPO	Eiropas Prokuratūra
ES	Eiropas Savienība
ESAO	Ekonomiskās sadarbības un attīstības organizācija
EST	Eiropas Savienības Tiesa (līdz 2009. gada decembrim Eiropas Kopienu Tiesa, EKT)
eTEN	Eiropas telekomunikāciju tīkli
eu-LISA	Lielapjoma IT sistēmu ES aģentūra
EuroPriSe	Eiropas privātuma zīmogs
EVTI	Eiropas Vērtspapīru un tirgu iestāde

FRA	Eiropas Savienības Pamattiesību aģentūra
GPS	Globālās pozicionēšanas sistēma
Harta	Eiropas Savienības Pamattiesību harta
ICCPR	Starptautiskais pakts par pilsoniskajām un politiskajām tiesībām
IKT	Informācijas un komunikācijas tehnoloģijas
IPS	Interneta pakalpojumu sniedzējs
Konvencija Nr. 108	Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (Eiropas Padome). Konvencijas Nr. 108 grozījumu protokolu (*CETS* Nr. 223) Eiropas Padomes Ministru komiteja pieņēma savā 128. sesijā, kas norisinājās Helsingērā, Dānijā (2018. gada 17.–18. maijā). Atsauces uz "modernizēto Konvenciju Nr. 108" attiecas uz konvenciju, kas grozīta ar protokolu *CETS* Nr. 223.
LES	Līgums par Eiropas Savienību
LESD	Līgums par Eiropas Savienības darbību
MIS	Muitas informācijas sistēma
N-SIS	Nacionālā Šengenas informācijas sistēma
NVO	Nevalstiska organizācija
OV	Oficiālais Vēstnesis
PDR	Pasažieru datu reģistrs
PIN	Personas identifikācijas numurs:
SCG	Uzraudzības koordinācijas grupa
SEPA	Vienotā euro maksājumu telpa
SIS	Šengenas informācijas sistēma
SWIFT	Vispasaules Starpbanku finanšu telekomunikāciju sabiedrība
VCD	Vispārējā cilvēktiesību deklarācija
VDAR	Vispārīgā datu aizsardzības regula
VIS	Vīzu informācijas sistēma

Kā lietot šo rokasgrāmatu

Šajā rokasgrāmatā ir sniegts pārskats par Eiropas Savienības (ES) un Eiropas Padomes (EP) noteiktajiem juridiskajiem standartiem datu aizsardzības jomā. Šī rokasgrāmata ir izstrādāta kā palīgmateriāls praktizējošiem juristiem, kuri nav specializējušies datu aizsardzības jomā. Tā ir domāta advokātiem, tiesnešiem vai citiem profesionāļiem, kā arī personām, kuras strādā citās struktūrās, piemēram, nevalstiskajās organizācijās (NVO), kam var nākties saskarties ar juridiskiem jautājumiem par datu aizsardzību.

Rokasgrāmata ir pirmais atskaites punkts gan par attiecīgiem ES tiesību aktiem, gan par Eiropas Cilvēktiesību konvenciju (ECTK), kā arī EP Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (Konvencija Nr. 108) un citiem EP instrumentiem.

Tabulā katras nodaļas sākumā ir norādīti juridiskie noteikumi, kas attiecas uz konkrētajā nodaļā aplūkotajām tēmām. Tabulas attiecas gan uz EP, gan ES tiesību aktiem, un tajās ir ietverta atlasīta Eiropas Cilvēktiesību tiesas (ECT) un Eiropas Savienības Tiesas (EST) judikatūra. Tālāk secīgi norādīti abu atšķirīgo Eiropas sistēmu attiecīgie tiesību akti, kas attiecas uz konkrētām aplūkotajām tēmām. Tas lasītājam ļauj salīdzināt abu tiesību sistēmu kopīgos un atšķirīgos elementus. Tam vajadzētu arī palīdzēt lasītājiem atrast būtisko informāciju attiecībā uz viņu situāciju, jo īpaši, ja uz viņiem attiecas tikai EP tiesību akti. Dažās nodaļās, lai īsi un kodolīgi atspoguļotu saturu, tēmu secība tabulās var nedaudz atšķirties no secības pašā nodaļā. Rokasgrāmatā sniegts arī īss Apvienoto Nāciju Organizācijas regulējuma pārskats.

Praktiķi no valstīm, kas nav ES dalībvalstis, bet ir EP un līdz ar to ECTK un Konvencijas Nr. 108 dalībvalstis, var piekļūt par savu valsti būtiskajai informācijai tieši iedaļās par EP. Praktiķiem no valstīm, kas nav ES dalībvalstis, ir arī jāpatur prātā, ka kopš ES Vispārīgās datu aizsardzības regulas pieņemšanas ES datu aizsardzības noteikumi attiecas uz organizācijām un citām iestādēm, kas nav reģistrētas ES, ja tās apstrādā personas datus un piedāvā preces un pakalpojumus datu subjektiem Savienībā vai pārrauga šādu datu subjektu uzvedību.

Praktiķiem ES dalībvalstīs būs jāizmanto abas iedaļas, jo šīm valstīm ir saistošas abas tiesību sistēmas. Jāatzīmē, ka Eiropā notiekošās datu aizsardzības noteikumu reformas un modernizācija, kas uzsāktas gan Eiropas Padomes (modernizētās Konvencijas Nr. 108, kas grozīta ar protokolu *CETS* Nr. 223), gan ES (Vispārīgās datu aizsardzības regulas un Direktīvas (ES) 2016/680 pieņemšanas) ietvaros, tika īstenotas

paralēli. Abu tiesību sistēmu regulatori ir darījuši visu iespējamo, lai nodrošinātu abu tiesisko regulējumu konsekvenci un savietojamību. Tādējādi reformas ir sniegušas augstāku saskaņotības pakāpi starp EP un ES tiesību aktiem datu aizsardzības jomā. Tiem, kuriem nepieciešama plašāka informācija par kādu konkrētu jautājumu, iedaļā "Papildliteratūra" ir sniegts saraksts ar specializētākiem materiāliem. Informācijai par Konvencijas Nr. 108 un tās 2001. gada Papildu protokola noteikumiem, kas joprojām tiek piemēroti līdz grozījumu protokola stāšanās spēkā brīdim, lasītājiem ir jāizmanto rokasgrāmatas 2014. gada izdevums.

EP tiesību akti ir norādīti, izmantojot īsas atsauces uz atlasītajām ECT lietām. Tās izvēlētas no lielā ECT spriedumu un lēmumu skaita par datu aizsardzības jautājumiem.

Attiecīgie ES tiesību akti ietver pieņemtos likumdošanas pasākumus, attiecīgos līgumu noteikumus un Eiropas Savienības Pamattiesību hartu, kā interpretēts EST judikatūrā. Turklāt šajā rokasgrāmatā ir sniegti atzinumi un vadlīnijas, ko pieņēmusi 29. panta darba grupa – padomdevēja struktūra, kurai saskaņā ar Datu aizsardzības direktīvu ir uzticēts sniegt ekspertu ieteikumus ES dalībvalstīm un kuru no 2018. gada 25. maija aizstās Eiropas Datu aizsardzības kolēģija (EDAK). Eiropas Datu aizsardzības uzraudzītāja atzinumi sniedz arī svarīgu ieskatu ES tiesību aktu interpretācijā, tāpēc tie iekļauti šajā rokasgrāmatā.

Šajā rokasgrāmatā aprakstītās vai citētās lietas sniedz svarīgus gan ECT, gan EST judikatūras piemērus. Rokasgrāmatas beigās sniegto norāžu mērķis ir palīdzēt lasītājiem atrast judikatūru tiešsaistē. Sniegtā EST judikatūra attiecas uz iepriekšējo Datu aizsardzības direktīvu. Tomēr EST sniegtās interpretācijas joprojām ir piemērojamas attiecīgajām tiesībām un pienākumiem, kas noteikti Vispārīgajā datu aizsardzības regulā.

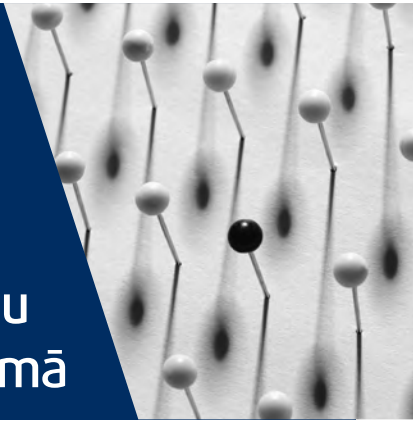
Turklāt tekstlodziņos ar zilu fonu ir iekļauti praktiski piemēri ar hipotētiskiem scenārijiem. Tajos ir plašāk atspoguļota Eiropas datu aizsardzības noteikumu piemērošanas prakse, jo īpaši gadījumos, ja nepastāv konkrēti atbilstoša ECT vai EST judikatūra. Citos tekstlodziņos ar pelēku fonu ir sniegti piemēri no avotiem, kas nav ECT un EST judikatūra, piemēram, tiesību akti un atzinumi, ko izdevusi 29. panta darba grupa.

Rokasgrāmatas ievadā sniegts īss abu tiesību sistēmu nozīmes apraksts, kā noteikts ECTK un ES tiesību aktos (1. nodaļa). Šādi jautājumi ir aplūkoti 2.–10. nodaļā:

- datu aizsardzības terminoloģija;
- Eiropas datu aizsardzības tiesību aktu galvenie principi;
- Eiropas datu aizsardzības tiesību aktu noteikumi;
- neatkarīga uzraudzība;
- datu subjektu tiesības un to īstenošana;
- personas datu pārrobežu nosūtīšana un plūsma;
- datu aizsardzība saistībā ar policiju un krimināltiesībām;
- citi Eiropas datu aizsardzības noteikumi konkrētās jomās;
- mūsdienu problēmas personas datu aizsardzības jomā.

1

Konteksts un vēsturiskā informācija Eiropas tiesību aktu datu aizsardzības jomā



ES	Aptvertie jautājumi	EP
Tiesības uz datu aizsardzību		
Līgums par Eiropas Savienības darbību, 16. pants Eiropas Savienības Pamattiesību harta (Harta), 8. pants (tiesības uz personas datu aizsardzību) Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (Datu aizsardzības direktīva), OV 1995 L 281 (spēkā līdz 2018. gada maijam) Padomes Pamatlēmums 2008/977/TI par tādu personas datu aizsardzību, ko apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās, OV 2008 L 350 (spēkā līdz 2018. gada maijam) Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula), OV 2016 L 119 Direktīva (ES) 2016/680 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināls odus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (Datu aizsardzība policijas un tiesu iestādēm), OV 2016 L 119		ECTK, 8. pants (tiesības uz privātās un ģimenes dzīves, dzīvokļa un korespondences neaizskaramību) Modernizētā Konvencija par personu aizsardzību attiecībā uz personas datu automātisku apstrādi (modernizētā Konvencija Nr. 108)

ES	Aptvertie jautājumi	EP
Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (Direktīva par privāto dzīvi un elektronisko komunikāciju), OV 2002 L 201 Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti (ES iestāžu datu aizsardzības regula), OV 2001 L 8.		
Tiesību uz personas datu aizsardzību ierobežojumi		
Harta, 52. panta 1. punkts Vispārīgā datu aizsardzības regula, 23. pants EST apvienotās lietas C-92/09 un C-93/09 *Volker und Markus Schecke GbR un Hartmut Eifert pret Land Hessen* [GC], 2010		ECTK, 8. panta 2. punkts. Modernizētā Konvencija Nr. 108, 11. pants ECT lieta *S. un Marper pret Apvienoto Karalisti* [GC], Nr. 30562/04 un Nr. 30566/04, 2008
Tiesību līdzsvarošana		
EST apvienotās lietas C-92/09 un C-93/09 *Volker und Markus Schecke GbR un Hartmut Eifert pret Land Hessen* [GC], 2010	**Vispārīgi**	
EST lieta C-73/07 *Tietosuojavaltuutettu pret Satakunnan Markkinapörssi Oy un Satamedia Oy* [GC], 2008 EST lieta C-131/12 *Google Spain SL, Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	**Vārda brīvība**	ECT lieta *Axel Springer AG pret Vāciju* [GC], Nr. 39954/08, 2012 ECT lieta *Mosley pret Apvienoto Karalisti*, Nr. 48009/08, 2011 ECT lieta *Bohlen pret Vāciju*, Nr. 53495/09, 2015
EST lieta C-28/08 P *Eiropas Komisija pret The Bavarian Lager Co. Ltd* [GC], 2010 EST lieta C-615/13P *ClientEarth, PAN Europe pret EFSA*, 2015	**Piekļuve dokumentiem**	ECT lieta *Magyar Helsinki Bizottság pret Ungāriju* [GC], Nr. 18030/11, 2016
Vispārīgā datu aizsardzības regula, 90. pants	**Dienesta noslēpums**	ECT lieta *Pruteanu pret Rumāniju*, Nr. 30181/05, 2015
Vispārīgā datu aizsardzības regula, 91. pants	**Reliģijas vai ticības brīvība**	
	Humanitāro un eksakto zinātņu brīvība	ECT lieta *Vereinigung bildender Künstler pret Austriju*, Nr. 68345/01, 2007

ES	Aptvertie jautājumi	EP
EST lieta C-275/06 *Productores de Música de España (Promusicae) pret Telefónica de España SAU* [GC], 2008	Īpašuma aizsardzība	
EST lieta C-131/12 *Google Spain SL, Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 EST lieta C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce pret Salvatore Manni*, 2017	Ekonomiskās tiesības	

1.1. Tiesības uz personas datu aizsardzību

Svarīgākie aspekti

- Saskaņā ar ECTK 8. pantu personas tiesības uz aizsardzību attiecībā uz personas datu apstrādi ietilpst tiesībās uz privātās un ģimenes dzīves, dzīvokļa un korespondences neaizskaramību.
- EP Konvencija Nr. 108 ir pirmais un līdz šim vienīgais starptautiskais juridiski saistošais dokuments, kas attiecas uz datu aizsardzību. Konvencija tika modernizēta, noslēgumā pieņemot grozījumu protokolu *CETS* Nr. 223.
- ES tiesību aktos atzīts, ka datu aizsardzība ir atsevišķa pamattiesību joma. Tas ir apliecināts Līguma par ES darbību 16. pantā, kā arī ES Pamattiesību hartas 8. pantā.
- ES tiesiskajā regulējumā datu aizsardzība pirmo reizi reglamentēta 1995. gadā ar Datu aizsardzības direktīvu.
- Ņemot vērā straujo tehnoloģiju attīstību, ES 2016. gadā pieņēma jaunus tiesību aktus, lai pielāgotu datu aizsardzības noteikumus digitālajam laikmetam. Vispārīgā datu aizsardzības regula stājās spēkā 2018. gada maijā, atceļot Datu aizsardzības direktīvu.
- Reizē ar Vispārīgo datu aizsardzības regulu ES pieņēma tiesību aktus par personas datu apstrādi valsts iestādēs tiesībaizsardzības nolūkos. Direktīvā (ES) 2016/680 ir noteikti datu aizsardzības noteikumi un principi, ar ko reglamentē personas datu apstrādi, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu par tiem pie atbildības vai izpildītu krimināLsodus.

1.1.1. Tiesības uz privātās dzīves neaizskaramību un tiesības uz personas datu aizsardzību: īss ievads

Tiesības uz privātās dzīves neaizskaramību un tiesības uz personas datu aizsardzību ir atsevišķas tiesības, lai arī cieši saistītas. Tiesības uz privātumu, ko Eiropas tiesību aktos sauc par tiesībām uz privātās dzīves neaizskaramību, starptautiskajās cilvēktiesībās parādījās 1948. gadā pieņemtajā Vispārējā cilvēktiesību deklarācijā (VCD) kā vienas no aizsargātajām cilvēka pamattiesībām. Drīz pēc VCD pieņemšanas arī Eiropā tika apstiprinātas šīs tiesības – Eiropas Cilvēktiesību konvencijā (ECTK) – līgumā, kas ir juridiski saistošs tās līgumslēdzējām pusēm un kas tika izstrādāts 1950. gadā. ECTK paredz, ka ikvienam ir tiesības uz savas privātās un ģimenes dzīves, dzīvokļa un korespondences neaizskaramību. Publiskām iestādēm ir aizliegts ierobežot šīs tiesības, izņemot likumā paredzētos gadījumus, kad tiek aizstāvētas svarīgas un leģitīmas sabiedriskās intereses un ierobežojumi ir nepieciešami demokrātiskā sabiedrībā.

VCD un ECTK tika pieņemtas krietni pirms datoru un interneta attīstības un informācijas sabiedrības uzplaukuma. Šīs norises ir sniegušas ievērojamas priekšrocības indivīdiem un sabiedrībai, uzlabojot dzīves kvalitāti, efektivitāti un produktivitāti. Tajā pašā laikā tās rada jaunus riskus tiesībām uz privātās dzīves neaizskaramību. Atbildot uz nepieciešamību ieviest īpašus noteikumus, kas reglamentē personiskas informācijas vākšanu un izmantošanu, radies jauns privātuma jēdziens, kas dažās jurisdikcijās pazīstams kā "informācijas privātums", savukārt citās – "tiesības uz informācijas privātumu"[1]. Tāpēc tika izstrādāti īpaši tiesiskie regulējumi, kas nodrošina personas datu aizsardzību.

Datu aizsardzība Eiropā aizsākās pagājušā gadsimta septiņdesmitajos gados, kad dažās valstīs tika pieņemti tiesību akti, lai kontrolētu personiskās informācijas apstrādi publiskās iestādēs un lielos uzņēmumos[2]. Pēc tam Eiropā tika izveidoti datu

1 Vācijas Federatīvā Konstitucionālā tiesa tiesības uz informācijas privātumu apstiprināja 1983. gada spriedumā *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1ff. Tiesa uzskatīja, ka informācijas privātums izriet no Vācijas konstitūcijā aizsargātajām pamattiesībām uz cieņu pret personību. ECT 2017. gada spriedumā atzina, ka ECTK 8. pants "paredz tiesības uz sava veida informācijas privātumu". Skatīt ECT 2017. gada 27. jūnija spriedumu lietā *Satakunnan Markkinapörssi Oy un Satamedia Oy pret Somiju* [GC], Nr. 931/13, 137. punkts.

2 Vācijas Hesenes federālajā zemē 1970. gadā tika pieņemts pirmais datu aizsardzības likums, kas tika piemērots tikai šajā federālajā zemē. Zviedrijā 1973. gadā tika pieņemts pasaulē pirmais valsts datu aizsardzības likums. Līdz 20. gadsimta 80. gadu beigām vairākas Eiropas valstis (Apvienotā Karaliste, Francija, Nīderlande un Vācija) arī bija pieņēmušas tiesību aktus datu aizsardzības jomā.

aizsardzības instrumenti[3], un gadu gaitā datu aizsardzība kļuva par atsevišķu vērtību, kas nav daļa no tiesībām uz privātās dzīves neaizskaramību. ES tiesību sistēmā datu aizsardzība ir atzīta par pamattiesībām atsevišķi no pamattiesībām uz privātās dzīves neaizskaramību. Šis nodalījums rada jautājumu par šo divu tiesību savstarpējām saistībām un atšķirībām.

Tiesības uz privātās dzīves neaizskaramību un tiesības uz personas datu aizsardzību ir cieši saistītas. Abas tiecas aizsargāt līdzīgas vērtības, t. i., indivīdu autonomiju un cilvēka cieņu, nodrošinot personisko zonu, kurā tie var brīvi attīstīt savas personības, domāt un veidot savu viedokli. Tādējādi šīs tiesības ir būtisks priekšnoteikums citu pamatbrīvību, piemēram, vārda brīvības, mierīgas pulcēšanās un biedrošanās brīvības, kā arī reliģijas brīvības izmantošanai.

Atšķiras abu tiesību formulējums un tvērums. Vispārējs iejaukšanās aizliegums veido tiesības uz privātās dzīves neaizskaramību, ievērojot noteiktus sabiedrības interešu kritērijus, kas atsevišķos gadījumos var attaisnot iejaukšanos. Personas datu aizsardzību uzskata par mūsdienīgām un aktīvām tiesībām[4], ieviešot līdzsvara un atsvara sistēmu, lai aizsargātu personas viņu datu apstrādes laikā. Apstrādei jāatbilst būtiskām personas datu aizsardzības komponentēm, proti, jānodrošina neatkarīga uzraudzība un datu subjekta tiesību ievērošana[5].

ES Pamattiesību hartas (Hartas) 8. pantā ne tikai apliecinātas tiesības uz personas datu aizsardzību, bet arī izklāstītas pamatvērtības, kas saistītas ar šīm tiesībām. Tajā paredzēts, ka personas datu apstrādei jābūt godprātīgai, veiktai noteiktiem mērķiem, kā arī balstītai vai nu uz attiecīgās personas piekrišanu, vai likumā noteikto likumīgo pamatojumu. Personām jābūt tiesībām piekļūt saviem personas datiem un pieprasīt veikt tajos labojumus, un šo tiesību ievērošanu kontrolē neatkarīga iestāde.

Tiesības uz personas datu aizsardzību iestājas ikreiz, kad tiek veikta personas datu apstrāde. Tādējādi tās ir plašākas par tiesībām uz privātās dzīves neaizskaramību.

---

3 Eiropas Padomes Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (Konvencija Nr. 108) tika pieņemta 1981. gadā. ES pieņēma savu pirmo visaptverošo datu aizsardzības instrumentu 1995. gadā: Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti.

4 Ģenerāladvokāte *Sharpston* rakstīja, ka šajā lietā piesauktas divas atsevišķas tiesības: "klasiskās" tiesības uz privātuma aizsardzību un "modernākas" tiesības uz datu aizsardzību. Skatīt EST apvienotās lietas C-92/09 un C-93/02 *Volker un Markus Schecke GbR pret Land Hessen*, ģenerāladvokātes Sharpston secinājumi, 2010. gada 17. jūnijs, 71. punkts.

5 Hustinx, P., EDPS Speeches & Articles, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation* ("ES datu aizsardzības tiesību akti: Direktīvas 95/46/EK pārskatīšana un ierosinātā Vispārīgā datu aizsardzības regula"), 2013. gada jūlijs.

Jebkurai personas datu apstrādes darbībai piemēro attiecīgu aizsardzību. Datu aizsardzība attiecas uz visu veidu personas datiem un datu apstrādi neatkarīgi no attiecībām un ietekmes uz privātumu. Ar personas datu apstrādi var arī pārkāpt tiesības uz privāto dzīvi, kas tiks demonstrēts turpmākajos piemēros. Tomēr, lai datu aizsardzības noteikumi stātos spēkā, nav jāpierāda tiesību uz privāto dzīvi pārkāpums.

Tiesības uz privātumu attiecas uz situācijām, kad ir apdraudētas privātās intereses vai indivīda "privātā dzīve". Kā parādīts šajā rokasgrāmatā, judikatūrā "privātās dzīves" jēdziens ir plaši interpretēts, aptverot gan intīmas situācijas, gan slepenu vai konfidenciālu informāciju, informāciju, kas varētu kaitēt sabiedrības attieksmei pret indivīdu, kā arī pat indivīda profesionālās dzīves un sabiedrības izturēšanās aspektus. Tomēr novērtējums, vai bijusi iejaukšanās "privātajā dzīvē", ir atkarīgs no katras lietas konteksta un faktiem.

Turpretī jebkura darbība, kas saistīta ar personas datu apstrādi, varētu ietilpt datu aizsardzības noteikumu darbības jomā un radīt tiesības uz personas datu aizsardzību. Piemēram, ja darba devējs reģistrē informāciju par darbinieku vārdiem un atalgojumu, tad šādas informācijas reģistrēšanu nevar uzskatīt par iejaukšanos privātajā dzīvē. Taču var runāt par iejaukšanos, ja, piemēram, darba devējs nodod darbinieku personisko informāciju trešām personām. Darba devējiem jebkurā gadījumā ir jāievēro datu aizsardzības noteikumi, jo darbinieku informācijas reģistrēšana ir datu apstrāde.

Piemērs. Lietā *Digital Rights Ireland*[6] EST tika lūgta lemt par Direktīvas 2006/24/EK spēkā esamību, ņemot vērā pamattiesības uz personas datu aizsardzību un privātās dzīves neaizskaramību, kas nostiprinātas ES Pamattiesību hartā. Direktīva pieprasīja publiski pieejamu elektronisko komunikāciju pakalpojumu un publisko komunikāciju tīklu nodrošinātājiem saglabāt pilsoņu telekomunikāciju datus uz laikposmu līdz diviem gadiem, lai nodrošinātu šo datu pieejamību smagu noziegumu novēršanai, izmeklēšanai un kriminālvajāšanai. Pasākums attiecās tikai uz metadatiem, atrašanās vietas datiem un datiem, kas nepieciešami abonenta vai lietotāja identificēšanai. Tas neattiecās uz elektroniskās komunikāciju saturu.

6 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C-293/12 un C-594/12 *Digital Rights Ireland Ltd pret Minister for Communications, Marine and Natural Resources un citiem un Kärntner Landesregierung un citiem* [GC].

EST uzskatīja, ka ar direktīvu notiek iejaukšanās pamattiesībās uz personas datu aizsardzību, "jo tajā paredzēta personas datu apstrāde"[7]. Turklāt tā konstatēja, ka direktīva pārkāpj tiesības uz privātās dzīves neaizskaramību[8]. Skatot kopumā, saskaņā ar direktīvu saglabātie personas dati, kuriem var piekļūt kompetentās iestādes, varētu ļaut izdarīt "ļoti precīzus secinājumus par personu, kuru dati tikuši saglabāti, privāto dzīvi, tostarp ikdienas paradumiem, pastāvīgajām vai pagaidu dzīvesvietām, ikdienas vai citām gaitām, veiktajām darbībām, šo personu sociālajām attiecībām un aprindām, kurās tās mēdz uzturēties"[9]. Iejaukšanās abās tiesībās bija plaša un īpaši nopietna.

EST pasludināja Direktīvu 2006/24/EK par spēkā neesošu, uzskatot, ka, lai arī tai bija leģitīms mērķis, iejaukšanās tiesībās uz personas datu aizsardzību un privātās dzīves neaizskaramību ir nopietna un pārsniedz noteikti nepieciešamo.

1.1.2. Starptautiskais tiesiskais regulējums: Apvienoto Nāciju Organizācija

Apvienoto Nāciju Organizācija neatzīst personas datu aizsardzību kā pamattiesības, kaut gan starptautiskajā tiesību sistēmā tiesības uz privātumu jau sen noteiktas kā pamattiesības. VCD 12. pants par privātās un ģimenes dzīves neaizskaramību[10] pirmo reizi iezīmēja starptautisko instrumentu, kurā noteiktas indivīda tiesības uz privātās jomas aizsardzību pret citu personu, jo īpaši valsts, iejaukšanos. Lai arī VCD nav saistoša deklarācija, tai ir būtisks statuss kā starptautisko cilvēktiesību tiesību aktu pamata instrumentam, tā ir ietekmējusi citu cilvēktiesību instrumentu attīstību Eiropā. Starptautiskais pakts par pilsoniskajām un politiskajām tiesībām (*ICCPR*) stājās spēkā 1976. gadā. Tajā pausts, ka nedrīkst patvarīgi vai nelikumīgi iejaukties nevienas personas privātajā vai ģimenes dzīvē, apdraudēt mājas neaizskaramību, korespondences noslēpumu vai nelikumīgi uzbrukt personas godam un reputācijai. *ICCPR* ir starptautisks līgums, kas tā 169 dalībvalstīm uzliek pienākumu ievērot un nodrošināt personu pilsonisko tiesību, tostarp tiesību uz privātumu, īstenošanu.

7 Turpat, 36. punkts.

8 Turpat, 32.–35. punkts.

9 Turpat, 27. punkts.

10 Apvienoto Nāciju Organizācija (ANO), Vispārējā cilvēktiesību deklarācija (VCD), 1948. gada 10. decembris.

Kopš 2013. gada Apvienoto Nāciju Organizācija ir pieņēmusi divas rezolūcijas par privātuma jautājumiem ar nosaukumu "tiesības uz privāto dzīvi digitālajā laikmetā"[11], reaģējot uz jauno tehnoloģiju attīstību un dažās valstīs veiktiem atklājumiem par masveida novērošanu (Snoudena atklāsmes). Tajās stingri nosodīta masveida novērošana, uzsvērta šādas novērošanas iespējamā ietekme uz pamattiesībām uz privātumu un vārda brīvību, kā arī uz dinamiskas un demokrātiskas sabiedrības funkcionēšanu. Lai arī tās nav juridiski saistošas, tās izraisīja svarīgas starptautiskas, augsta līmeņa politiskas debates par privātumu, jaunajām tehnoloģijām un novērošanu. Tāpēc tika izveidots arī īpašā referenta amats jautājumos par privātumu digitālajā laikmetā, kurš pilnvarots veicināt un aizsargāt šīs tiesības. Referenta īpašie uzdevumi ietver informācijas vākšanu par valstu praksi un pieredzi saistībā ar privātumu un problēmām, ko rada jaunās tehnoloģijas, labākās prakses apmaiņu un popularizēšanu, kā arī iespējamo šķēršļu identificēšanu.

Lai gan iepriekšējās rezolūcijās galvenā uzmanība bija pievērsta masveida novērošanas negatīvajai ietekmei un valstu atbildībai ierobežot izlūkošanas iestāžu pilnvaras, jaunākās rezolūcijas atspoguļo būtisku attīstību debatēs par privātumu Apvienoto Nāciju Organizācijā[12]. Rezolūcijas, ko pieņēma 2016. un 2017. gadā, apstiprina nepieciešamību ierobežot izlūkošanas aģentūru pilnvaras un nosodīt masveida novērošanu. Tomēr tajās arī skaidri noteikts, ka "pieaugošās uzņēmumu iespējas vākt, apstrādāt un izmantot personas datus var apdraudēt tiesību uz privātumu īstenošanu digitālajā laikmetā". Tādējādi papildus valsts iestāžu atbildībai rezolūcijās ir norādīts uz privātā sektora atbildību ievērot cilvēktiesības: uzņēmumi aicināti informēt lietotājus par personas datu vākšanu, izmantošanu, apmaiņu un saglabāšanu un izveidot pārredzamu apstrādes politiku.

1.1.3. Eiropas Cilvēktiesību konvencija

Eiropas Padome tika izveidota pēc Otrā pasaules kara, lai apvienotu Eiropas valstis, veicinātu tiesiskumu, demokrātiju, cilvēktiesības un sociālo attīstību. Šim nolūkam 1950. gadā tika pieņemta ECTK, kas stājās spēkā 1953. gadā.

11 Skatīt ANO Ģenerālās asamblejas Rezolūciju par tiesībām uz privāto dzīvi digitālajā laikmetā, A/RES/68/167, Ņujorka, 2013. gada 18. decembris; un ANO Ģenerālās asamblejas Pārskatītu rezolūcijas projektu par tiesībām uz privāto dzīvi digitālajā laikmetā, A/C.3/69/L.26/Rev.1, Ņujorka, 2014. gada 19. novembris.

12 ANO Ģenerālās asamblejas Pārskatīts rezolūcijas projekts par tiesībām uz privāto dzīvi digitālajā laikmetā, A/C.3/71/L.39/Rev.1, Ņujorka, 2016. gada 16. novembris; ANO Cilvēktiesību padome, Tiesības uz privāto dzīvi digitālajā laikmetā, A/HRC/34/L.7/Rev.1, 2017. gada 22. marts.

Līgumslēdzējām pusēm ir starptautisks pienākums ievērot ECTK. Visas EP dalībvalstis tagad ir iestrādājušas ECTK vai ieviesušas to savos tiesību aktos, kas tām uzliek pienākumu rīkoties saskaņā ar konvencijas noteikumiem. Līgumslēdzējām pusēm, veicot jebkādas darbības vai īstenojot pilnvaras, jāievēro konvencijā noteiktās tiesības. Tas attiecas arī uz pasākumiem, kas veikti valsts drošības labā. Eiropas Cilvēktiesību tiesas (ECT) nozīmīgākie spriedumi ir bijuši saistīti ar valsts darbībām sensitīvajās valsts drošības tiesību un prakses jomās[13]. Tiesa nav vilcinājusies apstiprināt, ka novērošanas darbības ir iejaukšanās privātās dzīves neaizskaramībā[14].

Lai nodrošinātu, ka līgumslēdzējas puses ievēro savus ECTK paredzētos pienākumus, Strasbūrā, Francijā, 1959. gadā tika izveidota ECT. ECT nodrošina, ka valstis ievēro savus konvencijā paredzētos pienākumus, izskatot personu, personu grupu, NVO vai juridisko personu sūdzības par konvencijas pārkāpumiem. ECT var izskatīt arī starpvalstu lietas, ko viena vai vairākas EP dalībvalstis ierosina pret citu dalībvalsti.

Kopš 2018. gada Eiropas Padomes sastāvā ir 47 līgumslēdzējas puses, no kurām 28 ir arī ES dalībvalstis. Lietas iesniedzējam ECT nav jābūt kādas līgumslēdzējas puses pilsonim, taču iespējamajiem pārkāpumiem jānotiek vienas no līgumslēdzējām pusēm jurisdikcijā.

Tiesības uz personas datu aizsardzību ir daļa no tiesībām, ko aizsargā ECTK 8. pants, kas garantē tiesības uz privātās un ģimenes dzīves, dzīvokļa un korespondences neaizskaramību, un paredz nosacījumus, saskaņā ar kuriem ir pieļaujami šo tiesību ierobežojumi[15].

ECT ir izskatījusi daudzus ar datu aizsardzību saistītus jautājumus. Tie skar sakaru pārtveršanu[16], dažādus novērošanas veidus gan privātajā, gan publiskajā sektorā[17] un aizsardzību pret personas datu glabāšanu publiskās iestādēs[18]. Privātās dzīves

13 Skatīt, piemēram: ECT 1978. gada 6. septembra spriedumu lietā *Klass un citi pret Vāciju*, Nr. 5029/71; ECT 2000. gada 4. maija spriedumu lietā *Rotaru pret Rumāniju* [GC], Nr. 28341/95; un ECT 2016. gada 12. janvāra spriedumu lietā *Szabó un Vissy pret Ungāriju*, Nr. 37138/14.

14 Turpat.

15 Eiropas Padomes Cilvēktiesību konvencija, *CETS* Nr. 005, 1950.

16 Skatīt, piemēram: ECT 1984. gada 2. augusta spriedumu lietā *Malone pret Apvienoto Karalisti*, Nr. 8691/79; ECT 2007. gada 3. aprīļa spriedumu lietā *Copland pret Apvienoto Karalisti*, Nr. 62617/00; vai ECT 2017. gada 18. jūlija spriedumu lietā *Mustafa Sezgin Tanrıkulu pret Turciju*, Nr. 27473/06.

17 Skatīt, piemēram: ECT 1978. gada 6. septembra spriedumu lietā *Klass un citi pret Vāciju*, Nr. 5029/71; ECT 2010 .gada 2. septembra spriedumu lietā *Uzun pret Vāciju*, Nr. 35623/05.

18 Skatīt, piemēram: ECT 2015. gada 4. decembra spriedumu lietā *Roman Zakharov pret Krieviju* [GC], Nr. 47143/06; ECT 2016. gada 12. janvāra spriedumu lietā *Szabó un Vissy pret Ungāriju*, Nr. 37138/14.

neaizskaramība nav absolūtas tiesības, jo tiesību uz privātumu izmantošana varētu apdraudēt citas tiesības, piemēram, vārda brīvību un piekļuvi informācijai, un otrādi. Tādēļ Tiesa cenšas rast līdzsvaru starp dažādām attiecīgajām tiesībām. Tā ir precizējusi, ka ECTK 8. pants ne tikai uzliek valstīm pienākumu atturēties no jebkādām darbībām, kas varētu pārkāpt šīs konvencijas tiesības, bet arī noteiktos apstākļos tām ir pozitīvs pienākums aktīvi nodrošināt efektīvu privātās un ģimenes dzīves neaizskaramību[19]. Attiecīgajās nodaļās šīs lietas ir izvērsti aprakstītas.

1.1.4. Eiropas Padomes Konvencija Nr. 108

Kopš informācijas tehnoloģiju parādīšanās pagājušā gadsimta sešdesmitajos gados arvien pieaug nepieciešamība pēc detalizētākiem noteikumiem, lai pasargātu personas, aizsargājot viņu personas datus. Līdz 20. gadsimta 70. gadu vidum Eiropas Padomes Ministru komiteja pieņēma dažādas rezolūcijas par personas datu aizsardzību, atsaucoties uz ECTK 8. pantu[20]. Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (Konvencija Nr. 108)[21] tika atvērta parakstīšanai 1981. gadā. Konvencija Nr. 108 bija un joprojām ir vienīgais juridiski saistošs starptautiskais dokuments datu aizsardzības jomā.

Konvencija Nr. 108 attiecas uz visu datu apstrādi, ko veic gan privātais, gan publiskais sektors, tostarp datu apstrādi, ko veic tiesas un tiesībaizsardzības iestādes. Tā aizsargā personas pret ļaunprātīgu izmantošanu saistībā ar personas datu apstrādi un tajā pašā laikā tiecas regulēt personas datu pārrobežu plūsmas. Attiecībā uz personas datu apstrādi konvencijā noteiktie principi jo īpaši attiecas uz godprātīgu un likumīgu datu vākšanu un automātisku apstrādi noteiktiem likumīgiem mērķiem. Tas nozīmē, ka datus nedrīkst izmantot mērķiem, kas nav saderīgi ar šiem mērķiem, un dati jāglabā ne ilgāk, kā tas ir nepieciešams. Tie attiecas arī uz datu kvalitāti, jo īpaši nosacījumu, ka tiem jābūt adekvātiem, būtiskiem un ne pārmērīgiem (proporcionalitāte), kā arī precīziem.

Papildus garantiju sniegšanai par personas datu apstrādi un datu drošības saistībām Konvencija Nr. 108 aizliedz apstrādāt "sensitīvus" datus, piemēram, par personas

19 Skatīt, piemēram: ECT 2008. gada 17. jūlija spriedumu lietā *I pret Somiju*, Nr. 20511/03; ECT 2008. gada 2. decembra spriedumu lietā *K.U. pret Somiju*, Nr. 2872/02.

20 Eiropas Padomes Ministru komiteja (1973), 1973. gada 26. septembra Rezolūcija (73) 22 par personu privātuma aizsardzību *vis-à-vis* elektroniskām datu bankām privātajā sektorā; Eiropas Padomes Ministru komiteja (1974), 1974. gada 20. septembra Rezolūcija (74) 29 par personu privātuma aizsardzību *vis-à-vis* elektroniskām datu bankām publiskajā sektorā.

21 Eiropas Padomes Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi, *CETS* Nr. 108, 1981.

rasi, politiskajiem uzskatiem, veselības stāvokli, reliģisko pārliecību, seksuālo dzīvi vai sodāmību, ja nav pienācīgu tiesisko garantiju.

Konvencijā ir iekļautas arī personas tiesības zināt, ka par viņu tiek glabāta informācija, un vajadzības gadījumā panākt tās labošanu. Konvencijā minēto tiesību ierobežojumi ir iespējami tikai tad, ja ir apdraudētas pārākas intereses, piemēram, valsts drošība vai aizsardzība. Turklāt konvencijā paredzēta brīva personas datu aprite starp līgumslēdzējām pusēm un paredzēti daži ierobežojumi plūsmai uz valstīm, kurās tiesiskais regulējums nenodrošina līdzvērtīgu aizsardzību.

Jāatzīmē, ka Konvencija Nr. 108 ir saistoša valstīm, kuras to ir ratificējušas. Uz to neattiecas ECT tiesiskā uzraudzība, bet to ņem vērā ECT judikatūrā ECTK 8. panta kontekstā. Gadu gaitā Tiesa ir lēmusi, ka personas datu aizsardzība ir būtiska tiesību uz privātās dzīves neaizskaramību sastāvdaļa (8. pants), un, nosakot, vai ir noticis šo pamattiesību aizskārums, tā ir vadījusies no Konvencijas Nr. 108 principiem[22].

Lai turpinātu pilnveidot Konvencijā Nr. 108 noteiktos vispārīgos principus un noteikumus, EP Ministru komiteja ir pieņēmusi vairākus juridiski nesaistošus ieteikumus. Šie ieteikumi ir ietekmējuši datu aizsardzības tiesību aktu attīstību Eiropā. Piemēram, gadiem ilgi vienīgais instruments Eiropā, kurā sniegtas norādes par personas datu izmantošanu policijas darbā, bija Policijas ieteikums[23]. Ieteikumā ietvertie principi, piemēram, datu failu glabāšanas līdzekļi un nepieciešamība ieviest skaidrus noteikumus attiecībā uz personām, kurām atļauts piekļūt šiem failiem, tika detalizētāk izstrādāti un atspoguļoti turpmākajos ES tiesību aktos[24]. Nesenāku ieteikumu mērķis ir risināt digitālā laikmeta problēmas, piemēram, saistībā ar datu apstrādi nodarbinātības kontekstā (skatīt 9. nodaļu).

Visas ES dalībvalstis ir ratificējušas Konvenciju Nr. 108. Konvencijas Nr. 108 grozījumi, saskaņā ar kuriem ES varētu kļūt par konvencijas dalībnieci, tika ierosināti 1999. gadā, taču tie nestājās spēkā[25]. Konvencijas Nr. 108 Papildu protokols tika pieņemts 2001. gadā. Tajā tika ieviesti noteikumi par pārrobežu datu plūsmām uz

22 Skatīt, piemēram: ECT 1997. gada 25. februāra spriedumu lietā *Z pret Somiju*, Nr. 22009/93.

23 Eiropas Padomes Ministru komiteja (1987), Ieteikums Rec(87)15 dalībvalstīm, kas regulē personas datu izmantošanu policijas darbā, Strasbūra, 1987. gada 17. septembris.

24 Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti, OV L 281, 1995. gada 23. novembris

25 Eiropas Padome, Konvencijas par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (ETS Nr. 108) grozījumi, ko 1999 gada 15. jūnijā Strasbūrā pieņēma Ministru komiteja.

valstīm, kas nav dalībvalstis, tā saucamajām trešām valstīm, un par obligātu valsts datu aizsardzības uzraudzības iestāžu izveidošanu[26].

Konvencijai Nr. 108 var pievienoties valstis, kas nav EP līgumslēdzējas puses. Konvencijas kā universālā standarta potenciāls apvienojumā ar tās atvērto raksturu kalpo par pamatu datu aizsardzības veicināšanai globālā mērogā. Līdz šim Konvencijai Nr. 108 ir pievienojusies 51 valsts. Tās ir visas Eiropas Padomes dalībvalstis (47 valstis); Urugvaja, pirmā valsts ārpus Eiropas, kas pievienojās 2013. gada augustā; kā arī Maurīcija, Senegāla un Tunisija, kas pievienojās 2016. un 2017. gadā.

Konvencija nesen tika modernizēta. Sabiedriskā apspriešana, ko īstenoja 2011. gadā, apstiprināja divus galvenos šā darba mērķus: stiprināt privātās dzīves aizsardzību digitālajā vidē un nostiprināt konvencijas uzraudzības mehānismu. Modernizācijas procesā galvenā uzmanība tika pievērsta šiem mērķiem, un darbs tika pabeigts, pieņemot Konvencijas Nr. 108 grozījumu protokolu (protokolu *CETS* Nr. 223). Darbs notika paralēli citām starptautisko datu aizsardzības instrumentu reformām, kā arī paralēli ES datu aizsardzības noteikumu reformai, kas tika uzsākta 2012. gadā. Regulatori Eiropas Padomes un ES mērogā ir darījuši visu iespējamo, lai nodrošinātu abu tiesisko regulējumu konsekvenci un savietojamību. Modernizācijas gaitā tika saglabāts konvencijas vispārīgais un elastīgais raksturs un nostiprināts tās kā universālā instrumenta potenciāls tiesību aktos datu aizsardzības jomā. Šeit atkārtoti apstiprināti un nostabilizēti svarīgi principi, kā arī nodrošinātas jaunas tiesības indivīdiem, vienlaikus palielinot to personu atbildību, kuras apstrādā personas datus, un nodrošinot lielāku pārskatatbildību. Piemēram, personām, kuru personas dati tiek apstrādāti, ir tiesības iegūt informāciju par šādas datu apstrādes pamatojumu un tiesības iebilst pret šo apstrādi. Lai cīnītos pret arvien pieaugošo profilēšanas izmantošanu tiešsaistes jomā, konvencijā arī noteiktas personas tiesības nebūt tādu lēmumu subjektam, kuru pamatā ir vienīgi automatizēta apstrāde, neņemot vērā personas uzskatus. Konvencijas praktiskā īstenošanā svarīga nozīme ir līgumslēdzēju pušu neatkarīgu uzraudzības iestāžu efektīvai datu aizsardzības noteikumu izpildes panākšanai. Šajā nolūkā modernizētajā konvencijā ir uzsvērta nepieciešamība uzraudzības iestādēm piešķirt efektīvas pilnvaras un funkcijas un, pildot savu misiju, tām jābūt patiesi neatkarīgām.

26 Eiropas Padome, Konvencijas par personu aizsardzību attiecībā uz personu datu automātisko apstrādi Papildu protokols par uzraudzības institūcijām un pārrobežu datu plūsmām, *CETS* Nr. 181, 2001. Pēc Konvencijas Nr. 108 modernizācijas šo protokolu vairs nepiemēro, jo tā noteikumi ir atjaunināti un integrēti modernizētajā Konvencijā Nr. 108.

1.1.5. Eiropas Savienības tiesību akti datu aizsardzības jomā

Primārie un sekundārie ES tiesību akti veido ES tiesības. Līgumus, proti Līgumu par Eiropas Savienību (LES) un Līgumu par Eiropas Savienības darbību (LESD), ir ratificējušas visas ES dalībvalstis. Tie veido "primāros ES tiesību aktus". ES iestādes, kurām saskaņā ar līgumiem piešķirta šāda vara, ir pieņēmušas ES regulas, direktīvas un lēmumus. Tie veido "sekundāros ES tiesību aktus".

Datu aizsardzība primārajos ES tiesību aktos

Sākotnējos Eiropas Kopienu līgumos nebija atsauces uz cilvēktiesībām vai to aizsardzību, ņemot vērā, ka Eiropas Ekonomikas kopiena sākotnēji bija paredzēta kā reģionāla organizācija ar uzsvaru uz ekonomisko integrāciju un kopējā tirgus izveidi. Eiropas Kopienas izveides un attīstības pamatā esošais pamatprincips, kas ir spēkā arī šodien, ir pilnvaru piešķiršanas princips. Saskaņā ar šo principu ES darbojas tikai to kompetenču robežās, ko dalībvalstis tai piešķir, kā tas atspoguļots ES līgumos. Pretstatā Eiropas Padomei ES līgumos nav skaidri noteikta kompetence pamattiesību jautājumos.

Tā kā EST ir izskatījusi lietas par cilvēktiesību pārkāpumiem jomās, uz kurām attiecas ES tiesību akti, EST tomēr ir sniegusi svarīgu līgumu interpretāciju. Piešķirot indivīdiem aizsardzību, Tiesa ieviesa pamattiesības tā sauktajos vispārējos Eiropas tiesību principos. Saskaņā ar EST šie vispārējie principi atspoguļo cilvēktiesību aizsardzības saturu, kas atrodams valstu konstitūcijās un cilvēktiesību līgumos, jo īpaši ECTK. EST norādīja, ka, izmantojot šos principus, tā nodrošinās ES tiesību aktu ievērošanu.

Atzīstot, ka tās politika varētu ietekmēt cilvēktiesības, un tiecoties panākt, lai pilsoņi justos "tuvāk" ES, 2000. gadā ES pasludināja Eiropas Savienības Pamattiesību hartu (Hartu). Tajā ir ietvertas visas Eiropas pilsoņu civilās, politiskās, ekonomiskās un sociālās tiesības, apkopojot dalībvalstu kopīgās konstitucionālās tradīcijas un starptautiskās saistības. Hartā aprakstītās tiesības ir sadalītas sešās iedaļās: cieņa, brīvības, vienlīdzība, solidaritāte, pilsoņu tiesības un tiesiskums.

Sākotnēji Harta bija tīri politisks dokuments, kas kļuva juridiski saistošs[27] kā Savienības primārās tiesības (skatīt LES 6. panta 1. punktu), Lisabonas līgumam stājoties

27 ES (2012), Eiropas Savienības Pamattiesību harta, OV 2012 C 326.

spēkā 2009. gada 1. decembrī[28]. Hartas noteikumi ir paredzēti ES iestādēm un struktūrām, uzliekot tām saistības ievērot tajā uzskaitītās tiesības savu pienākumu izpildes gaitā. Hartas noteikumi ir arī saistoši dalībvalstīm, īstenojot ES tiesības.

Hartā ir ne tikai garantētas tiesības uz privātās un ģimenes dzīves ievērošanu (7. pants), bet arī noteiktas tiesības uz personas datu aizsardzību (8. pants). Harta nepārprotami paaugstina šo aizsardzības līmeni ES tiesību aktos līdz pamattiesību līmenim. ES iestādēm un struktūrām, tāpat arī dalībvalstīm, īstenojot Savienības tiesību aktus (Hartas 51. pants), ir jāgarantē un jāievēro šīs tiesības. Hartas 8. pants, kas formulēts vairākus gadus pēc Datu aizsardzības direktīvas, ir jāsaprot tā, ka tajā ietverti iepriekš spēkā esoši ES tiesību akti datu aizsardzības jomā. Tādēļ Hartā ne tikai skaidri minētas tiesības uz datu aizsardzību 8. panta 1. punktā, bet sniegta arī atsauce uz galvenajiem datu aizsardzības principiem 8. panta 2. punktā. Visbeidzot, Hartas 8. panta 3. punktā noteikta prasība neatkarīgai iestādei kontrolēt šo principu īstenošanu.

Lisabonas līguma pieņemšana ir atskaites punkts datu aizsardzības tiesību aktu attīstībā, ne tikai paaugstinot Hartas statusu līdz juridiski saistošam dokumentam primāro tiesību līmenī, bet arī nodrošinot tiesības uz personas datu aizsardzību. Šīs tiesības ir jo īpaši paredzētas LESD 16. pantā saskaņā ar līguma daļu, kas veltīta ES vispārējiem principiem. Jaunu juridisko pamatu rada arī 16. pants, piešķirot ES kompetenci pieņemt tiesību aktus datu aizsardzības jautājumos. Šis ir svarīgs notikums, jo ES datu aizsardzības noteikumi, jo īpaši Datu aizsardzības direktīva, sākotnēji balstījās uz iekšējā tirgus juridisko pamatu un nepieciešamību tuvināt valstu likumus, lai netiktu kavēta brīva datu aprite ES. LESD 16. pantā ir sniegts neatkarīgs juridiskais pamats mūsdienīgai, visaptverošai pieejai datu aizsardzībai, kas ietver visus ES kompetencē esošos jautājumus, tostarp policijas un tiesu iestāžu sadarbību krimināllietās. LESD 16. pants arī apliecina, ka atbilstībai datu aizsardzības noteikumiem, kas pieņemti saskaņā ar to, jāpiemēro neatkarīgu uzraudzības iestāžu kontrole. Līguma 16. pants kalpoja par juridisko pamatu, lai 2016. gadā pieņemtu visaptverošu datu aizsardzības noteikumu reformu, t. i., Vispārīgo datu aizsardzības regulu un Datu aizsardzības direktīvu policijas un krimināltiesību jomā (skatīt zemāk).

Vispārīgā datu aizsardzības regula

No 1995. gada līdz 2018. gada maijam ES galvenais tiesību instruments datu aizsardzības jomā bija Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu

28 Skatīt Eiropas Kopienas (2012) Līguma par Eiropas Savienību, OV 2012 C 326, un Eiropas Kopienas (2012) LESD, OV 2012 C 326, konsolidētas versijas.

datu brīvu apriti (Datu aizsardzības direktīva)[29]. Tā tika pieņemta 1995. gadā, kad vairākas dalībvalstis jau bija pieņēmušas valsts datu aizsardzības likumus[30], un radās nepieciešamība šos likumus harmonizēt, lai nodrošinātu augstu aizsardzības līmeni un brīvu personas datu plūsmu starp dažādām dalībvalstīm. Preču, kapitāla, pakalpojumu un cilvēku brīvai apritei iekšējā tirgū bija nepieciešama brīva datu plūsma, kuru varēja realizēt tikai tad, ja dalībvalstis varētu paļauties uz vienādi augstu datu aizsardzības līmeni.

Datu aizsardzības direktīva atspoguļoja datu aizsardzības principus, kas jau bija ietverti valstu likumos un Konvencijā Nr. 108, vienlaikus nereti tos paplašinot. Tā atsaucās uz iespēju, kas paredzēta Konvencijas Nr. 108 11. pantā, pievienot aizsardzības instrumentus. Proti, neatkarīgas uzraudzības ieviešana direktīvā kā instruments datu aizsardzības noteikumu ievērošanas uzlabošanai izrādījās nozīmīgs ieguldījums efektīvā Eiropas datu aizsardzības tiesību darbībā. Līdz ar to šis jautājums tika iekļauts EP tiesību aktos 2001. gadā ar Konvencijas Nr. 108 Papildu protokolu. Tas parāda abu instrumentu ciešo mijiedarbību un pozitīvu savstarpējo ietekmi gadu gaitā.

Ar Datu aizsardzības direktīvu ES tika izveidota detalizēta un visaptveroša datu aizsardzības sistēma. Tomēr saskaņā ar ES tiesību sistēmu direktīvas nav tieši piemērojamas, tās ir jātransponē dalībvalstu tiesību aktos. Neizbēgami dalībvalstīm, transponējot direktīvas noteikumus, ir rīcības brīvība. Lai arī direktīvas nolūks bija panākt pilnīgu harmonizāciju[31] (un pilnīgu aizsardzības līmeni), praksē tā dalībvalstīs tika transponēta atšķirīgi. Tāpēc visā ES tika izveidoti dažādi datu aizsardzības noteikumi, kuru definīcijas un noteikumi valstu tiesību aktos tika interpretēti atšķirīgi. Arī izpildes līmeņi un sankciju bardzība dažādās dalībvalstīs atšķīrās. Visbeidzot, kopš direktīvas izstrādes 1990. gadu vidū notikušas ievērojamas pārmaiņas informācijas tehnoloģijās. Kopumā šie iemesli mudināja reformēt ES datu aizsardzības tiesību aktus.

Reformas rezultātā 2016. gada aprīlī pēc ilgstošām un intensīvām diskusijām tika pieņemta Vispārīgā datu aizsardzības regula. Debates par nepieciešamību modernizēt ES datu aizsardzības noteikumus sākās 2009. gadā, kad Komisija uzsāka

29 Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti, OV 1995 L 281.

30 Vācijas federālajā zemē Hesenē 1970. gadā tika pieņemts pasaulē pirmais datu aizsardzības likums, kas tika piemērots tikai šajā federālajā zemē. Zviedrija pieņēma *Datalagen* 1973. gadā, Vācija pieņēma *Bundesdatenschutzgestez* 1976. gadā, un Francija pieņēma *Loi relatif à l'informatique, aux fichiers et aux libertés* 1977. gadā. Apvienotajā Karalistē Datu aizsardzības likums tika pieņemts 1984. gadā. Visbeidzot 1989. gadā Nīderlande pieņēma *Wet Persoonregistraties*.

31 EST 2011. gada 24. novembra spriedums apvienotajās lietās C-468/10 un C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) un Federación de Comercio Electrónico y Marketing Directo (FECEMD) pret Administración del Estado*, 29. punkts.

sabiedrisko apspriešanu par turpmāko tiesisko regulējumu pamattiesībām uz personas datu aizsardzību. Regulas priekšlikumu Komisija publicēja 2012. gada janvārī, uzsākot garu likumdošanas procesu sarunās starp Eiropas Parlamentu un ES Padomi. Pēc pieņemšanas Vispārīgajā datu aizsardzības regulā bija paredzēts divu gadu pārejas periods. Tā kļuva pilnībā piemērojama 2018. gada 25. maijā, kad tika atcelta Datu aizsardzības direktīva.

Pieņemot Vispārīgo datu aizsardzības regulu 2016. gadā, tika modernizēti ES datu aizsardzības tiesību akti, padarot tos piemērotus pamattiesību aizsardzībai digitālā laikmeta ekonomisko un sociālo problēmu kontekstā. VDAR saglabāti un pilnveidoti pamatprincipi un datu subjekta tiesības, kas noteiktas Datu aizsardzības direktīvā. Turklāt tajā ir noteikti jauni pienākumi, pieprasot organizācijām ieviest integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma, noteiktos apstākļos iecelt datu aizsardzības speciālistu, ievērot jaunas tiesības uz datu pārnesamību, kā arī ievērot pārskatatbildības principu. Saskaņā ar ES tiesību aktiem noteikumi ir tieši piemērojami. Nav nepieciešama to ieviešana valstī. Tādējādi ar Vispārīgo datu aizsardzības regulu visā ES paredz vienotu datu aizsardzības noteikumu kopumu. Līdz ar to visā ES izveidoti konsekventi datu aizsardzības noteikumi, radot juridiskās noteiktības vidi, kurā ieguvēji ir gan uzņēmēji, gan privātpersonas kā "datu subjekti".

Tomēr, kaut arī Vispārīgā datu aizsardzības regula ir tieši piemērojama, no dalībvalstīm tiek sagaidīts, ka tās atjaunina savus spēkā esošos valsts tiesību aktus datu aizsardzības jomā, lai tos pilnībā saskaņotu ar šo regulu, vienlaikus atspoguļojot arī rīcības brīvību attiecībā uz īpašiem noteikumiem, kas ietverti 10. apsvērumā. Galvenie regulā ietvertie noteikumi un principi, kā arī spēcīgās tiesības, ko tā piešķir indivīdiem, sastāda būtisku šīs rokasgrāmatas daļu un ir aprakstīti turpmākajās nodaļās. Regulā ir visaptveroši noteikumi par teritoriālo darbības jomu. Tas attiecas uz ES reģistrētiem uzņēmumiem, kā arī uz pārziņiem un apstrādātājiem, kas nav reģistrēti ES, bet piedāvā preces vai pakalpojumus datu subjektiem ES vai uzrauga viņu uzvedību. Tā kā vairāki aizjūras tehnoloģiju uzņēmumi aizņem būtisku Eiropas tirgus daļu un tiem ir miljoniem ES klientu, ir svarīgi piemērot šīm organizācijām ES datu aizsardzības noteikumus, lai nodrošinātu personu aizsardzību, kā arī līdzvērtīgus konkurences apstākļus.

Datu aizsardzība tiesībaizsardzības jomā – Direktīva (ES) 2016/680

Atceltā Datu aizsardzības direktīva nodrošināja visaptverošu datu aizsardzības režīmu. Šis režīms tagad ir uzlabots, pieņemot Vispārīgo datu aizsardzības regulu. Lai arī atceltās Datu aizsardzības direktīvas piemērošanas joma bija visaptveroša, tā attiecās tikai uz darbībām iekšējā tirgū un uz tādu publisko iestāžu darbībām, kas

nav tiesībaizsardzības iestādes. Tāpēc bija nepieciešams pieņemt īpašus instrumentus, lai panāktu vajadzīgo skaidrību un līdzsvaru starp datu aizsardzību un citām likumīgajām interesēm un pievērstos problēmām, kas īpaši aktuālas konkrētās nozarēs. Tas attiecas uz noteikumiem, kas reglamentē personas datu apstrādi tiesībaizsardzības iestādēs.

Pirmais ES tiesību instruments šīs jomas regulēšanai bija Padomes Pamatlēmums 2008/977/TI par tādu personas datu aizsardzību, ko apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās. Tā noteikumi attiecās tikai uz policijas un tiesu datiem to apmaiņā starp dalībvalstīm. Personas datu apstrāde vietējā līmenī, ko veic tiesībaizsardzības iestādes, tika izslēgta no tā piemērošanas jomas.

Šī situācija tika novērsta, pieņemot Direktīvu (ES) 2016/680 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus, sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti[32], ko dēvē par Datu aizsardzības direktīvu policijas un krimināltiesību jomā. Ar direktīvu, kas pieņemta vienlaikus ar Vispārīgo datu aizsardzības regulu, tika atcelts Pamatlēmums 2008/977/TI un izveidota visaptveroša personas datu aizsardzības sistēma tiesībaizsardzības jomā, vienlaikus atzīstot arī ar sabiedrisko drošību saistītās datu apstrādes īpatnības. Vispārīgā datu aizsardzības regula paredz vispārīgus noteikumus, lai aizsargātu personas saistībā ar viņu personas datu apstrādi un nodrošinātu šādu datu brīvu apriti ES, direktīvā savukārt paredzēti īpaši datu aizsardzības noteikumi tiesu iestāžu sadarbības krimināllietās un policijas sadarbības jomā. Ja kompetentā iestāde apstrādā personas datus noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas vai krimināvajāšanas nolūkā, tiks piemērota Direktīva (ES) 2016/680. Ja kompetentās iestādes apstrādā personas datus citiem nolūkiem, nevis iepriekšminētajiem, tiks piemērots Vispārīgajā datu aizsardzības regulā noteiktais vispārīgais režīms. Atšķirībā no sava priekšgājēja (Padomes Pamatlēmuma 2008/977/TI) Direktīvas (ES) 2016/680 piemērošanas joma attiecas uz personas datu apstrādi iekšzemē, ko veic tiesībaizsardzības iestādes, un tā neattiecas tikai uz šādu datu apmaiņu starp dalībvalstīm. Turklāt direktīva tiecas panākt līdzsvaru starp indivīdu tiesībām un ar drošību saistītas apstrādes likumīgajiem mērķiem.

Šim nolūkam direktīvā ir apliecinātas tiesības uz personas datu aizsardzību un pamatprincipi, kas ir jāpiemēro datu apstrādei, stingri ievērojot noteikumus un

32 Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Direktīva (ES) 2016/680 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, OV L 119, 2016. gada 4. maijs.

principus, kādi ietverti Vispārīgajā datu aizsardzības regulā. Personu tiesības un pārziņiem uzliktie pienākumi, piemēram, attiecībā uz datu drošību, integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma, kā arī paziņojumu sniegšanu par datu aizsardzības pārkāpumiem, atgādina Vispārīgajā datu aizsardzības regulā noteiktās tiesības un pienākumus. Direktīvā ir ņemtas vērā un mēģināts risināt arī jauno tehnoloģiju radītās būtiskās problēmas, kas var īpaši smagi ietekmēt indivīdus, piemēram, profilēšanas metožu izmantošana tiesībaizsardzības iestādēs. Kopumā lēmumi, kuru pamatā ir vienīgi automatizēta apstrāde, tostarp profilēšana, ir jāaizliedz[33]. Turklāt tie nedrīkst būt balstīti sensitīvos datos. Šiem principiem piemēro dažus direktīvā paredzētos izņēmumus. Turklāt šāda apstrāde nedrīkst radīt personas diskrimināciju[34].

Direktīvā ir arī noteikumi pārziņu pārskatatbildības nodrošināšanai. Pārziņiem ir pienākums iecelt datu aizsardzības speciālistu, kurš uzrauga datu aizsardzības noteikumu ievērošanu, informē un konsultē organizāciju un darbiniekus, kas pilda apstrādes pienākumus, kā arī sadarbojas ar uzraudzības iestādi. Personas datu apstrādi policijas un krimināltiesību jomā šobrīd uzrauga neatkarīgas uzraudzības iestādes. Gan vispārīgajam datu aizsardzības tiesiskajam režīmam, gan īpašajam datu aizsardzības režīmam tiesībaizsardzības un kriminālllietu jomās ir vienādi jāatbilst ES Pamattiesību hartas prasībām.

Īpašais režīms datu apstrādei saistībā ar policijas un tiesu iestāžu sadarbību, kas izveidots, pieņemot Datu aizsardzības direktīvu policijas un krimināltiesību jomā, ir izvērsti aprakstīts 8. nodaļā.

Direktīva par privāto dzīvi un elektronisko komunikāciju

Tika uzskatīts, ka īpašu datu aizsardzības noteikumu ieviešana ir nepieciešama arī elektronisko komunikāciju nozarē. Attīstoties internetam, kā arī fiksētajai un mobilajai telefonijai, bija svarīgi nodrošināt, ka tiek ievērotas lietotāju tiesības uz privātumu un konfidencialitāti. Direktīvā 2002/58/EK[35] par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (Direktīvā par privāto dzīvi un elektronisko komunikāciju jeb E-privātuma direktīvā) ir izklāstīti noteikumi par

33 Datu aizsardzības direktīva policijas un krimināltiesību jomā, 11. panta 1. punkts.

34 Turpat, 11. panta 2. un 3. punkts.

35 Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē, OV L 201 (Direktīva par privāto dzīvi un elektronisko komunikāciju jeb E-privātuma direktīva).

personas datu drošību šajos tīklos, par paziņojumu sniegšanu personas datu aizsardzības pārkāpumu gadījumā un komunikācijas konfidencialitāti.

Saistībā ar drošību elektronisko komunikāciju pakalpojumu sniedzējiem cita starpā ir jānodrošina, ka piekļuve personas datiem ir tikai pilnvarotām personām, un jāveic pasākumi, lai novērstu personas datu iznīcināšanu, nozaudēšanu vai nejaušu sabojāšanu[36]. Ja pastāv īpašs sabiedriskā komunikāciju tīkla drošības pārkāpuma risks, operatoriem par šo risku jāinformē abonenti[37]. Ja, neraugoties uz ieviestajiem drošības pasākumiem, rodas drošības pārkāpums, operatoriem jāpaziņo par personas datu aizsardzības pārkāpumu kompetentajai valsts iestādei, kurai uzticēta šīs direktīvas ieviešana un izpilde. Operatoriem dažkārt tiek prasīts arī informēt par personas datu aizsardzības pārkāpumiem indivīdus, proti, ja pārkāpums var negatīvi ietekmēt viņu personas datus vai privātumu[38]. Komunikācijas konfidencialitātes nodrošināšanai sakaru un metadatu klausīšanai, noklausīšanai, glabāšanai vai jebkāda veida novērošanai vai pārtveršanai principā jābūt aizliegtai. Direktīva aizliedz arī nevēlamu komunikāciju (bieži to dēvē par "surogātpastu"), izņemot gadījumus, kad lietotāji ir snieguši savu piekrišanu, un tajā ir ietverti noteikumi par "sīkdatņu" glabāšanu datoros un ierīcēs. Šie galvenie negatīvie pienākumi skaidri norāda, ka komunikācijas konfidencialitāte ir cieši saistīta ar Hartas 7. pantā nostiprinātajām tiesībām uz privātās dzīves aizsardzību un Hartas 8. pantā nostiprinātajām tiesībām uz personas datu aizsardzību.

Komisija 2017. gada janvārī publicēja priekšlikumu regulai par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko komunikāciju nozarē, ar ko paredzēts aizstāt E-privātuma direktīvu. Reformas mērķis ir saskaņot elektronisko komunikāciju regulējošos noteikumus ar jauno datu aizsardzības režīmu, kas izveidots saskaņā ar Vispārīgo datu aizsardzības regulu. Jaunā regula būs tieši piemērojama visā ES. Visiem indivīdiem būs vienāds to elektronisko komunikāciju aizsardzības līmenis, savukārt telekomunikāciju operatori un uzņēmumi būs ieguvēji, pateicoties skaidrībai, juridiskajai noteiktībai un vienotam noteikumu kopumam visā ES. Ierosinātie noteikumi par elektronisko komunikāciju konfidencialitāti attieksies arī uz jauniem dalībniekiem, kas sniedz elektronisko komunikāciju pakalpojumus, uz kuriem neattiecas E-privātuma direktīva. Pēdējā attiecās tikai uz tradicionālo telekomunikāciju pakalpojumu sniedzējiem. Tā kā ziņojumu nosūtīšanai un zvanu veikšanai plaši tiek izmantoti tādi pakalpojumi kā *Skype*, *WhatsApp*, *Facebook Messenger*

36 Direktīva par privāto dzīvi un elektronisko komunikāciju, 4. panta 1. punkts.

37 Turpat, 4. panta 2. punkts.

38 Turpat, 4. panta 3. punkts.

un *Viber*, šie *over-the-top* pakalpojumi tagad ietilps regulas darbības jomā, tiem piemēros regulas prasības attiecībā uz datu aizsardzību, privātumu un drošību. Šīs rokasgrāmatas publicēšanas laikā likumdošanas process par E-privātuma noteikumiem nebija pabeigts.

Regula (EK) Nr. 45/2001

Tā kā Datu aizsardzības direktīvu varēja piemērot tikai ES dalībvalstīm, bija nepieciešams papildu tiesību instruments, lai izveidotu datu aizsardzību personas datu apstrādei ES iestādēs un struktūrās. Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās, kā arī par šādu datu brīvu apriti (ES iestāžu datu aizsardzības regula) pilda šo uzdevumu[39].

Regulā (EK) Nr. 45/2001 ir stingri ievēroti vispārējā ES datu aizsardzības režīma principi, un šie principi tiek piemēroti datu apstrādei, ko veic ES iestādes un struktūras, pildot savas funkcijas. Turklāt ar regulu izveido neatkarīgu uzraudzības iestādi, kas pārrauga tās noteikumu piemērošanu – Eiropas Datu aizsardzības uzraudzītāju (EDAU). EDAU ir piešķirtas uzraudzības pilnvaras un pienākums uzraudzīt personas datu apstrādi ES iestādēs un struktūrās, kā arī izskatīt un izmeklēt sūdzības par iespējamiem datu aizsardzības noteikumu pārkāpumiem. Uzraudzītājs arī sniedz konsultācijas ES iestādēm un struktūrām visos jautājumos saistībā ar personas datu aizsardzību, sākot no jaunu tiesību aktu priekšlikumiem un beidzot ar iekšējo noteikumu izstrādi attiecībā uz datu apstrādi.

Eiropas Komisija 2017. gada janvārī iesniedza priekšlikumu jaunai regulai par datu apstrādi ES iestādēs, ar ko tiks atcelta šobrīd spēkā esošā regula. Tāpat kā ar E-privātuma direktīvas reformu, arī Regulas (EK) Nr. 45/2001 reformas rezultātā tās noteikumi tiks modernizēti un saskaņoti ar jauno datu aizsardzības režīmu, kas izveidots atbilstoši Vispārīgajai datu aizsardzības regulai.

EST funkcija

EST ir kompetenta noteikt, vai kāda dalībvalsts ir izpildījusi savas saistības saskaņā ar ES tiesību aktiem datu aizsardzības jomā, kā arī interpretēt ES tiesību aktus, lai nodrošinātu to efektīvu un vienādu piemērošanu visās dalībvalstīs. Kopš Datu aizsardzības direktīvas pieņemšanas 1995. gadā ir uzkrāts apjomīgs judikatūras kopums, ar ko precizē datu aizsardzības principu un pamattiesību uz personas datu

39 Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti, OV 2001 L 8.

aizsardzību piemērojamību un nozīmi, kā noteikts Hartas 8. pantā. Kaut arī direktīva ir atcelta un tagad ir spēkā jauns tiesību instruments – Vispārīgā datu aizsardzības regula, šī iepriekš pastāvošā judikatūra joprojām ir būtiska un spēkā esoša ES datu aizsardzības principu interpretācijai un piemērošanai, ciktāl Datu aizsardzības direktīvas pamatprincipi un jēdzieni ir saglabāti VDAR.

1.2. Tiesību uz personas datu aizsardzību ierobežojumi

Svarīgākie aspekti

- Tiesības uz personas datu aizsardzību nav absolūtas tiesības. Tās var tikt ierobežotas, ja tas nepieciešams vispārēju interešu mērķim vai citu personu tiesību un brīvību aizsardzībai.
- Nosacījumi tiesību uz privātās dzīves neaizskaramību un personas datu aizsardzību ierobežošanai ir uzskaitīti ECTK 8. pantā un Hartas 52. panta 1. punktā. Tie izstrādāti un interpretēti, ņemot vērā ECT un EST judikatūru.
- Saskaņā ar EP tiesību aktiem datu aizsardzības jomā personas datu apstrāde ir likumīga iejaukšanās tiesībās uz privātās dzīves neaizskaramību, un to var veikt tikai tad, ja:
  - tā atbilst tiesību aktiem;
  - tai ir likumīgs mērķis;
  - tajā ievēro pamattiesību un brīvību būtību;
  - tā ir nepieciešama un samērīga demokrātiskā sabiedrībā, lai sasniegtu likumīgu mērķi.
- ES tiesību sistēmā ir Hartā aizsargāto pamattiesību izmantošanas ierobežojumiem līdzīgi nosacījumi. Jebkuru pamattiesību, tostarp personas datu aizsardzības, ierobežojums var būt likumīgs tikai tad, ja tas:
  - atbilst tiesību aktiem;
  - ievēro tiesību būtību;
  - ievērojot proporcionalitātes principu, ir nepieciešams; un
  - ir ES atzīts vispārēju interešu mērķis vai nepieciešamība aizsargāt citu tiesības.

Hartas 8. pantā noteiktās pamattiesības uz personas datu aizsardzību nav absolūtas, "bet tās ir jāievēro atkarībā no to uzdevuma sabiedrībā"[40]. Hartas 52. panta 1. punktā tiek atzīts, ka tādu tiesību, kādas ir paredzētas tās 7. un 8. pantā, izmantošanai var tikt noteikti ierobežojumi, ciktāl šie ierobežojumi ir noteikti tiesību aktos, tajos respektē šo tiesību un brīvību būtību un, ievērojot proporcionalitātes principu, tie ir nepieciešami un patiešām atbilst vispārējas nozīmes mērķiem, ko atzīst ES, vai vajadzībai aizsargāt citu personu tiesības un brīvības[41]. Tāpat ECTK sistēmā datu aizsardzība ir garantēta 8. pantā, un šo tiesību īstenošanu var ierobežot, ja tas nepieciešams likumīga mērķa sasniegšanai. Šī iedaļa attiecas uz tiesību aizskāruma nosacījumiem saskaņā ar ECTK, kā tie ir interpretēti ECT judikatūrā, kā arī uz nosacījumiem likumīgu ierobežojumu noteikšanai saskaņā ar Hartas 52. pantu.

1.2.1. Pamatota aizskāruma prasības saskaņā ar ECTK

Personas datu apstrāde var nozīmēt iejaukšanos datu subjekta tiesībās uz privātās dzīves neaizskaramību, ko aizsargā ECTK 8. pants[42]. Kā paskaidrots iepriekš (skatīt 1.1.1. un 1.1.4. iedaļu): pretēji ES tiesību sistēmai ECTK nav apstiprināta personas datu aizsardzība kā atsevišķas pamattiesības. Personas datu aizsardzība drīzāk ir daļa no tiesībām, ko aizsargā tiesības uz privātās dzīves neaizskaramību. Tādējādi neviena ar personas datu apstrādi saistīta darbība nevar ietilpt ECTK 8. panta darbības jomā. Lai sāktu darboties 8. pants, vispirms ir jānosaka, vai ir apdraudētas privātas intereses vai personas privātā dzīve. ECT savā judikatūrā ir traktējusi jēdzienu "privātā dzīve" jēdzienu kā plašu, tas aptver pat profesionālās dzīves un sabiedrības uzvedības aspektus. Tiesa arī lēmusi, ka personas datu aizsardzība ir svarīga tiesību uz privātās dzīves neaizskaramību sastāvdaļa. Tomēr, neraugoties uz plašo privātās dzīves jēdziena interpretāciju, ne visi apstrādes veidi paši par sevi veido 8. pantā aizsargāto tiesību apdraudējumu.

Ja ECT uzskata, ka aplūkotā apstrādes darbība skar personu tiesības uz privātās dzīves neaizskaramību, tā pārbauda, vai aizskārums ir pamatots. Tiesības uz privātās dzīves neaizskaramību nav absolūtas, bet tās ir jālīdzsvaro un jāsaskaņo ar citām likumīgām interesēm un tiesībām neatkarīgi no tā, vai tās ir citas personas (privātās intereses) vai sabiedrība kopumā (publiskās intereses).

40 Skatīt EST 2010. gada 9. novembra spriedumu apvienotajās lietās C-92/09 un C-93/09 *Volker und Markus Schecke GbR un Hartmut Eifert pret Land Hessen* [GC], 48. punkts.

41 Turpat, 50. punkts.

42 ECT 2008. gada 8. decembra spriedums lietā *S. un Marper pret Apvienoto Karalisti* [GC], Nr. 30562/04 un Nr. 30566/04, 67. punkts.

Kumulatīvie nosacījumi, kuros iejaukšanās var būt pamatota, ir šādi:

Saskaņā ar tiesību aktiem

Atbilstoši ECT judikatūrai aizskārums ir saskaņā ar tiesību aktiem, ja tā pamatā ir valsts tiesību aktu noteikums, kuram ir zināmas īpašības. Tiesību aktam jābūt "pieejamam attiecīgajām personām un paredzamam attiecībā uz tā sekām"[43]. Norma ir paredzama, "ja tā ir formulēta pietiekami precīzi, lai dotu iespēju ikvienai personai – attiecīgā gadījumā saņemot atbilstošu padomu – regulēt savu rīcību"[44]. Turklāt "attiecībā uz "tiesību aktu" prasītā precizitātes pakāpe šajā saistībā būs atkarīga no konkrētā temata"[45].

Piemēri. Lietā *Rotaru pret Rumāniju*[46] prasītājs apgalvoja, ka ir pārkāptas viņa tiesības uz privātās dzīves neaizskaramību, jo Rumānijas izlūkdienests turēja un izmantoja lietu, kurā bija viņa personīgā informācija. ECT konstatēja, ka, lai arī valsts tiesību akti ļāva vākt, reģistrēt un arhivēt slepenās datnēs informāciju, kas skar valsts drošību, tie nenoteica nekādus ierobežojumus šo pilnvaru izmantošanai, tas palika iestāžu ziņā. Piemēram, valsts tiesību aktos nebija definēts apstrādājamas informācijas veids, cilvēku kategorijas, attiecībā uz kurām var veikt uzraudzības pasākumus, apstākļi, kuros tādus pasākumus var veikt, vai procedūra, kas jāievēro. Šo trūkumu dēļ Tiesa secināja, ka valsts tiesību akti neatbilda paredzamības prasībai atbilstoši ECTK 8. pantam, tāpēc ir noticis minētā panta pārkāpums.

43 ECT 2000. gada 16. februāra spriedums lietā *Amann pret Šveici* [GC], Nr. 27798/95, 50. punkts; skatīt arī ECT 1998. gada 25. marta spriedumu lietā *Kopp pret Šveici*, Nr. 23224/94, 55. punkts, un ECT 2009. gada 10. februāra spriedumu lietā *Iordachi un citi pret Moldovu*, Nr. 25198/02, 50. punkts.

44 ECT 2000. gada 16. februāra spriedums lietā *Amann pret Šveici* [GC], Nr. 27798/95, 56. punkts; skatīt arī ECT 1984. gada 2. augusta spriedumu lietā *Malone pret Apvienoto Karalisti*, Nr. 8691/79, 66. punkts; ECT 1983. gada 25. marta spriedumu lietā *Silver un citi pret Apvienoto Karalisti*, Nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 88. punkts.

45 ECT 1979. gada 26. aprīļa spriedums lietā *The Sunday Times pret Apvienoto Karalisti*, Nr. 6538/74, 49. punkts; skatīt arī ECT 1983. gada 25. marta spriedums lietā *Silver un citi pret Apvienoto Karalisti*, Nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 88. punkts.

46 ECT 2000. gada 4. maija spriedums lietā *Rotaru pret Rumāniju* [GC], Nr. 28341/95, 57. punkts; skatīt arī ECT 2007. gada 28. jūnija spriedumu lietā *Association for European Integration and Human Rights un Ekimdzhiev pret Bulgāriju*, Nr. 62540/00; ECT 2011. gada 21. jūnija spriedumu lietā *Shimovolos pret Krieviju*, Nr. 30194/09; un ECT 2005. gada 31. maija spriedumu lietā *Vetter pret Franciju*, Nr. 59842/00.

Lietā *Taylor-Sabori pret Apvienoto Karalisti*[47] prasītājs bija kļuvis par policijas uzraudzības mērķi. Izmantojot "klonu" prasītāja peidžerim, policija spēja pārtvert viņam sūtītos ziņojumus. Prasītājs tika apcietināts, viņam tika uzrādīta apsūdzība par konspirāciju kontrolēto narkotiku piegādē. Daļa no apsūdzības pret viņu bija vienā laikā rakstītas peidžera ziņojumu piezīmes, ko policija bija transkribējusi. Tomēr prasītāja tiesas prāvas laikā Lielbritānijas tiesību aktos netika regulēta privātā telekomunikāciju sistēmā pārraidītas komunikācijas pārtveršana. Tātad viņa tiesību aizskārums nebija noticis "saskaņā ar tiesību aktiem". ECT secināja, ka tādējādi tika pārkāpts ECTK 8. pants.

Lieta *Vukota-Bojić pret Šveici*[48] skāra sociālās apdrošināšanas prasītājas slepenu novērošanu, ko viņas apdrošināšanas sabiedrības uzdevumā veica privāti izmeklētāji. ECT uzskatīja, ka, kaut arī sūdzībā izskatāmo uzraudzības pasākumu ir pasūtījusi privāta apdrošināšanas sabiedrība, valsts šai sabiedrībai bija piešķīrusi tiesības nodrošināt pabalstus, kas izriet no obligātās medicīniskās apdrošināšanas, kā arī iekasēt apdrošināšanas prēmijas. Valsts nevar atbrīvoties no atbildības, ko paredz konvencija, deleģējot savus pienākumus privātām struktūrām vai privātpersonām. Valsts tiesību aktiem bija jānodrošina pietiekamas garantijas pret ļaunprātīgu iejaukšanos ECTK 8. pantā noteiktajās tiesībās, lai tā būtu "saskaņā ar likumu". Konkrētajā gadījumā ECT secināja, ka ir ticis pārkāpts ECTK 8. pants, jo valsts tiesību aktos nav pietiekami skaidri definēts apdrošināšanas sabiedrībām, kuras apdrošināšanas strīdos darbojas kā publiskas iestādes, piešķirtās rīcības brīvības apmērs un veids attiecībā uz apdrošinātās personas slepenu novērošanu. Jo īpaši tajos nebija ietverti pietiekami aizsardzības pasākumi pret ļaunprātīgu izmantošanu.

Tiekšanās pēc likumīga mērķa sasniegšanas

Likumīgs mērķis var būt vai nu kāda no nosauktajām vispārējām interesēm, vai citu tiesību un brīvību aizsardzība. Likumīgi mērķi, kas varētu attaisnot iejaukšanos, saskaņā ar ECTK 8. panta 2. punktu ir valsts drošības, sabiedriskās kārtības vai valsts labklājības intereses, lai nepieļautu nekārtības vai noziegumus, lai aizsargātu veselību vai morāli vai lai aizstāvētu citu tiesības un brīvības.

47 ECT 2002. gada 22. oktobra spriedums lietā *Taylor-Sabori pret Apvienoto Karalisti*, Nr. 47114/99.

48 ECT 2016. gada 18. oktobra spriedums lietā *Vukota-Bojić pret Šveici*, Nr. 61838/10, 77. punkts.

Piemērs. Lietā *Peck pret Apvienoto Karalisti*[49] prasītājs uz ielas centās izdarīt pašnāvību, pārgriežot sev vēnas, nezinādams, ka viņu bija filmējusi *CCTV* kamera. Pēc tam, kad policija, kas vēroja *CCTV* kameras, viņu izglāba, *CCTV* kameras ierakstu tā tālāk nodeva plašsaziņas līdzekļiem, kuri to publicēja, neaizklājot prasītāja seju. ECT konstatēja, ka nebija būtisku vai pietiekamu iemeslu, kas attaisnotu iestādes veiktu ieraksta tiešu atklāšanu sabiedrībai, iepriekš nesaņemot prasītāja piekrišanu vai nenoslēpjot viņa identitāti. Tāpēc tiesa atzina, ka šajā lietā ir pārkāpts ECTK 8. pants.

Nepieciešamība demokrātiskā sabiedrībā

ECT ir apgalvojusi, ka "nepieciešamības jēdziens ietver nosacījumu, ka iejaukšanās atbilst akūtai sociālai vajadzībai un jo īpaši ir samērīga izvirzītajam likumīgajam mērķim"[50]. Novērtējot, vai pasākums ir nepieciešams steidzamu sociālo vajadzību apmierināšanai, ECT pārbauda tā atbilstību un piemērotību attiecībā uz sasniedzamo mērķi. Šajā nolūkā var ņemt vērā, vai ar iejaukšanos mēģināts risināt jautājumu, kurš nerisināts varētu nodarīt kaitējumu sabiedrībai, vai ir pierādījumi, ka iejaukšanās var mazināt šādu kaitējošu iedarbību, un kādi ir plašāki sabiedrības uzskati par apskatāmo jautājumu[51]. Piemēram, ja drošības dienesti vāc un glabā konkrētu indivīdu, kuriem ir saikne ar teroristu kustībām, personas datus, tā būtu iejaukšanās indivīdu tiesībās uz privātās dzīves neaizskaramību, kas tomēr kalpo nopietnai, neatliekamai sociālajai vajadzībai: valsts drošībai un cīņai pret terorismu. Lai izturētu nepieciešamības pārbaudi, aizskārumam jābūt arī samērīgam. ECT judikatūrā proporcionalitāte tiek aplūkota nepieciešamības jēdziena kontekstā. Proporcionalitāte prasa, lai iejaukšanās ECTK aizsargātajās tiesībās nepārsniegtu izvirzītā likumīgā mērķa sasniegšanai nepieciešamo. Svarīgi faktori, kas jāņem vērā, veicot proporcionalitātes pārbaudi, ir iejaukšanās tvērums, jo īpaši skarto personu skaits, un aizsardzības pasākumi vai brīdinājumi, kas ieviesti, lai ierobežotu tās tvērumu vai kaitējumu indivīdu tiesībām[52].

49 ECT 2003. gada 28. janvāra spriedums lietā *Peck pret Apvienoto Karalisti*, Nr. 44647/98, 85. punkts.

50 ECT 1987. gada 26. marta spriedums lietā *Leander pret Zviedriju*, Nr. 9248/81, 58. punkts.

51 29. panta datu aizsardzības darba grupa (29. panta darba grupa) (2014), *Atzinums par vajadzīguma un samērīguma jēdziena un datu aizsardzības piemērošanu tiesībaizsardzības nozarē*, WP 211, Brisele, 2014. gada 27. februāris, 7.–8. lpp.

52 Turpat, 9.–11. lpp.

Piemērs. Lietā *Khelili pret Šveici*[53] policijas pārbaudes laikā policija atklāja, ka prasītājai bija līdzi zvanāmās kartes ar uzrakstu: "Pievilcīga sieviete, gandrīz 40 gadu veca, gribētu satikt vīrieti, lai laiku pa laikam kopīgi iedzertu vai izietu sabiedrībā. Tālr. Nr. (..)". Prasītāja apgalvoja, ka pēc šā atklājuma policija reģistrēja viņu savos reģistros kā prostitūtu – šo nodarbi prasītāja konsekventi noliedza. Prasītāja pieprasīja, lai no policijas datora reģistriem tiktu dzēsts vārds "prostitūta". ECT principā atzina, ka personas datu saglabāšana, pamatojot ar to, ka šī persona vēl var izdarīt noziedzīgu nodarījumu, zināmos apstākļos var būt samērīga. Tomēr prasītājas gadījumā apgalvojums par nelikumīgu prostitūciju šķita pārāk netiešs un vispārīgs, to nepamatoja konkrēti fakti, jo prasītāja nekad nav bijusi notiesāta par nodarbošanos ar nelikumīgu prostitūciju, tāpēc nevarēja uzskatīt, ka tā atbilst "akūtai sociālai vajadzībai" ECTK 8. panta izpratnē. Uzskatot to par iestāžu uzdevumu pierādīt par prasītāju uzglabāto datu precizitāti un skatot prasītājas tiesību aizskāruma nopietnību, Tiesa nosprieda, ka vārda "prostitūta" gadiem ilgā saglabāšana policijas kartotēkās nav bijusi vajadzīga demokrātiskā sabiedrībā. Tāpēc tiesa atzina, ka šajā lietā ir pārkāpts ECTK 8. pants.

Piemērs. Lietā *S. un Marper pret Apvienoto Karalisti*[54] abi prasītāji tika apcietināti un apsūdzēti par noziedzīgiem nodarījumiem. Policija paņēma viņu pirkstu nospiedumus un DNS paraugus saskaņā ar Likumu par pierādījumiem policijas un kriminālllietu jomā. Prasītāji netika notiesāti par nodarījumiem: viens tika attaisnots tiesā, savukārt pret otro prasītāju kriminālprocess tika pārtraukts. Tomēr policija viņu pirkstu nospiedumus, DNS profilus un šūnu paraugus paturēja un glabāja datubāzē, un valstu tiesību aktos bija atļauts tos saglabāt bez piemērojama laika ierobežojuma. Lai gan Apvienotā Karaliste apgalvoja, ka saglabāšana palīdz identificēt likumpārkāpējus nākotnē un tādējādi kalpo noziedzības novēršanas un atklāšanas likumīgā mērķa sasniegšanai, ECT uzskatīja, ka iejaukšanās prasītāju tiesībās uz privātās dzīves neaizskaramību ir nepamatota. Tiesa atgādināja, ka datu aizsardzības pamatprincipi pieprasa, lai personas dati tiktu saglabāti proporcionāli to vākšanas mērķim un ka glabāšanas periodi ir jāierobežo. Tiesa atzina, ka datubāzes paplašināšana, iekļaujot tajā ne tikai notiesāto personu, bet arī visu aizdomās turamo personu, kuras nav notiesātas, DNS profilus, var sniegt

53 ECT 2011. gada 18. oktobra spriedums lietā *Khelili pret Šveici*, Nr. 16188/07.

54 ECT 2008. gada 4. decembra spriedums lietā *S. un Marper pret Apvienoto Karalisti* [GC], Nr. 30562/04 un Nr. 30566/04.

ieguldījumu noziegumu atklāšanā un novēršanā Apvienotajā Karalistē. Tomēr to "pārsteidza saglabāšanas pilnvaru visaptverošais un nediskriminējošais raksturs"[55].

Ņemot vērā ģenētisko un veselības datu apjomu šūnu paraugos, iejaukšanās prasītāju tiesībās uz privāto dzīvi bija īpaši aizskaroša. No apcietinātajām personām varēja ņemt pirkstu nospiedumus un paraugus, kas nenoteiktu laiku tika glabāti policijas datubāzē neatkarīgi no nodarījuma veida un smaguma pat par maznozīmīgiem nodarījumiem, kas nav sodāmi ar brīvības atņemšanu. Turklāt attaisnoto personu iespējas izņemt savus datus no datubāzes bija ierobežotas. Visbeidzot ECT īpašu uzmanību pievērsa faktam, ka prasītājs apcietināšanas brīdī bija 11 gadus vecs. Nepilngadīgas personas, kura nav notiesāta, datu saglabāšana var būt īpaši kaitīga, ņemot vērā šīs personas neaizsargātību un viņas attīstības un integrācijas nozīmi sabiedrībā[56]. Tiesa vienbalsīgi uzskatīja, ka saglabāšana veido nesamērīgu iejaukšanos privātajā dzīvē, ko nevar uzskatīt par nepieciešamu demokrātiskā sabiedrībā.

Piemērs. Lietā *Leander pret Zviedriju*[57] ECT sprieda, ka personu, kuras piesakās darbam svarīgos amatos valsts drošības sistēmā, slepena izvērsta pārbaude pati par sevi nav pretrunā vajadzības prasībai demokrātiskā sabiedrībā. Valsts tiesību aktos noteiktās īpašās garantijas, lai aizsargātu datu subjekta intereses, piemēram, Parlamenta un Tieslietu kanclera veiktas kontroles, lika ECT secināt, ka Zviedrijas personāla kontroles sistēma atbilst ECTK 8. panta 2. punkta prasībām. Ņemot vērā tai pieejamo plašo rīcības brīvību novērtējumā, atbildētājai valstij bija tiesības uzskatīt, ka prasītāja gadījumā valsts drošības intereses bija augstākas par atsevišķas personas interesēm. Tiesa atzina, ka šajā lietā nav pārkāpts ECTK 8. pants.

1.2.2. Likumīgu ierobežojumu nosacījumi saskaņā ar ES Pamattiesību hartu

Hartas struktūra un formulējums ir atšķirīgi no ECTK struktūras un formulējuma. Hartā netiek runāts par garantēto tiesību aizskārumiem, bet tā satur noteikumu par ierobežojumu(-iem) Hartā atzīto tiesību un brīvību īstenošanā.

55 Turpat, 119. punkts.

56 Turpat, 124. punkts.

57 ECT 1987. gada 26. marta spriedums lietā *Leander pret Zviedriju*, Nr. 9248/81, 59. un 67. punkts.

Atbilstoši 52. panta 1. punktam ierobežojumi Hartā atzīto tiesību un brīvību īstenošanā un attiecīgi tiesību uz personas datu aizsardzību īstenošanā ir pieļaujami tikai tad, ja tie:

- ir likumā paredzēti; un
- respektē tiesību uz datu aizsardzību būtību; un
- ir vajadzīgi, ievērojot proporcionalitātes principu[58]; un
- atbilst Savienībā atzītiem vispārējo interešu kritērijiem vai vajadzībai aizsargāt citu tiesības un brīvības.

Tā kā personas datu aizsardzība ES tiesību sistēmā ir atšķirīgas un atsevišķas pamattiesības, ko aizsargā Hartas 8. pants, jebkura personas datu apstrāde pati par sevi ir iejaukšanās šajās tiesībās. Nav nozīmes, vai attiecīgie personas dati attiecas uz indivīda privāto dzīvi, vai tie ir sensitīvi, vai datu subjektiem ir sagādātas jebkādas neērtības. Lai iejaukšanās būtu likumīga, tai jāatbilst visiem Hartas 52. panta 1. punktā uzskaitītajiem nosacījumiem.

Likumā paredzēti

Tiesību uz personas datu aizsardzību ierobežojumi ir jāparedz tiesību aktos. Šī prasība nozīmē, ka ierobežojumiem jābūt juridiskam pamatam, kas ir pietiekami pieejams un paredzams, ir formulēts pietiekami precīzi, lai indivīdi varētu saprast savus pienākumus un pielāgot savu rīcību. Juridiskajā pamatā ir arī skaidri jādefinē kompetento iestāžu pilnvaru tvērums un veids, kā aizsargāt personas pret patvaļīgu iejaukšanos. Šī interpretācija atgādina ECT judikatūrā[59] noteikto prasību par "likumīgu iejaukšanos", un ticis apgalvots, ka Hartā izmantoto vārdu "likumā paredzēts" nozīmei vajadzētu būt tādai pašai, kāda tiem piešķirta saistībā ar ECT[60]. ECT judikatūra un jo īpaši tās "tiesību kvalitātes" jēdziens, ko tā ir attīstījusi gadu gaitā, ir būtisks

58 Par pamattiesību uz personas datu aizsardzību ierobežojošu pasākumu vajadzības izvērtēšanu skatīt: EDAU (2017), *Necessity Toolkit*, Brisele, 2017. gada 11. aprīlis.

59 EDAU (2017), *Necessity Toolkit*, Brisele, 2017. gada 11. aprīlis, 4. lpp.; skatīt arī EST *Tiesas (virspalātas) atzinumu 1/15*, 2017. gada 26. jūlijs.

60 EST apvienotās lietas C-203/15 un C-698/15 *Tele2 Sverige AB pret Post- och telestyrelsen* un *Secretary of State for the Home Department pret Tom Watson, Peter Brice, Geoffrey Lewis*, ģenerāladvokāta Saugmandsgora Ēes (*Saugmandsgaard Øe*) secinājumi, sniegti 2016. gada 19. jūlijā, 140. punkts.

apsvērums, kas EST jāņem vērā, interpretējot Hartas 52. panta 1 punkta darbības jomu[61].

Respektē tiesību būtību

ES tiesību sistēmā visos Hartā aizsargāto pamattiesību ierobežojumos ir jārespektē šo tiesību būtība. Tas nozīmē, ka ierobežojumi, kas ir tik plaši un aizskaroši, ka tie laupa pamattiesībām to pamata saturu, nav attaisnojami. Ja tiesību būtība ir apdraudēta, ierobežojums jāuzskata par nelikumīgu un nav nepieciešams sīkāk novērtēt, vai tas kalpo vispārējas nozīmes mērķim un atbilst nepieciešamības un samērīguma kritērijiem.

Piemērs. Lieta *Schrems*[62] attiecās uz personu aizsardzību saistībā ar viņu personas datu nosūtīšanu trešām valstīm – šajā gadījumā Amerikas Savienotajām Valstīm. Austrijas pilsonis *Schrems*, kurš bija *Facebook* lietotājs vairākus gadus, iesniedza sūdzību Īrijas datu aizsardzības uzraudzības iestādē par viņa personas datu nosūtīšanu no *Facebook* Īrijas meitasuzņēmuma uz *Facebook Inc.* un serveriem, kas atrodas ASV, kur dati tika apstrādāti. Prasītājs apgalvoja, ka, ņemot vērā amerikāņu trauksmes cēlēja Edvarda Snoudena 2013. gada atklājumus par ASV novērošanas dienestu novērošanas darbībām, ASV tiesību akti un prakse nepiedāvāja uz ASV teritoriju nosūtītajiem personas datiem pietiekamu aizsardzību. Snoudens bija atklājis, ka Nacionālās drošības aģentūra tieši piekļūst uzņēmumu serveriem, piemēram, *Facebook*, un var lasīt tērzēšanas un privātu ziņojumu saturu.

Datu nosūtīšana uz ASV tika balstīta uz 2000. gadā pieņemto Komisijas lēmumu par pienācīgu aizsardzību, kas ļauj nosūtīt datus ASV uzņēmumiem, kuri pašsertifikācijas sistēmas ietvaros ir apliecinājuši, ka aizsargā no ES nosūtītos personas datus un ievēro tā dēvētos "drošības zonas principus". Kad lieta tika nodota EST, tā pārbaudīja Komisijas lēmuma spēkā esamību Hartas kontekstā. Tiesa atgādināja, ka saskaņā ar pamattiesību aizsardzības noteikumiem ES atkāpes un šo tiesību ierobežojumi jāīsteno tikai tiktāl, ciktāl tas ir noteikti nepieciešams. EST uzskatīja, ka tiesību akti, kas atļauj publiskām iestādēm vispārīgi piekļūt elektronisko komunikāciju saturam, "apdraud

61 EST lieta C-70/10 *Scarlet Extended SA pret Société belge des auteurs compositeurs et éditeurs (SABAM)*, ģenerāladvokāta Krusa Viljalona (*Cruz Villalón*) secinājumi, sniegti 2011. gada 14. aprīlī, 100. punkts.

62 EST 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems pret Datu aizsardzības komisāru* [GC].

pašu Hartas 7. pantā garantēto pamattiesību uz privātās dzīves neaizskaramību būtību". Tiesības zaudētu nozīmi, ja ASV publisko iestāžu piekļuvei komunikācijai būtu gadījuma raksturs un tai nebūtu objektīva pamatojuma, kas balstīts konkrētos valsts drošības vai noziedzības novēršanas apsvērumos saistībā ar konkrēto personu, un ja šīs uzraudzības darbības netiktu papildinātas ar attiecīgiem aizsardzības pasākumiem, kas vērsti pret varas ļaunprātīgu izmantošanu.

Turklāt EST atzīmēja, ka tiesiskais regulējums, "kurā indivīdiem nav paredzētas nekādas iespējas likt lietā tiesību aizsardzības līdzekļus, lai piekļūtu personas datiem, kas uz tiem attiecas, vai panākt šādu datu labošanu vai dzēšanu", nav saderīgs ar pamattiesībām uz efektīvu tiesību aizsardzību (Hartas 47. pants). Tādējādi lēmums par drošības zonu nespēja nodrošināt pamattiesību aizsardzības līmeni ASV, kas būtībā ir līdzvērtīgs ES direktīvā garantētajam, skatot kontekstā ar Hartu. Tādējādi EST lēmumu atzina par spēkā neesošu[63].

Piemērs. Lietā *Digital Rights Ireland*[64] EST pārbaudīja Direktīvas 2006/24/EK (Datu saglabāšanas direktīvas) saderību ar Hartas 7. un 8. pantu. Ar šo direktīvu elektronisko komunikāciju pakalpojumu sniedzējiem tika uzlikts pienākums saglabāt datus par datu plūsmu un atrašanās vietu vismaz sešus mēnešus līdz pat 24 mēnešiem, kā arī ļaut valstu kompetentajām iestādēm piekļūt šiem datiem, lai novērstu, izmeklētu, atklātu smagus noziegumus un sauktu pie atbildības. Direktīva neatļāva saglabāt elektroniskās komunikācijas saturu. EST atzīmēja, ka datos, kas pakalpojumu sniedzējiem bija jāsaglabā saskaņā ar direktīvu, bija ietverti tādi dati, kas nepieciešami, lai izsekotu un identificētu komunikācijas avotu un galamērķi, komunikācijas datumu, laiku un ilgumu, izsaukšanas numuru, izsauktos numurus un IP adreses. Šie dati, "skatot kopumā, varētu ļaut izdarīt ļoti precīzus secinājumus par personu, kuru dati tikuši saglabāti, privāto dzīvi, tostarp ikdienas paradumiem,

63 EST lēmums atzīt Komisijas Lēmumu 520/2000/EK par spēkā neesošu balstījās arī uz citiem iemesliem, kas tiks aplūkoti citās šīs rokasgrāmatas sadaļās. Proti, EST uzskatīja, ka lēmums nelikumīgi ierobežo valstu datu aizsardzības uzraudzības iestāžu pilnvaras. Turklāt saskaņā ar drošības zonas režīmu indivīdiem nebija pieejami tiesiskās aizsardzības līdzekļi, ja viņi vēlētos piekļūt saviem personas datiem un/vai labot vai dzēst tos. Tādējādi tika apdraudēta arī Hartas 47. pantā nostiprināto pamattiesību uz efektīvu tiesību aizsardzību tiesā būtība.

64 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C-293/12 un C-594/12 *Digital Rights Ireland Ltd pret Minister for Communications, Marine and Natural Resources un citiem un Kärntner Landesregierung un citiem* [GC].

pastāvīgajām vai pagaidu dzīvesvietām, ikdienas vai citām gaitām, veiktajām darbībām, šo personu sociālajām attiecībām un aprindām, kurās tās mēdz uzturēties".

Tādējādi personas datu saglabāšana saskaņā ar direktīvu ir sevišķi nopietna iejaukšanās privātuma un personas datu aizsardzības tiesībās. Tomēr EST uzskatīja, ka iejaukšanās nav atstājusi nelabvēlīgu ietekmi uz šo tiesību būtību. Tiesību uz privātumu būtība netika apdraudēta, jo direktīva neļāva iegūt zināšanas par elektronisko komunikāciju saturu kā tādu. Tāpat netika apdraudēta tiesību uz personas datu aizsardzību būtība, jo direktīvā elektronisko komunikāciju pakalpojumu sniedzējiem tika prasīts ievērot noteiktus datu aizsardzības un datu drošības principus un šajā nolūkā ieviest attiecīgus tehniskos un organizatoriskos pasākumus.

Nepieciešamība un samērīgums

Ar Hartas 52. panta 1. punktu paredz, ka, ievērojot proporcionalitātes principu, Hartā atzīto pamattiesību un brīvību īstenošanu var ierobežot tikai tad, ja tas ir nepieciešams.

Ierobežojums var būt **nepieciešams**, ja ir jāveic pasākumi sabiedrības izvirzīto mērķu sasniegšanai, taču nepieciešamība, kā to interpretējusi EST, nozīmē arī to, ka īstenotajiem pasākumiem jābūt mazāk aizskarošiem salīdzinājumā ar citām iespējām tā paša mērķa sasniegšanai. Ierobežojumiem tiesībām uz privātās dzīves neaizskaramību un personas datu aizsardzību EST piemēro absolūtas nepieciešamības pārbaudi, norādot, ka "atkāpes un ierobežojumi jāīsteno tikai tiktāl, ciktāl tas ir noteikti nepieciešams". Ja ierobežojums tiek uzskatīts par noteikti nepieciešamu, jāizvērtē arī, vai tas ir samērīgs.

Proporcionalitāte nozīmē, ka priekšrocībām, kas izriet no ierobežojuma, jābūt lielākām nekā trūkumiem, ko tas rada attiecīgo pamattiesību īstenošanā[65]. Lai mazinātu ar tiesību uz privātumu un datu aizsardzību īstenošanu saistītos trūkumus un riskus, ir svarīgi, lai ierobežojumi ietvertu attiecīgus aizsardzības pasākumus.

65 EDAU (2017), *Necessity Toolkit*, 5. lpp.

Piemērs. Lietā *Volker und Markus Schecke*[66] EST secināja, ka, nosakot pienākumu publicēt visu noteikto lauksaimniecības fondu atbalsta saņēmēju – fizisku personu personas datus, nenošķirot tos atbilstoši tādiem pienācīgiem kritērijiem kā laikposmi, kuros viņi ir saņēmuši šādu atbalstu, atbalsta biežumu vai arī tā veidu un apmēru, Padome un Komisija ir pārkāpušas robežas, ko nosaka proporcionalitātes principa ievērošana.

Tāpēc EST secināja, ka ir jāizziņo par spēkā neesošiem daži Padomes Regulas (EK) Nr. 1290/2005 noteikumi un jāpaziņo Regula (EK) Nr. 259/2008 par spēkā neesošu kopumā[67].

Piemērs. Lietā *Digital Rights Ireland*[68] EST sprieda, ka Datu saglabāšanas direktīvas radītā iejaukšanās tiesībās uz privātumu neapdraudēja šo tiesību būtību, jo ar to tika aizliegts saglabāt elektronisko komunikāciju saturu. Tomēr tā secināja, ka direktīva nav saderīga ar Hartas 7. un 8. pantu, un atzina to par spēkā neesošu. Tā kā datus par datu plūsmu un atrašanās vietu, apkopojot un skatot kopumā, varēja analizēt un iezīmēt detalizētu indivīdu privātās dzīves ainu, tā nozīmēja nopietnu iejaukšanos šajās tiesībās. EST ņēma vērā, ka direktīva pieprasa saglabāt visus metadatus, kas attiecas uz fiksēto telefoniju, mobilo telefoniju, piekļuvi internetam, interneta e-pastu un interneta telefoniju, piemērojot visiem elektroniskās komunikācijas līdzekļiem, kuru izmantošana cilvēku ikdienas dzīvē ir ļoti izplatīta. Praktiski šī iejaukšanās skāra visus Eiropas iedzīvotājus. Ņemot vērā šīs iejaukšanās apjomu un nopietnību, EST uzskatīja, ka datu plūsmas un atrašanās vietas saglabāšana varētu būt attaisnojama tikai smagu noziegumu apkarošanai. Turklāt direktīva nenoteica nekādus objektīvus kritērijus, kas nodrošinātu, ka kompetento valsts iestāžu piekļuve saglabātajiem datiem būtu ierobežota ar noteikti nepieciešamo. Tajā nebija arī ietverti materiālie un procesuālie

66 EST 2010. gada 9. novembra spriedums apvienotajās lietas C-92/09 un C-93/09 *Volker und Markus Schecke GbR un Hartmut Eifert pret Land Hessen* [GC], 89. un 86. punkts.

67 Padomes 2005. gada 21. jūnija Regula (EK) Nr. 1290/2005 par kopējās lauksaimniecības politikas finansēšanu, OV 2005 L 209; Komisijas 2008. gada 18. marta Regula (EK) Nr. 259/2008, ar ko nosaka sīki izstrādātus noteikumus par to, kā piemērot Padomes Regulu (EK) Nr. 1290/2005 attiecībā uz informācijas publicēšanu par Eiropas Lauksaimniecības garantiju fonda (ELGF) un Eiropas Lauksaimniecības fonda lauku attīstībai (ELFLA) līdzekļu saņēmējiem, OV 2008 L 76.

68 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C-293/12 un C-594/12 *Digital Rights Ireland Ltd pret Minister for Communications, Marine and Natural Resources un citiem un Kärntner Landesregierung un citiem* [GC], 39. punkts.

nosacījumi, kas reglamentē valsts iestāžu, uz kurām neattiecās iepriekšējas pārbaudes tiesā vai citā neatkarīgā struktūrā, piekļuvi saglabātajiem datiem un to izmantojumu.

EST nonāca pie līdzīga secinājuma apvienotajās lietās *Tele2 Sverige AB pret Post-och telestyrelsen* un *Secretary of State for the Home Department pret Tom Watson un citiem*[69]. Tās attiecās uz "visu abonentu un reģistrēto lietotāju un visu elektronisko sakaru līdzekļu" datu plūsmas un atrašanās vietas informācijas, kā arī metadatu saglabāšanu bez "diferencēšanas, ierobežojumiem vai izņēmumiem atkarībā no sasniedzamā mērķa"[70]. Konkrētajā gadījumā tas, vai persona tikusi tieši vai netieši saistīta ar smagiem noziedzīgiem nodarījumiem, vai arī šī persona vai tās paziņojumi ir vai nav bijuši būtiski valsts drošībai, nebija priekšnosacījums viņas datu saglabāšanai. Tā kā nepastāv nedz nepieciešamā saikne starp saglabātajiem datiem un draudiem sabiedrības drošībai, nedz arī perioda vai ģeogrāfiskās zonas ierobežojumi, EST secināja, ka valsts tiesību akti pārsniedz to, kas ir noteikti nepieciešams cīņai ar smagiem noziegumiem[71].

Līdzīgu pieeju attiecībā uz nepieciešamības prasību izmanto Eiropas Datu aizsardzības uzraudzītājs savā metodiskajā līdzeklī *Necessity Toolkit*[72]. Metodiskā līdzekļa mērķis ir palīdzēt novērtēt ierosināto pasākumu atbilstību ES tiesību aktiem par datu aizsardzību. Tas tika izstrādāts, lai labāk sagatavotu ES politikas veidotājus un likumdevējus, kuri ir atbildīgi par tādu pasākumu sagatavošanu vai pārbaudi, kas saistīti ar personas datu apstrādi un ierobežo tiesības uz personas datu aizsardzību, kā arī citas Hartā noteiktās tiesības un brīvības.

Vispārējas nozīmes mērķi

Lai jebkāds Hartā atzīto tiesību izmantošanas ierobežojums būtu pamatots, tam ir arī patiesi jāatbilst Savienībā atzītajiem vispārējas nozīmes mērķiem vai nepieciešamībai aizsargāt citu tiesības un brīvības. Kas attiecas uz nepieciešamību aizsargāt citu tiesības un brīvības, tiesības uz personas datu aizsardzību bieži ir mijiedarbībā

69 EST 2016. gada 21. decembra spriedums apvienotajās lietās C-203/15 un C-698/15 *Tele2 Sverige AB pret Post- och telestyrelsen un Secretary of State for the Home Department pret Tom Watson un citiem* [GC], 105.–106. punkts.

70 Turpat, 105. punkts.

71 Turpat, 107. punkts.

72 EDAU (2017), *Necessity Toolkit*, Brisele, 2017. gada 11. aprīlis.

ar citām pamattiesībām. 1.3. iedaļā sniegta šādas mijiedarbības detalizēta analīze. Vispārējas nozīmes mērķi ietver ES vispārējos mērķus, kas noteikti Līguma par Eiropas Savienību (LES) 3. pantā, piemēram, miera un savas tautas labklājības veicināšanu, sociālo taisnīgumu un aizsardzību, kā arī brīvības, drošības un tiesiskuma telpas izveidošanu, kurā tiek nodrošināta personu brīva pārvietošanās, apvienojumā ar attiecīgiem noziedzības novēršanas un apkarošanas pasākumiem, kā arī citiem mērķiem un interesēm, ko aizsargā īpaši līgumu noteikumi[73]. Vispārīgajā datu aizsardzības regulā šajā sakarībā ir precizēts Hartas 52. panta 1. punkts: regulas 23. panta 1. punktā ir uzskaitīti vairāki vispārējas nozīmes mērķi, kas tiek uzskatīti par likumīgiem personu tiesību ierobežošanai, ar nosacījumu, ka ierobežojums ievēro tiesību uz personas datu aizsardzību būtību un ir nepieciešams un samērīgs. Valsts drošība un aizsardzība, noziedzības novēršana, svarīgu ES un dalībvalstu ekonomisko un finanšu interešu aizsardzība, sabiedrības veselība un sociālā drošība ir daži no šeit minētajiem sabiedrības interešu mērķiem.

Ir svarīgi pietiekami sīki definēt un izskaidrot vispārējo interešu mērķi, uz kuru attiecas ierobežojums, jo ierobežojuma nepieciešamība tiks vērtēta, balstoties uz šo informāciju. Skaidrs, detalizēts ierobežojuma mērķa un ierosināto pasākumu apraksts ir būtisks, lai varētu novērtēt tā nepieciešamību[74]. Ierobežojuma mērķis, tā nepieciešamība un samērīgums ir cieši saistīti.

Piemērs. Lieta *Schwarz pret Stadt Bochum*[75] attiecās uz tiesību uz privātās dzīves neaizskaramību un tiesību uz personas datu aizsardzību ierobežojumiem saistībā ar pirkstu nospiedumu ņemšanu un glabāšanu, dalībvalstu iestādēm izsniedzot pases[76]. Prasītājs iesniedza pieteikumu *Stadt Bochum*, lai saņemtu pasi, bet atteicās nodot pirkstu nospiedumus. Pēc tam *Stadt Bochum* noraidīja viņa pases pieteikumu. Tad viņš iesniedza prasību Vācijas tiesā par pases izsniegšanu bez pirkstu nospiedumu noņemšanas. Vācijas tiesa nodeva prejudiciālo jautājumu EST – vai 1. panta 2. punkts Regulā (EK) Nr. 2252/2004 par drošības elementu un biometrijas standartiem dalībvalstu izdotās pasēs un ceļošanas dokumentos ir uzskatāms par spēkā esošu.

73 Paskaidrojumi attiecībā uz Pamattiesību hartu (2007/C 303/02), OV 2007 Nr. C 303, 17.–35. lpp.

74 EDAU (2017), *Necessity Toolkit*, Brisele, 2017. gada 11. aprīlis, 4. lpp.

75 EST 2013. gada 17. oktobra spriedums lietā C-291/12 *Michael Schwarz pret Stadt Bochum*.

76 Turpat, 33.–36. punkts.

EST norādīja, ka pirkstu nospiedumi **ir personas dati**, jo tie objektīvi satur unikālu informāciju par indivīdiem, ļaujot tos precīzi identificēt, savukārt pirkstu nospiedumu ņemšana un glabāšana ir apstrāde. Pēdējā minētā apstrāde, ko regulē ar Regulas (EK) Nr. 2252/2004 1. panta 2. punktu, apdraud tiesības uz privātās dzīves neaizskaramību un personas datu aizsardzību[77]. Tomēr Hartas 52. panta 1. punkts pieļauj ierobežojumus šo tiesību īstenošanai, ja vien šie ierobežojumi ir paredzēti tiesību aktos, ievēro šo tiesību būtību un saskaņā ar proporcionalitātes principu ir nepieciešami un patiesi atbilst Savienības atzītajiem vispārējās nozīmes mērķiem vai nepieciešamībai aizsargāt citu tiesības un brīvības.

Šajā gadījumā EST, pirmkārt, atzīmēja, ka ierobežojums, kas izriet no pirkstu nospiedumu ņemšanas un glabāšanas, izsniedzot pases, ir jāuzskata **par tiesību aktos paredzētu**, jo šīs darbības ir paredzētas Regulas (EK) Nr. 2252/2004 1. panta 2. punktā. Otrkārt, šis regulējums tika izstrādāts, lai novērstu pasu viltošanu un to izmantošanu krāpnieciskos nolūkos. Tādējādi 1. panta 2. punkts ir izstrādāts, lai cita starpā novērstu nelikumīgu ieceļošanu ES, tādējādi tas ir Savienības atzīts vispārējo interešu mērķis. Treškārt, no EST rīcībā esošajiem pierādījumiem neizriet, ne arī tika apgalvots, ka šo tiesību īstenošanas ierobežojumi šajā gadījumā neievērotu šo tiesību būtību. Ceturtkārt, pirkstu nospiedumu glabāšanai īpaši drošā datu nesējā, kā paredzēts šajā normā, nepieciešama sarežģīta tehnoloģija. Šāda glabāšana, iespējams, samazinātu pasu viltošanas risku un atvieglotu to iestāžu darbu, kuras ir atbildīgas par pasu autentiskuma pārbaudi uz ES robežām. Fakts, ka metode nav pilnībā uzticama, nav noteicošais. Lai gan šī metode nenovērš visu nepiederošo personu ielaišanu, pietiek ar to, ka tā ievērojami samazina šādu iespējamību. Ņemot vērā iepriekš minēto, EST secināja, ka pirkstu nospiedumu ņemšana un saglabāšana, kas minētas Regulas (EK) Nr. 2252/2004 1. panta 2. punktā, ir piemērotas, lai sasniegtu šīs regulas izvirzīto mērķi un, paplašinot – arī nelegālas ieceļošanas ES novēršanu[78].

Pēc tam EST vērtēja, vai šāda apstrāde ir **nepieciešama**, atzīmējot, ka attiecīgā darbība bija saistīta tikai ar divu pirkstu nospiedumu noņemšanu, kurus parasti var redzēt arī citas personas, tāpēc šī nav intīma rakstura darbība. Tā neizraisa arī īpašu fizisku vai garīgu diskomfortu skartajai personai vairāk nekā tad, kad tiek uzņemts šīs personas sejas attēls. Jāatzīmē arī, ka vienīgā

77 Turpat, 27.–30. punkts.

78 Turpat, 35.–45. punkts.

reālā alternatīva pirkstu nospiedumu noņemšanai, kas tika piedāvāta tiesvedības laikā EST, bija varavīksnenes skenēšana. Nekas EST iesniegtajos lietas materiālos neliecina, ka pēdējā minētā procedūra veido mazāku Hartas 7. un 8. pantā atzīto tiesību aizskārumu nekā pirkstu nospiedumu ņemšana. Turklāt attiecībā uz šo divu metožu efektivitāti nav šaubu, ka varavīksnenes atpazīšanas tehnoloģija vēl nav tik attīstīta kā pirkstu nospiedumu atpazīšanas tehnoloģija, turklāt šobrīd tā ir ievērojami dārgāka nekā pirkstu nospiedumu salīdzināšanas procedūra, un šā iemesla dēļ tā ir mazāk piemērota vispārējai izmantošanai. Attiecīgi EST nebija informēta par pasākumiem, kas būtu pietiekami efektīvi, lai palīdzētu sasniegt mērķi nodrošināt aizsardzību pret pasu izmantošanu krāpnieciskos nolūkos, un veidotu mazāku apdraudējumu Hartas 7. un 8. pantā atzītajām tiesībām nekā pasākumi, kas izriet no metodes, kuras pamatā ir pirkstu nospiedumu izmantošana[79].

EST atzīmēja, ka Regulas (EK) Nr. 2252/2004 4. panta 3. punktā ir skaidri noteikts, ka pirkstu nospiedumus var izmantot tikai, lai pārbaudītu pases autentiskumu un tās turētāja identitāti, savukārt Regulas 1. panta 2. punkts neparedz pirkstu nospiedumu glabāšanu nekur citur, kā tikai pasē, kas pieder turētājam. Tādējādi regula nenodrošināja juridisku pamatu tās ietvaros savākto datu centralizētai glabāšanai vai šādu datu izmantošanai citiem mērķiem kā tikai nelikumīgas ieceļošanas ES novēršanai[80]. Ņemot vērā visus iepriekš minētos apsvērumus, EST secināja, ka uzdotā jautājuma pārbaude neatklāja neko tādu, kas varētu ietekmēt Regulas (EK) Nr. 2252/2004 1. panta 2. punkta spēkā esamību.

Hartas un Cilvēktiesību konvencijas (ECTK) salīdzinājums

Lai gan formulējums ir atšķirīgs, Hartas 52. panta 1. punktā paredzētie tiesību likumīgo ierobežojumu nosacījumi ir līdzīgi ECTK 8. panta 2. punktam par tiesībām uz privātās dzīves neaizskaramību. Savā judikatūrā EST un ECT bieži atsaucas viena uz otras spriedumiem pastāvīga dialoga starp abām tiesām ietvaros, tiecoties panākt saskaņotu datu aizsardzības noteikumu interpretāciju. Hartas 52. panta 3. punktā noteikts, ka "ciktāl Hartā ir ietvertas tiesības, kuras atbilst Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijā garantētajām tiesībām, šo tiesību nozīme un apjoms ir tāds pats kā minētajā Konvencijā noteiktajām tiesībām". Tomēr Hartas

79 EST 2013. gada 17. oktobra spriedums lietā C-291/12 *Michael Schwarz pret Stadt Bochum*, 46.–53. punkts.

80 Turpat, 56.–61. punkts.

8. pants tieši neatbilst ECTK pantam[81]. Hartas 52. panta 3. punkts attiecas uz tiesību, ko aizsargā jebkura tiesību sistēma, saturu un apjomu, nevis uz to ierobežošanas nosacījumiem. Tomēr, ņemot vērā plašāku dialogu un sadarbību starp abām tiesām, EST savā analīzē var ņemt vērā likumīga ierobežojuma kritērijus saskaņā ar ECTK 8. pantu, kā to interpretējusi ECT. Ir iespējams arī pretējs scenārijs, saskaņā ar kuru ECT var atsaukties uz Hartā paredzētajiem likumīga ierobežojuma nosacījumiem. Jebkurā gadījumā ir jāņem vērā arī tas, ka ECT neietilpst pilnīgs Hartas 8. panta ekvivalents, kas atsaucas uz personas datu aizsardzību un jo īpaši uz datu subjekta tiesībām, apstrādes likumīgajiem pamatiem un neatkarīgas iestādes veiktu uzraudzību. Daži Hartas 8. panta elementi var būt balstīti ECT judikatūrā, kas izstrādāta saskaņā ar ECTK 8. pantu un attiecas uz Konvenciju Nr. 108[82]. Šī saikne nodrošina EST un ECT savstarpēju iedvesmu jautājumos, kas saistīti ar datu aizsardzību.

1.3. Mijiedarbība ar citām tiesībām un leģitīmajām interesēm

Svarīgākie aspekti

- Tiesības uz datu aizsardzību bieži mijiedarbojas ar citām tiesībām, piemēram, vārda brīvību un tiesībām saņemt un izplatīt informāciju.
- Šī mijiedarbība bieži ir pretrunīga. Lai gan ir situācijas, kad tiesības uz personas datu aizsardzību ir pretrunā konkrētām tiesībām, ir arī situācijas, kad tiesības uz personas datu aizsardzību efektīvi nodrošina šo pašu konkrēto tiesību ievērošanu. Piemēram, saistībā ar vārda brīvību, ņemot vērā, ka dienesta noslēpums ir tiesību uz privātās dzīves neaizskaramību sastāvdaļa.
- Nepieciešamība aizsargāt citu personu tiesības un brīvības ir viens no kritērijiem, ko izmanto, vērtējot tiesību uz personas datu aizsardzību likumīgo ierobežojumu.
- Ja uz spēles ir liktas dažādas tiesības, tiesas veic izsvēršanu, lai tās saskaņotu.
- Vispārīgā datu aizsardzības regula uzliek dalībvalstīm pienākumu saskaņot tiesības uz personas datu aizsardzību ar vārda un informācijas brīvību.
- Dalībvalstis var arī pieņemt īpašus noteikumus savos tiesību aktos, lai saskaņotu tiesības uz personas datu aizsardzību ar publisku piekļuvi oficiālajiem dokumentiem un pienākumu ievērot dienesta noslēpumu.

81 EDAU (2017), *Necessity Toolkit*, Brisele, 2017. gada 11. aprīlis, 6. lpp.

82 Paskaidrojumi attiecībā uz Pamattiesību hartu (2007/C 303/02), 8. pants.

Tiesības uz personas datu aizsardzību nav absolūtas. Priekšnosacījumi šo tiesību likumīgai ierobežošanai ir aprakstīti iepriekš. Viens no kritērijiem likumīgiem tiesību ierobežojumiem, kas atzīts gan EP, gan ES tiesību aktos, ir tāds, ka iejaukšanās datu aizsardzībā ir nepieciešama citu personu tiesību un brīvību aizsardzībai. Ja datu aizsardzība mijiedarbojas ar citām tiesībām, gan ECT, gan EST ir vairākkārt norādījušas, ka, piemērojot un interpretējot ECTK 8. pantu un Hartas 8. pantu, ir jāveic izsvēršana ar citām tiesībām[83]. Vairākos būtiskos piemēros tiks parādīts, kā panākt šo līdzsvaru.

Papildus šo tiesu veiktajai izsvēršanai valstis nepieciešamības gadījumā var pieņemt tiesību aktus, lai līdzsvarotu tiesības uz personas datu aizsardzību ar citām tiesībām. Šā iemesla dēļ Vispārīgajā datu aizsardzības regulā ir paredzētas vairākas jomas, kurās valstis piemēro atkāpes.

Attiecībā uz vārda brīvību VDAR pieprasa, lai dalībvalstis ar tiesību aktiem saglabātu līdzsvaru "starp tiesībām uz personas datu aizsardzību saskaņā ar šo regulu un tiesībām uz vārda un informācijas brīvību, tostarp apstrādi žurnālistikas vajadzībām un akadēmiskās, mākslinieciskās vai literārās izpausmes vajadzībām"[84]. Dalībvalstis var arī pieņemt tiesību aktus, lai līdzsvarotu datu aizsardzību ar publisku piekļuvi oficiālajiem dokumentiem un pienākumiem ievērot dienesta noslēpumu, kas ir tiesību uz privātās dzīves neaizskaramību veids[85].

1.3.1. Vārda brīvība

Vienas no tiesībām, kas visbūtiskāk mijiedarbojas ar tiesībām uz datu aizsardzību, ir tiesības uz vārda brīvību.

Vārda brīvību aizsargā Hartas 11. pants ("Vārda un informācijas brīvība"). Šīs tiesības ietver "brīvību saņemt un izplatīt informāciju vai idejas bez valsts iestāžu iejaukšanās un neatkarīgi no valstu robežām". Informācijas brīvība atbilstoši Hartas 11. pantam un ECTK 10. pantam aizsargā tiesības ne tikai sniegt, bet arī *saņemt* informāciju.

83 ECT 2012. gada 7. februāra spriedums lietā *Von Hannover pret Vāciju (Nr. 2)* [GC], Nr. 40660/08 un Nr. 60641/08; EST 2011. gada 24. novembra spriedums apvienotajās lietās C-468/10 un C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) un Federación de Comercio Electrónico y Marketing Directo (FECEMD) pret Administración del Estado*, 48. punkts; EST 2008. gada 29. janvāra spriedums lietā C-275/06 *Productores de Música de España (Promusicae) pret Telefónica de España SAU* [GC], 68. punkts.

84 Vispārīgā datu aizsardzības regula, 85. pants

85 Turpat, 86. un 90. pants.

Vārda brīvības ierobežojumiem jāatbilst iepriekš aprakstītajiem Hartas 52. panta 1. punktā paredzētajiem kritērijiem. Turklāt 11. pants atbilst ECTK 10. pantam. Saskaņā ar Hartas 52. panta 3. punktu, ciktāl tajā ietvertas tiesības, kas atbilst ECTK garantētajām tiesībām, "šo tiesību nozīme un apjoms ir tāds pats kā minētajā Konvencijā noteiktajām tiesībām". Līdz ar to ierobežojumi, ko var likumīgi piemērot Hartas 11. pantā garantētajām tiesībām, nedrīkst pārsniegt ECTK 10. panta 2. punktā paredzētos ierobežojumus, proti, tiem jābūt noteiktiem tiesību aktos un tiem jābūt nepieciešamiem demokrātiskā sabiedrībā, "lai aizsargātu citu cilvēku cieņu un tiesības". Šādas tiesības jo īpaši ietver tiesības uz privātās dzīves neaizskaramību un tiesības uz personas datu aizsardzību.

Saistību starp personas datu aizsardzību un vārda brīvību regulē Vispārīgās datu aizsardzības regulas 85. pants "Apstrāde un vārda un informācijas brīvība". Atbilstoši šim pantam dalībvalstis līdzsvaro tiesības uz personas datu aizsardzību ar tiesībām uz vārda un informācijas brīvību. Jo īpaši atbrīvojumus un atkāpes no Vispārīgās datu aizsardzības regulas konkrētām nodaļām izdara žurnālistikas vajadzībām un akadēmiskās, mākslinieciskās vai literārās izpausmes vajadzībām, ciktāl tie ir nepieciešami, lai līdzsvarotu tiesības uz personas datu aizsardzību ar vārda un informācijas brīvību.

Piemērs. Lietā *Tietosuojavaltuutettu pret Satakunnan Markkinapörssi Oy un Satamedia Oy*[86] EST lūdza definēt attiecības starp datu aizsardzību un preses brīvību[87]. Tiesai bija jāizskata gadījums, kurā uzņēmums, izmantojot SMS pakalpojumu, bija izplatījis no Somijas nodokļu iestādēm likumīgi iegūtus nodokļu datus par aptuveni 1,2 miljoniem fizisku personu. Somijas datu aizsardzības uzraudzības iestāde bija pieņēmusi lēmumu, prasot uzņēmumam pārtraukt šo datu izplatīšanu. Uzņēmums apstrīdēja šo lēmumu valsts tiesā, kura lūdza EST precizēt Datu aizsardzības direktīvas interpretāciju. Jo īpaši EST bija jāpārbauda, vai personas datu, ko nodokļu iestādes bija darījušas pieejamus, apstrāde, lai dotu iespēju mobilo tālruņu lietotājiem saņemt nodokļu datus saistībā ar citām fiziskām personām, ir jāuzskata par darbību, kas veikta tikai žurnālistikas nolūkiem. Secinājusi, ka uzņēmuma darbības veido

86 EST 2008. gada 16. decembra spriedums lietā C-73/07 *Tietosuojavaltuutettu pret Satakunnan Markkinapörssi Oy un Satamedia Oy* [GC], 56., 61. un 62. punkts.

87 Lieta attiecās uz Datu aizsardzības direktīvas 9. panta interpretāciju, kas tagad aizstāts ar Vispārīgās datu aizsardzības regulas 85. pantu, kurā teikts: "Dalībvalstis paredz izņēmumus vai atkāpes no šīs nodaļas, IV nodaļas un VI nodaļas noteikumiem personas datu apstrādei, kas veikta tikai un vienīgi žurnālistikas nolūkiem vai mākslinieciskās vai literārās izteiksmes nolūkiem tikai tad, ja tie vajadzīgi, lai saskaņotu tiesības uz privātās dzīves neaizskaramību ar normām, kas reglamentē vārda brīvību".

"personas datu apstrādi" Datu aizsardzības direktīvas 3. panta 1. punkta izpratnē, EST analizēja direktīvas 9. pantu (par personas datu apstrādi un vārda brīvību). Vispirms Tiesa norādīja uz to, cik svarīgas ir tiesības uz vārda brīvību katrā demokrātiskā sabiedrībā, un apgalvoja, ka ar minēto brīvību saistītie jēdzieni, ieskaitot žurnālistiku, ir jāinterpretē plaši. Tad Tiesa norādīja, ka, lai nodrošinātu līdzsvaru starp abām šīm pamattiesībām, atkāpes un tās ierobežojumi ir jāīsteno tikai tiktāl, ciktāl tas ir noteikti nepieciešams. Minētajos apstākļos EST uzskatīja, ka tādas darbības, kādas bija veikuši uzņēmumi saistībā ar datiem, kas saskaņā ar valsts tiesību aktiem iegūti no publiskiem dokumentiem, var tikt kvalificētas kā "žurnālistikas darbības", ja to mērķis ir publiskot informāciju, viedokļus vai idejas ar jebkāda izplatīšanas līdzekļa palīdzību. Tiesa arī nosprieda, ka ne tikai plašsaziņas līdzekļu uzņēmumi var veikt minētās darbības un tās var būt saistītas ar mērķi gūt peļņu. EST tomēr atstāja valsts tiesas ziņā noteikt, vai konkrētais gadījums bija tieši šāds gadījums.

Šo pašu lietu izskatīja arī ECT pēc tam, kad valsts tiesa, balstoties uz EST norādēm, lēma, ka uzraudzības iestādes rīkojums pārtraukt visas nodokļu informācijas publicēšanu bija pamatota iejaukšanās uzņēmuma vārda brīvībā. ECT šo pieeju atbalstīja[88]. Tā secināja, ka, kaut arī tika aizskartas uzņēmumu tiesības sniegt informāciju, šī iejaukšanās bija saskaņā ar tiesību aktiem, tai bija likumīgs mērķis un tā bija nepieciešama demokrātiskā sabiedrībā.

Tiesa atgādināja judikatūras kritērijus, pēc kuriem valstu iestādēm un pašai ECT ir jāvadās, līdzsvarojot vārda brīvību ar tiesībām uz privātās dzīves neaizskaramību. Ja uz spēles ir politiska runa vai debates par sabiedrībai svarīgu jautājumu, nav daudz iespēju ierobežot tiesības saņemt un izplatīt informāciju, jo sabiedrībai ir tiesības būt informētai, "un šīs ir pamattiesības demokrātiskā sabiedrībā"[89]. Tomēr nevar uzskatīt, ka raksti presē, kuru mērķis ir tikai apmierināt konkrētas lasītāju daļas interesi par personas privātās dzīves detaļām, veicina sabiedrības interešu diskusijas. Atkāpe no datu aizsardzības noteikumiem žurnālistikas vajadzībām ir paredzēta, lai ļautu žurnālistiem piekļūt datiem, tos vākt un apstrādāt, lai viņi varētu veikt savas žurnālistu darbības. Tādējādi patiešām piekļuves nodrošināšana lielajiem nodokļu datu apjomiem un atļauja prasītājiem uzņēmumiem vākt un apstrādāt lielus nodokļu datu apjomus ir sabiedrības interesēs. Turpretī Tiesa konstatēja, ka

88 ECT 2017. gada 27. jūnija spriedums lietā *Satakunnan Markkinapörssi Oy un Satamedia Oy pret Somiju* [GC], Nr. 931/13.

89 Turpat, 169. punkts.

šādu neapstrādātu datu masveida izplatīšana laikrakstos nemainītā veidā un bez jebkāda analītiska ieguldījuma nav sabiedrības interesēs. Informācija par nodokļiem, iespējams, ļāva ziņkārīgiem sabiedrības locekļiem klasificēt indivīdus pēc viņu ekonomiskā stāvokļa un apmierināt sabiedrības alkas pēc informācijas par citu privāto dzīvi. To nevar uzskatīt par ieguldījumu sabiedrības interešu diskusijā.

Piemērs. Lietā *Google Spain*[90] EST apsvēra, vai *Google* bija pienākums no sava meklēšanas saraksta rezultātiem dzēst novecojušu informāciju par prasītāja finansiālajām grūtībām. Veicot *Google* meklētājprogrammā meklēšanu ar prasītāja vārdu, meklēšanas rezultātos tika parādītas saites uz veciem rakstiem laikrakstos, kuros minēta viņa saistība ar bankrota procedūrām. Prasītājs to uzskatīja par viņa tiesību uz privātās dzīves neaizskaramību un personas datu aizsardzību pārkāpumu, jo tiesvedība tika pabeigta pirms vairākiem gadiem, kā rezultātā šādas atsauces bija nebūtiskas.

EST vispirms paskaidroja, ka interneta meklētājprogrammas un meklēšanas rezultāti ar personas datiem var izveidot detalizētu personas profilu. Ņemot vērā sabiedrības pieaugošo digitalizāciju, prasība, lai personas dati būtu precīzi un lai to publicēšana nepārsniegtu nepieciešamo, t. i., sniegt informāciju sabiedrībai, ir būtiska, lai nodrošinātu indivīdiem augstu datu aizsardzības līmeni. Pārzinim attiecībā uz šo apstrādi viņa pienākumu, pilnvaru un iespēju ietvaros ir jāpārliecinās, ka apstrāde atbilst ES tiesību aktu prasībām, lai ieviestajām juridiskajām garantijām būtu pilnīgs spēks. Tas nozīmē, ka tiesības uz personas datu dzēšanu, kad apstrāde vairs nav nepieciešama vai tās termiņš ir notecējis, attiecas arī uz meklētājprogrammām, kuras tika atzītas par pārziņiem, nevis tikai apstrādātājiem (skatīt 2.3.1. iedaļu).

Pārbaudot, vai uzņēmumam *Google* bija jāizņem ar pieteikuma iesniedzēju saistītās saites, EST nosprieda, ka noteiktos apstākļos indivīdiem ir tiesības pieprasīt savu personīgo datu dzēšanu no interneta meklētājprogrammas meklēšanas rezultātiem. Šīs tiesības var tikt izmantotas, ja informācija, kas attiecas uz personu, ir neprecīza, neadekvāta, neatbilstoša vai pārmērīga datu apstrādes nolūkiem. EST atzina, ka šīs tiesības nav absolūtas. Tās ir jālīdzsvaro ar citām tiesībām, jo īpaši ar plašas sabiedrības interesēm un tiesībām piekļūt informācijai. Katrs dzēšanas pieprasījums ir jāizvērtē atsevišķi, lai nodrošinātu līdzsvaru starp datu subjekta pamattiesībām uz personas

90 EST 2014. gada 13. maija spriedums lietā C-131/12 *Google Spain SL un Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 81.–83. punkts.

datu aizsardzību un privāto dzīvi, no vienas puses, un visu interneta lietotāju likumīgajām interesēm, no otras puses. EST sniedza norādījumus par faktoriem, kas jāņem vērā izsvēršanas gaitā. Īpaši svarīgs faktors ir konkrētās informācijas raksturs. Ja informācija ir sensitīva attiecībā uz indivīda privāto dzīvi un ja attiecībā uz informācijas pieejamību nav sabiedrības intereses, datu aizsardzība un privātums ir svarīgāki par plašas sabiedrības tiesībām piekļūt informācijai. Tieši pretēji, ja izrādās, ka datu subjekts ir publiska persona vai informācijas raksturs attaisno piekļuves šādai informācijai piešķiršanu plašākai sabiedrībai, tad iejaukšanās datu aizsardzības un privātuma pamattiesībās ir pamatota.

Pēc sprieduma 29. panta darba grupa pieņēma pamatnostādnes par EST nolēmuma īstenošanu. Pamatnostādnēs ir iekļauts kopējais kritēriju saraksts, kas uzraudzības iestādēm jāizmanto, izskatot sūdzības, kas saistītas ar personu dzēšanas pieprasījumiem, un līdzsvarojot šīs tiesības[91].

Attiecībā uz datu aizsardzības tiesību un vārda brīvības saskaņošanu ECT ir izdevusi vairākus nozīmīgus spriedumus.

Piemērs. Lietā *Axel Springer AG pret Vāciju*[92] ECT uzskatīja, ka tiesas noteiktais aizliegums prasītājam uzņēmumam, kurš vēlējās publicēt rakstu par populāra aktiera apcietināšanu un notiesāšanu, pārkāpa ECTK 10. panta prasības. ECT atkārtoti norādīja kritērijus, kas jāņem vērā, līdzsvarojot vārda brīvību ar tiesībām uz privātās dzīves neaizskaramību, kā noteikts tās judikatūrā:

- vai notikums, uz kuru publicētais raksts attiecās, bija vispārējas nozīmes;
- vai attiecīgā persona bija publiska persona; un
- kā informācija tika iegūta un vai tā bija ticama.

ECT secināja, ka aktiera apcietināšana un notiesāšana bija publisks juridisks fakts, tāpēc bija sabiedrības interesēs, jo aktieris bija pietiekami labi pazīstams, lai būtu uzskatāms par publisku personu, informāciju sniedza

91 29. panta darba grupas (2014) *EST sprieduma "Google Spain SL un Google Inc pret Agencia Española de Protección de Datos (AEPD) un Mario Costeja González" (C-131/12) īstenošanas pamatnostādnes*, WP 225, Brisele, 2014. gada 26. novembris.

92 ECT 2012. gada 7. februāra spriedums lietā *Axel Springer AG pret Vāciju* [GC], Nr. 39954/08, 90. un 91. punkts.

prokuratūra, savukārt puses tās precizitāti neapstrīdēja. Tāpēc uzņēmumam noteiktie publicēšanas ierobežojumi nebija samērīgi attiecībā uz likumīgo mērķi aizsargāt prasītāja privāto dzīvi. Tāpēc tiesa atzina, ka šajā lietā ir pārkāpts ECTK 10. pants.

Piemērs. Lieta *Coudec un Hachette Filipacchi Associés pret Franciju*[93] skāra Francijas nedēļas žurnāla publicēto interviju ar *Coste* kundzi, kura apgalvoja, ka Monako princis Alberts ir viņas dēla tēvs. Intervijā tika aprakstītas arī *Coste* kundzes attiecības ar princi un tas, kā viņš reaģēja uz bērna piedzimšanu, papildinot ar prinča un bērna fotogrāfijām. Princis Alberts cēla prasību pret izdevēju par viņa tiesību uz privātās dzīves aizsardzību pārkāpumiem. Francijas tiesas lēma, ka raksta publicēšana ir nodarījusi neatgriezenisku kaitējumu princim Albertam, un lika izdevējam atlīdzināt zaudējumus un publicēt informāciju par spriedumu uz žurnāla priekšējā vāka.

Žurnāla izdevēji ierosināja lietu ECT, apgalvojot, ka ar Francijas tiesu spriedumu ir nepamatoti pārkāptas viņu tiesības uz vārda brīvību. ECT bija jāizsver prinča Alberta tiesības uz privātās dzīves neaizskaramību ar izdevēja vārda brīvības tiesībām un plašākas sabiedrības tiesībām uz informāciju. Svarīgi apsvērumi bija arī *Coste* kundzes tiesības informēt sabiedrību par savu stāstu un bērna interese par tēva un bērna attiecību oficiālu nodibināšanu.

ECT uzskatīja, ka intervijas publicēšana ir iejaukšanās prinča privātajā dzīvē, un turpināja pārbaudīt, vai šāda iejaukšanās ir nepieciešama. Tā uzskatīja, ka publikācija skar publisku personu un sabiedrības intereses, jo Monako pilsoņiem bija interese uzzināt par prinča bērna esamību, jo mantotās monarhijas nākotne ir "nelokāmi saistīta ar pēcnācēju esamību", tādējādi šis jautājums satrauc sabiedrību[94]. Tiesa arī atzīmēja, ka raksts ļāva *Coste* kundzei un viņas bērnam īstenot viņu tiesības uz vārda brīvību. Valsts tiesas nebija pienācīgi apsvērušas principus un kritērijus, kas izstrādāti ECT judikatūrā, līdzsvarojot tiesības uz privātās dzīves neaizskaramību ar tiesībām uz vārda brīvību. Tiesa secināja, ka Francija ir pārkāpusi ECTK 10. pantu par vārda brīvību.

ECT judikatūrā viens no izšķirošajiem kritērijiem šo tiesību līdzsvarošanā ir jautājums, vai attiecīgā izpausme veicina debates, kas ir visas sabiedrības interesēs.

93 ECT 2015. gada 10. novembra spriedums lietā *Coudec un Hachette Filipacchi Associés pret Franciju* [GC], Nr. 40454/07.

94 Turpat, 104.–116. punkts.

Piemērs. Lietā *Mosley pret Apvienoto Karalisti*[95] nacionālais nedēļas laikraksts publicēja intīmas fotogrāfijas ar prasītāju – pazīstamu personu, kurš pēc tam veiksmīgi cēla civilprasību pret izdevēju un kuram tika piespriesta zaudējumu atlīdzība. Kaut arī viņam bija piešķirta naudas kompensācija, viņš sūdzējās, ka joprojām cieš no viņa tiesību uz privātumu pārkāpuma, jo pirms attiecīgo fotoattēlu publicēšanas viņam tika liegta iespēja lūgt tiesu noteikt aizliegumu, jo nepastāvēja likumīga prasība laikrakstam iepriekš brīdināt par publikāciju.

ECT atzīmēja, ka, kaut arī šāda materiāla izplatīšana galvenokārt bija paredzēta izklaidei, nevis izglītošanai, uz to neapšaubāmi attiecās ECTK 10. pantā paredzētā aizsardzība, kas varētu atbilst ECTK 8. panta prasībām, ja informācija bija privāta un intīma rakstura un tās izplatīšana nebija sabiedrības interesēs. Tomēr īpaša uzmanība bija jāpievērš, pārbaudot ierobežojumus, kas varētu darboties pirms publicēšanas kā sava veida cenzūra. Ņemot vērā atturošo efektu, ko varētu radīt iepriekšējas paziņošanas prasība, šaubas par tā efektivitāti un plašo rīcības brīvību šajā jomā, ECT secināja, ka juridiski saistošas iepriekšējas paziņošanas prasības pastāvēšana nav nepieciešama saskaņā ar 8. pantu. Attiecīgi Tiesa atzina, ka šajā lietā 8. pants nav pārkāpts.

Piemērs. Lietā *Bohlen pret Vāciju*[96] prasītājs, pazīstams dziedātājs un mākslinieciskais producents, bija publicējis autobiogrāfisku grāmatu un pēc tiesas spriedumiem bija spiests izņemt dažus fragmentus. Sižets tika plaši atspoguļots nacionālajos plašsaziņas līdzekļos, un kāds tabakas uzņēmums uzsāka humoristisku reklāmas kampaņu saistībā ar šo notikumu, izmantojot prasītāja vārdu bez viņa piekrišanas. Prasītājs neveiksmīgi lūdza reklāmas uzņēmumu atlīdzināt zaudējumus, apgalvojot, ka ir pārkāptas viņa tiesības saskaņā ar ECTK 8. pantu. ECT atkārtoti pauda kritērijus izsvēršanai starp tiesībām uz privātās dzīves neaizskaramību un tiesībām uz vārda brīvību un uzskatīja, ka 8. pants nav pārkāpts. Prasītājs bija publiska persona, un reklāmā nebija atsauces uz viņa privātās dzīves detaļām, bet gan uz publisku notikumu, par kuru jau runāja plašsaziņas līdzekļi un kas ietilpa publiskajās debatēs. Turklāt reklāmai bija humoristisks raksturs, un tajā nebija nekā pazemojoša vai negatīva attiecībā uz prasītāju.

95 ECT 2011. gada 10. maija spriedums lietā *Mosley pret Apvienoto Karalisti*, Nr. 48009/08, 129. un 130. punkts.

96 ECT 2015. gada 19. februāra spriedums lietā *Bohlen pret Vāciju*, Nr. 53495/09, 45.–60. punkts.

Piemērs. Lietā *Biriuk pret Lietuvu*[97] prasītāja ECT apgalvoja, ka Lietuva nav izpildījusi tās pienākumu nodrošināt viņas tiesību uz privāto dzīvi neaizskaramību, jo, lai arī viens no nozīmīgākajiem laikrakstiem bija izdarījis nopietnu viņas privātuma pārkāpumu, valsts tiesas, kuras izskatīja lietu, piesprieda viņai niecīgu kompensāciju materiālo zaudējumu atlīdzībai. Piespriežot atlīdzināt morālo kaitējumu, valsts tiesas bija piemērojušas valsts tiesību aktu noteikumus par informācijas sniegšanu sabiedrībai, ar kuriem noteica zemu maksimālās kompensācijas summu par morālo kaitējumu, ko izraisījusi plašsaziņas līdzekļu nelikumīga informācijas par personas privāto dzīvi izplatīšana sabiedrībai. Lietas pamatā bija fakts, ka lielākais Lietuvas dienas laikraksts publicēja rakstu sākumlapā, norādot, ka prasītāja bija *HIV* pozitīva. Rakstā arī tika kritizēta prasītājas uzvedība un apšaubīti viņas morāles standarti.

ECT atkārtoti uzsvēra, ka personas datu, kā arī medicīnisku datu aizsardzība ir būtiski svarīga, lai persona varētu izmantot savas tiesības uz privātās dzīves neaizskaramību, ko garantē ECTK. Veselības datu konfidencialitāte ir īpaši svarīga, jo medicīnisko datu izpaušana (šajā gadījumā prasītājas *HIV* statuss) var dramatiski ietekmēt personas privāto un ģimenes dzīvi, personas nodarbinātības situāciju un iekļaušanos sabiedrībā. Tiesa īpašu nozīmi piešķīra faktam, ka atbilstoši laikrakstā sniegtajam ziņojumam slimnīcas medicīniskais personāls bija sniedzis informāciju par prasītājas *HIV* statusu, acīmredzami pārkāpjot savu pienākumu ievērot mediķu noslēpumu. Tādējādi prasītājas tiesību uz privāto dzīvi aizskārums bija nelikumīgs.

Rakstu publicēja prese, un vārda brīvība arī veido ECTK ietvertās pamattiesības. Tomēr, pārbaudot, vai sabiedrības interešu klātesamība attaisno šāda veida informācijas publicēšanu par prasītāju, Tiesa secināja, ka publikācijas galvenais mērķis bija palielināt laikraksta pārdošanas apjomus, apmierinot lasītāju zinātkāri. Šāds mērķis nebija uzskatāms par ieguldījumu sabiedrības vispārējo interešu debatēs. Tā kā runa bija par "klaju preses brīvības ļaunprātīgu izmantošanu", valsts tiesību aktos paredzētie būtiskie ierobežojumi zaudējumu atlīdzināšanai un mazā morālā kaitējuma kompensācijas summa nozīmēja, ka Lietuva nebija izpildījusi savu pozitīvo pienākumu aizsargāt prasītājas tiesības uz privātās dzīves neaizskaramību. ECT atzina, ka šajā lietā ir pārkāpts ECTK 8. pants.

97 ECT 2008. gada 25. novembra spriedums lietā *Biriuk pret Lietuvu*, Nr. 23373/03.

Tiesības uz vārda brīvību un tiesības uz personas datu aizsardzību ne vienmēr ir pretrunā. Ir gadījumi, kad efektīva personas datu aizsardzība garantē vārda brīvību.

> Piemērs. Lietā *Tele2 Sverige* EST norādīja, ka iejaukšanās Hartas 7. un 8. pantā paredzētajās pamattiesībās, ko rada Direktīva 2006/24/EK (Datu saglabāšanas direktīva), ir "plaša un uzskatāma par īpaši būtisku. Turklāt (..) apstāklis, ka datu saglabāšana un to vēlāka izmantošana notiek, abonentu vai reģistrēto lietotāju par to neinformējot, var (..) attiecīgajām personām radīt sajūtu, ka viņu privātā dzīve tiek pastāvīgi uzraudzīta". EST arī secināja, ka vispārīga datu plūsmas un atrašanās vietas datu saglabāšana varētu ietekmēt elektroniskās komunikācijas izmantošanu un "attiecīgi – lietotāju iespēju izmantot viņu vārda brīvību, kas garantēta Hartas 11. pantā"[98]. Šajā ziņā, nosakot pienākumu ieviest stingrus datu saglabāšanas aizsardzības pasākumus, kas netiek piemēroti vispārināti, datu aizsardzības noteikumi galu galā veicina vārda brīvības tiesību izmantošanu.

Attiecībā uz tiesībām saņemt informāciju, kas arī ir daļa no tiesībām uz vārda brīvību, arvien vairāk tiek apzināta valdības pārredzamības nozīme demokrātiskas sabiedrības funkcionēšanā. Pārredzamība ir vispārējas nozīmes mērķis, kas tādējādi var attaisnot iejaukšanos tiesībās uz datu aizsardzību, ja tā ir vajadzīga un samērīga, kā paskaidrots 1.2. iedaļā. Līdz ar to pēdējās divās desmitgadēs tiesības piekļūt publisko iestāžu rīcībā esošajiem dokumentiem ir atzītas par nozīmīgām katra ES pilsoņa un ikvienas fiziskas vai juridiskas personas, kuras dzīvesvieta vai juridiskā adrese ir kādā dalībvalstī, tiesībām.

Saskaņā ar EP tiesību aktiem ir iespējams atsaukties uz ieteikumā par piekļuvi oficiālajiem dokumentiem ietvertajiem principiem, kas iedvesmoja Konvencijas par piekļuvi oficiālajiem dokumentiem (Konvencija Nr. 205) izstrādātājus[99].

Saskaņā ar ES tiesību aktiem tiesības piekļūt dokumentiem ir garantētas Regulā (EK) Nr. 1049/2001 par publisku piekļuvi Eiropas Parlamenta, Padomes un Komisijas

98 EST 2016. gada 21. decembra spriedums apvienotajās lietās C-203/15 un C-698/15 *Tele2 Sverige AB pret Post- och telestyrelsen un Secretary of State for the Home Department pret Tom Watson un citiem* [GC], 37. un 101. punkts; EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C-293/12 un C-594/12 *Digital Rights Ireland Ltd pret Minister for Communications, Marine and Natural Resources un citiem un Kärntner Landesregierung un citiem* [GC], 28. punkts.

99 Eiropas Padomes Ministru komiteja (2002), Ieteikums R (81) 19 un Ieteikums Rec(2002)2 dalībvalstīm par piekļuvi oficiāliem dokumentiem, 2002. gada 21. februāris; Eiropas Padomes Konvencija par piekļuvi oficiāliem dokumentiem, *CETS* Nr. 205, 2009. gada 18. jūnijs. Konvencija vēl nav stājusies spēkā.

dokumentiem (Regula par piekļuvi dokumentiem)[100]. Hartas 42. pantā un LESD 15. panta 3. punktā šīs tiesības ir paplašinātas, ietverot piekļuvi "Savienības iestāžu, struktūru, biroju un aģentūru dokumentiem neatkarīgi no to veida".

Šīs tiesības var nonākt pretrunā tiesībām uz datu aizsardzību, ja piekļuve dokumentam atklāj citu personas datus. Vispārīgās datu aizsardzības regulas 86. pantā ir skaidri noteikts, ka personas datus, kas iekļauti oficiālos dokumentos, kuri ir publiskas iestādes vai struktūras rīcībā, drīkst atklāt saskaņā ar Savienības[101] vai dalībvalsts tiesību aktiem, lai publisku piekļuvi oficiāliem dokumentiem saskaņotu ar tiesībām uz personas datu aizsardzību saskaņā ar šo regulu.

Tāpēc pieprasījumi piekļuvei publisko iestāžu rīcībā esošiem dokumentiem vai informācijai ir jālīdzsvaro ar to personu tiesībām uz datu aizsardzību, kuru dati ietverti pieprasītajos dokumentos.

Piemērs. Lietā *Volker un Markus Schecke un Hartmut Eifert pret Land Hessen*[102] EST bija jāvērtē ES tiesību aktos noteiktās ES lauksaimniecības subsīdiju saņēmēju vārdu un saņemto summu publicēšanas prasības samērīgums. Publicēšanas mērķis bija uzlabot pārskatāmību un dot ieguldījumu sabiedrības kontrolē pār to, vai administrācija pareizi izmanto valsts līdzekļus. Vairāki saņēmēji apstrīdēja šīs publikācijas samērīgumu.

EST, atzīmējot, ka tiesības uz datu aizsardzību nav absolūtas, apgalvoja, ka datu publicēšana tīmekļa vietnē, kurā nosaukti divu ES lauksaimniecības atbalsta fondu saņēmēji un precīzas saņemtās summas, ir iejaukšanās viņu privātajā dzīvē kopumā un jo īpaši viņu personas datu aizsardzībā.

EST secināja, ka šāda iejaukšanās Hartas 7. un 8. pantā ir paredzēta tiesību aktos un tā atbilst ES atzītajam vispārējo interešu mērķim, proti, uzlabot Kopienas līdzekļu izlietojuma pārskatāmību. Tomēr EST uzskatīja, ka to fizisko personu vārdu un uzvārdu, kuri saņem ES lauksaimniecības atbalstu no šiem diviem fondiem, kā arī precīzu saņemto summu publicēšana ir nesamērīgs pasākums un nav pamatots, ņemot vērā Hartas 52. panta 1. punktu. Tiesa atzina, ka demokrātiskā sabiedrībā ir būtiski informēt nodokļu maksātājus

100 Eiropas Parlamenta un Padomes 2001 gada 30. maija Regula (EK) Nr. 1049/2001 par publisku piekļuvi Eiropas Parlamenta, Padomes un Komisijas dokumentiem, OV 2001 L 145.

101 Hartas 42. pants, LESD 15. panta 3. punkts un Regula Nr. 1049/2009.

102 EST 2010. gada 9. novembra spriedums apvienotajās lietas C-92/09 un C-93/09 *Volker und Markus Schecke GbR un Hartmut Eifert pret Land Hessen* [GC], 47.–52., 58., 66–67., 75., 86. un 92. punkts.

par valsts līdzekļu izlietojumu. Tomēr, tā kā nevar uzskatīt, ka "pārskatāmības mērķis vispārīgi prevalē pār tiesībām uz personas datu aizsardzību"[103], ES iestādēm bija pienākums līdzsvarot Savienības intereses nodrošināt pārredzamību ar ierobežojumu attiecībā uz privātuma un datu aizsardzības tiesību izmantošanu, kas tika piemērots šiem atbalsta saņēmējiem publikācijas rezultātā.

EST uzskatīja, ka ES iestādes nav pareizi veikušas šo izsvēršanas uzdevumu, jo bija iespējams paredzēt pasākumus ar mazāk nelabvēlīgu ietekmi uz personu pamattiesībām, vienlaikus efektīvi veicinot publicēšanas rezultātā sasniedzamo pārredzamības mērķi. Piemēram, tā vietā, lai publicētu vispārēju informāciju, kas attiecas uz visiem saņēmējiem, norādot viņu vārdu un katra saņemto precīzo summu, ir iespējams nošķirt tos atbilstoši tādiem pienācīgiem kritērijiem kā laikposmi, kuros viņi ir saņēmuši šādu atbalstu, tā biežums vai apmērs un raksturs[104]. Tādējādi EST daļēji atzina par spēkā neesošiem ES tiesību aktus par informācijas publicēšanu attiecībā uz Eiropas lauksaimniecības fondu saņēmējiem.

Piemērs. Lietā *Rechnungshof pret Österreichischer Rundfunk un citi*[105] EST aplūkoja noteiktu Austrijas tiesību aktu saderību ar ES tiesību aktiem datu aizsardzības jomā. Tiesību aktos bija prasība valsts iestādēm apkopot un pārsūtīt datus par ienākumiem, lai publicētu plašākai sabiedrībai pieejamā gada pārskatā dažādu valsts iestāžu darbinieku vārdus un ienākumus. Dažas personas atteicās sniegt savus datus, pamatojoties uz datu aizsardzības noteikumiem.

Savā atzinumā EST balstījās uz pamattiesību aizsardzību kā uz vispārēju ES tiesību principu un uz ECTK 8. pantu, atgādinot, ka Harta tajā laikā nebija saistoša. Tā nosprieda, ka datu vākšana par personas profesionālā darbībā gūtajiem ienākumiem un jo īpaši to nodošana trešajām personām ietilpst tiesību uz privātās dzīves neaizskaramību piemērošanas jomā un ir šo tiesību pārkāpums. Iejaukšanos varētu attaisnot, ja tā būtu notikusi saskaņā ar tiesību aktiem, tai būtu likumīgs mērķis un ja tā būtu bijusi nepieciešama demokrātiskā sabiedrībā. EST atzīmēja, ka Austrijas tiesību aktiem ir likumīgs

103 Turpat, 85. punkts.

104 Turpat, 89. punkts.

105 EST 2003. gada 20. maija spriedums apvienotajās lietās C-465/00, C-138/01 un C-139/09 *Rechnungshof pret Österreichischer Rundfunk un citiem* un *Christa Neukomm un Jospeh Lauermann pret Österreichischer Rundfunk*.

mērķis, t. i., noturēt valsts pārvaldes darbinieku algas saprātīgās robežās – šis apsvērums ir saistīts arī ar valsts ekonomisko labklājību. Tomēr Austrijas interese par vislabāko publisko līdzekļu izlietojumu bija jāsamēro ar iejaukšanās attiecīgo personu tiesībām uz privātās dzīves neaizskaramību nopietnību.

Lai gan valsts tiesai bija jāpārbauda, vai datu par personu ienākumiem publicēšana bija nepieciešama un samērīga ar tiesību aktos noteikto mērķi, EST aicināja valsts tiesu pārbaudīt, vai šādu mērķi nevarēja sasniegt vienādi efektīvi, izmantojot mazāk aizskarošus līdzekļus. Kā piemēru var minēt personas datu pārsūtīšanu tikai uzraugošām publiskām struktūrām, nevis plašākai sabiedrībai.

Tālāk kļuva skaidrs, ka izsvēršanai starp datu aizsardzību un piekļuvi dokumentiem ir nepieciešama izvērsta analīze katrā atsevišķā gadījumā. Neviena no tiesībām nevar automātiski būt svarīgāka par citu. EST bija iespēja divās lietās interpretēt tiesības piekļūt dokumentiem, kas satur personas datus.

Piemērs. Lietā *Eiropas Komisija pret Bavarian Lager*[106] EST definēja personas datu aizsardzības tvērumu saistībā ar piekļuvi ES iestāžu dokumentiem un attiecībām starp Regulu (EK) Nr. 1049/2001 (Regulu par piekļuvi dokumentiem) un Regulu (EK) Nr. 45/2001 (ES iestāžu datu aizsardzības regulu). Uzņēmums *Bavarian Lager*, ko nodibināja 1992. gadā, importē pudelēs pildītu vācu alu Apvienotajā Karalistē, galvenokārt sabiedriskajām iestādēm un bāriem. Tomēr uzņēmums sastapās ar grūtībām, jo Lielbritānijas tiesību akti *de facto* deva priekšroku vietējiem ražotājiem. Atbildot uz *Bavarian Lager* sūdzību, Eiropas Komisija uzsāka tiesvedību pret Apvienoto Karalisti par saistību neizpildi, tādēļ Apvienotā Karaliste grozīja apstrīdētos noteikumus un pielāgoja tos ES tiesību aktiem. Pēc tam *Bavarian Lager* lūdza Komisijai papildus citiem dokumentiem izsniegt tās sanāksmes protokola kopiju, kurā piedalījās Komisijas, Lielbritānijas iestāžu un *Confédération des Brasseurs du Marché Commun* (*CBMC*) pārstāvji. Komisija piekrita atklāt dažus dokumentus, kas attiecās uz sanāksmi, taču aizklāja piecus protokolā norādītos vārdus – divas personas bija nepārprotami iebildušas pret to identitātes izpaušanu, savukārt Komisija nebija varējusi sazināties ar trim pārējām personām. Savā 2004. gada 18. marta lēmumā Komisija noraidīja

106 EST 2010. gada 29. jūnija spriedums lietā C-28/08 P *Eiropas Komisija pret The Bavarian Lager Co. Ltd* [GC].

jaunu *Bavarian Lager* pieteikumu saņemt pilnu sanāksmes protokolu, jo īpaši atsaucoties uz šo personu privātās dzīves aizsardzību, ko garantē ES iestāžu datu aizsardzības regula.

Tā kā *Bavarian Lager* nebija apmierināts ar šo nostāju, uzņēmums cēla prasību Vispārējā tiesā. Šī tiesa ar 2007. gada 8. novembra spriedumu (lieta T-194/04, *The Bavarian Lager Co. Ltd pret Eiropas Kopienu Komisiju*) atcēla Komisijas lēmumu, uzskatot, ka attiecīgo personu vārdu ierakstīšana to personu sarakstā, kuras piedalās sanāksmēs tās pārstāvētās struktūras vārdā, nav privātās dzīves aizskārums un tā neapdraudēja šo personu privāto dzīvi.

Komisija iesniedza apelācijas sūdzību, un EST atcēla Pirmās instances tiesas spriedumu. EST sprieda, ka Regulā par piekļuvi dokumentiem noteikts "īpašs un pastiprināts regulējums attiecībā uz tādas personas aizsardzību, kuras personas dati attiecīgajā gadījumā varētu tikt izpausti sabiedrībai". Atbilstoši EST paustajam, ja ar pieprasījumu, kas balstīts uz Regulu par piekļuvi dokumentiem, tiecas panākt piekļuvi dokumentiem, kas ietver personas datus, ES iestāžu datu aizsardzības regulas noteikumus piemēro pilnībā. Tālāk EST secināja, ka Komisija pamatoti noraidījusi pieteikumu nodrošināt piekļuvi pilnam 1996. gada oktobra sanāksmes protokolam. Tā kā nebija piecu šīs sanāksmes dalībnieku piekrišanas, Komisija pietiekamā apmērā izpildīja savu atklātības nodrošināšanas pienākumu, izsniedzot attiecīgā dokumenta versiju bez šo personu vārdiem.

Turklāt atbilstoši EST teiktajam, "tā kā *Bavarian Lager* nesniedza nedz skaidru un likumīgu pamatojumu, nedz pārliecinošus argumentus, lai pierādītu vajadzību nosūtīt šos personas datus, Komisija nevarēja izsvērt dažādās lietas dalībnieku intereses. Tāpat tā nevarēja pārbaudīt, vai nav pamata pieņemt, ka ar šo nosūtīšanu varētu tikt ierobežotas datu subjektu likumīgās intereses", kā to prasa ES institūciju datu aizsardzības regula.

Piemērs. Lietā *Client Earth un PAN Europe pret EFSA*[107] EST pārbaudīja, vai Eiropas Pārtikas un nekaitīguma iestādes (*EFSA*) lēmums atteikt prasītājiem pilnīgu piekļuvi dokumentiem bija nepieciešams, lai aizsargātu dokumentos minēto personu privātumu un datu aizsardzības tiesības. Šie dokumenti attiecās uz vadlīniju ziņojuma projektu, ko *EFSA* darba grupa sadarbībā ar

107 EST 2015. gada 16. jūlija spriedums lietā C-615/13P *ClientEarth, Pesticide Action Network Europe (PAN Europe) pret Eiropas Pārtikas nekaitīguma iestādi (EFSA), Eiropas Komisiju*.

ārējiem ekspertiem bija sagatavojusi par augu aizsardzības līdzekļu laišanu tirgū. Sākotnēji *EFSA* piešķīra prasītājiem daļēju piekļuvi, liedzot pieeju dažām vadlīniju dokumenta projekta darba versijām. Pēc tam tā piešķīra piekļuvi versijas projektam, kurā bija iekļautas ārējo ekspertu individuālās piezīmes. Tomēr tā izņēma ekspertu vārdus, atsaucoties uz Regulas (EK) Nr. 45/2001 par personas datu apstrādi ES iestādēs un struktūrās 4. panta 1. punkta b) apakšpunktu un nepieciešamību aizsargāt ārējo ekspertu privātumu. Pirmajā instancē ES Vispārējā tiesa atstāja spēkā *EFSA* lēmumu.

Prasītāji iesniedza apelācijas sūdzību, un EST atcēla pirmās instances spriedumu. Tiesa secināja, ka personas datu nodošana šajā gadījumā bija nepieciešama, lai pārliecinātos par katra ārējā eksperta objektivitāti, pildot zinātnieku funkcijas, un nodrošinātu, ka lēmumu pieņemšanas process *EFSA* joprojām ir pārredzams. EST uzskatīja, ka *EFSA* nav precizējusi, kā to ārējo ekspertu vārdu atklāšana, kuri bija iesnieguši īpašas piezīmes par vadlīniju dokumenta projektu, kaitētu ekspertu likumīgajām interesēm. Vispārējs arguments, ka informācijas izpaušana var kaitēt privātumam, nav pietiekams, ja to nepamato ar uz konkrēto gadījumu attiecināmiem pierādījumiem.

Atbilstoši šiem spriedumiem tiesību uz datu aizsardzību aizskārumam saistībā ar piekļuvi dokumentiem ir nepieciešams īpašs un pamatots iemesls. Tiesības uz piekļuvi dokumentiem nevar automātiski atcelt tiesības uz datu aizsardzību[108].

Šī pieeja ir līdzīga ECT pieejai attiecībā uz privātumu un piekļuvi dokumentiem, kas izriet arī no turpmāk aplūkotā sprieduma. Spriedumā lietā *Magyar Helsinki* ECT paziņoja, ka 10. pants nepiešķir indivīdiem tiesības piekļūt valsts iestādes rīcībā esošajai informācijai un neuzliek par pienākumu valdībai sniegt indivīdam šādu informāciju. Tomēr šādas tiesības vai pienākums varētu rasties, pirmkārt, ja informācijas izpaušanas pienākumu uzliek ar tiesas lēmumu, kas ir stājies spēkā; otrkārt, ja piekļuve informācijai ir būtiska, lai indivīds varētu īstenot savas tiesības uz vārda brīvību – jo īpaši brīvību saņemt un izplatīt informāciju, kā arī, ja tās liegšana varētu ietekmēt šīs tiesības[109]. Tas, vai un kādā mērā atteikums sniegt piekļuvi ir iejaukšanās prasītāja tiesībās uz vārda brīvību, ir jāvērtē katrā atsevišķā gadījumā, ņemot vērā tā

108 Skatīt tomēr EDAU detalizētās apspriedes (2011), *Publiska piekļuve dokumentiem, kas satur personas datus pēc nolēmuma lietā* Bavarian Lager, Brisele, 2011. gada 24. marts.

109 ECT 2016. gada 8. novembra spriedums lietā *Magyar Helsinki Bizottság pret Ungāriju* [GC], Nr. 18030/11, 148. punkts.

īpašos apstākļus, tostarp: i) informācijas pieprasījuma mērķi; ii) meklētās informācijas veidu; iii) prasītāja funkciju; un iv) vai informācija bija gatava un pieejama.

Piemērs. Lietā *Magyar Helsinki Bizottság pret Ungāriju*[110] prasītājs, kas ir cilvēktiesību NVO, policijai pieprasīja informāciju par *ex officio* valsts nodrošinātu aizstāvju darbu, lai pabeigtu pētījumu par valsts nodrošinātu aizstāvju sistēmas darbību Ungārijā. Policija atteicās sniegt informāciju, apgalvojot, ka tie ir personas dati, kas nav izpaužami. Piemērojot iepriekš minētos kritērijus, ECT uzskatīja, ka ir notikusi iejaukšanās tiesībās, ko aizsargā 10. pants. Precīzāk, prasītājs vēlēdamies izmantot tiesības sniegt informāciju par sabiedrībai svarīgu jautājumu, bija meklējis piekļuvi informācijai, turklāt šī informācija bija nepieciešama, lai īstenotu prasītāja vārda brīvības tiesības. Informācija par valsts nodrošinātu aizstāvju iecelšanu ir sabiedrības interesēs. Nebija pamata apšaubīt, ka attiecīgā aptauja saturēja informāciju, kuru prasītājs apņēmās darīt zināmu sabiedrībai un kuru sabiedrībai bija tiesības saņemt. Tādējādi Tiesa uzskatīja, ka piekļuve pieprasītajai informācijai prasītājam bija nepieciešama uzdevuma izpildei. Visbeidzot: informācija bija gatava un pieejama.

ECT secināja, ka atteikums nodrošināt piekļuvi informācijai šajā gadījumā ir kaitējis informācijas saņemšanas brīvības saturam. Izdarot šo secinājumu, tiesa jo īpaši pārbaudīja pieprasītās informācijas mērķi un tās ieguldījumu svarīgās sabiedriskajās debatēs, pieprasītās informācijas raksturu un to, vai tai ir sabiedrības interese, kā arī prasītāja funkciju sabiedrībā.

Savā argumentācijā Tiesa atzīmēja, ka NVO veiktais pētījums attiecās uz tiesu sistēmas darbību un tiesībām uz aizstāvību, kam saskaņā ar ECTK ir ārkārtīgi svarīga nozīme. Tā kā pieprasītajā informācijā nebija ietverti dati ārpus vispārpieejamā, attiecīgo datu subjektu (*ex officio* valsts nodrošinātu aizstāvju) tiesības uz privātumu nebūtu apdraudētas, ja policija prasītājam nodrošinātu piekļuvi šai informācijai. Prasītāja pieprasītajai informācijai bija statistikas raksturs, kas attiecās uz to reižu skaitu, kad *ex officio* aizstāvis tika nozīmēts pārstāvēt atbildētājus publiskā kriminālprocesā.

Tiesai, ņemot vērā to, ka pētījuma mērķis bija veicināt svarīgas debates par vispārējas nozīmes jautājumu, jebkādi ierobežojumi attiecībā uz NVO ierosināto publikāciju ir rūpīgi jāpārbauda. Aplūkojamā informācija bija sabiedrības interesēs, jo sabiedrības intereses aptver "jautājumus, kas var izraisīt

110 Turpat, 181., 187.–200. punkts.

ievērojamas pretrunas, kuri skar svarīgu sociālo jautājumu vai ir saistīti ar problēmu, par kuru sabiedrībai būtu jābūt informētai"[111]. Tādējādi šeit noteikti ietilptu diskusija par taisnīgumu un taisnīgu tiesu, kas bija prasītāja pētījuma priekšmets. Izsverot dažādās iesaistītās tiesības un piemērojot proporcionalitātes principu, ECT uzskatīja, ka ir nepamatoti pārkāptas prasītāja ECTK 10. pantā noteiktās tiesības.

1.3.2. Dienesta noslēpums

Saskaņā ar valsts tiesību aktiem uz noteiktu komunikāciju var attiekties dienesta noslēpuma glabāšanas pienākums. Dienesta noslēpumu var saprast kā īpašu ētisku pienākumu, kas uzliek noteiktām profesijām un funkcijām, kuras balstītas uz ticību un uzticību, raksturīgu juridisko pienākumu. Personām un institūcijām, kuras pilda šīs funkcijas, ir pienākums neizpaust konfidenciālu informāciju, ko tās saņēmušas, veicot savus pienākumus. Dienesta noslēpums jo īpaši attiecas uz mediķiem un jurista-klienta klusēšanas pienākumu, daudzās jurisdikcijās atzīstot arī dienesta noslēpuma glabāšanas pienākumu finanšu nozarē. Dienesta noslēpums nav pamattiesības, bet tiek aizsargāts kā tiesības uz privātās dzīves neaizskaramību. Piemēram, EST ir lēmusi, ka dažos gadījumos "var būt nepieciešams aizliegt izpaust noteiktu informāciju, kas ir kvalificēta kā konfidenciāla, lai aizsargātu uzņēmuma pamattiesības uz privāto dzīvi, kas ir aizsargātas ECTK 8. pantā un Hartas 7. pantā"[112]. ECT ir arī lūgta lemt par to, vai dienesta noslēpuma ierobežojumi ir ECTK 8. panta pārkāpums, kā parādīts izceltajos piemēros.

Piemērs. Lietā *Pruteanu pret Rumāniju*[113] prasītājs bija jurists komercsabiedrībā, kurai bija liegts veikt bankas darījumus, balstoties uz aizdomām par krāpšanu. Lietas izmeklēšanas gaitā Rumānijas tiesas pilnvaroja prokuratūras iestādes noteiktā laika posmā pārtvert un ierakstīt uzņēmuma partnera telefonsarunas. Ierakstos un pārtvertajās sarunās ietilpa viņa saziņa ar juristu.

Pruteanu kungs apgalvoja, ka tādējādi ir aizskartas viņa tiesības uz privātās dzīves un korespondences neaizskaramību. ECT savā spriedumā uzsvēra jurista attiecību ar viņa klientu statusu un nozīmi. Jurista sarunu ar viņu klientu pārtveršana, bez šaubām, ir dienesta noslēpuma, kas bija šo divu

111 Turpat, 156. punkts.

112 EST 2013. gada 11. marta spriedums lietā T-462/12 R *Pilkington Group Ltd pret Eiropas Komisiju*, Vispārējās tiesas priekšsēdētāja rīkojums, 44. punkts.

113 ECT 2015. gada 3. februāra spriedums lietā *Pruteanu pret Rumāniju*, Nr. 30181/05.

cilvēku attiecību pamatā, aizskārums. Šādā gadījumā jurists varēja sūdzēties arī par iejaukšanos viņa tiesībās uz privātās dzīves un korespondences neaizskaramību. EST ir atzinusi, ka šajā lietā ir pārkāpts ECTK 8. pants.

Piemērs. Lietā *Brito Ferrinho Bexiga Villa-Nova pret Portugāli*[114] prasītāja, juriste, atteicās uzrādīt nodokļu iestādēm savus personīgos bankas izrakstus, pamatojoties uz dienesta un bankas noslēpumu. Prokuratūra uzsāka izmeklēšanu saistībā ar krāpšanu nodokļu jomā un lūdza apturēt dienesta noslēpuma pilnvaras. Valsts tiesas lika apturēt dienesta un banku noslēpuma noteikumus, uzskatot, ka sabiedrības intereses ir svarīgākas pār prasītājas privātajām interesēm.

Kad lieta nonāca ECT, tiesa nosprieda, ka piekļūšana prasītājas bankas izrakstiem bija iejaukšanās viņas tiesībās ievērot dienesta noslēpumu, kas ietilpst privātās dzīves tvērumā. Aizskārumam bija juridisks pamats, balstoties uz kriminālprocesa kodeksu, un tam bija likumīgs mērķis. Tomēr, pārbaudot aizskāruma nepieciešamību un samērīgumu, ECT norādīja uz faktu, ka procedūras par dienesta noslēpuma atcelšanu tika veiktas bez prasītājas dalības un neinformējot viņu. Tādējādi prasītāja nevarēja iesniegt savus argumentus. Turklāt, kaut arī valsts tiesību akti paredzēja, ka šādā tiesvedībā ir jākonsultējas ar juristu asociāciju, šādas konsultācijas nav notikušas. Visbeidzot, prasītājai nebija iespējas efektīvi apstrīdēt dienesta noslēpuma atcelšanu un tiesiskās aizsardzības līdzekli, ar kura palīdzību varētu apstrīdēt šo pasākumu. Tā kā trūkst procesuālo garantiju un efektīvas tiesas kontroles attiecībā uz pasākumu, ar kuru tiek apturēts konfidencialitātes pienākums, ECT secināja, ka ECTK 8. pants ir pārkāpts.

Dienesta noslēpuma un datu aizsardzības mijiedarbība nereti ir pretrunīga. No vienas puses, datu aizsardzības noteikumi un tiesību aktos noteiktie aizsardzības pasākumi palīdz nodrošināt dienesta noslēpuma ievērošanu. Piemēram, noteikumi, kas pārziņiem un apstrādātājiem pieprasa ieviest stingrus datu drošības pasākumus, cita starpā paredzēti, lai novērstu ar dienesta noslēpumu aizsargāto personas datu konfidencialitātes zaudēšanu. Turklāt ES Vispārīgā datu aizsardzības regula ļauj apstrādāt veselības datus, kas ietilpst īpašo personas datu kategorijās, kurām nepieciešama

114 ECT 2015. gada 1. decembra spriedums lietā *Brito Ferrinho Bexiga Villa-Nova pret Portugāli*, Nr. 69436/10.

stingrāka aizsardzība, bet uzliek pienākumu tiem piemērot atbilstošus un konkrētus pasākumus, lai aizsargātu datu subjektu tiesības, jo īpaši dienesta noslēpumu[115].

No otras puses, pārziņiem un apstrādātājiem uzliktie dienesta noslēpuma glabāšanas pienākumi attiecībā uz noteiktiem personas datiem var ierobežot datu subjektu tiesības, jo īpaši tiesības saņemt informāciju. Kaut arī Vispārīgajā datu aizsardzības regulā ir plašs saraksts ar informāciju, kas principā ir jāsniedz datu subjektam, ja personas dati nav iegūti no viņa, šī prasība izpaust informāciju neattiecas uz gadījumiem, kad personas datiem jāpaliek konfidenciāliem dienesta noslēpuma glabāšanas pienākuma dēļ, kas noteikts valsts vai ES tiesību aktos[116].

Vispārīgajā datu aizsardzības regulā (VDAR) ir paredzēta iespēja dalībvalstīm tiesību aktos pieņemt īpašus noteikumus, lai aizsargātu dienesta noslēpumu vai citus pielīdzināmus slepenības pienākumus un līdzsvarotu tiesības uz personas datu aizsardzību ar dienesta noslēpumu[117].

Ar VDAR paredz, ka dalībvalstis var pieņemt īpašus noteikumus par uzraudzības iestāžu pilnvarām attiecībā uz pārziņiem vai apstrādātājiem, uz kuriem attiecas dienesta noslēpuma glabāšanas pienākums. Šie īpašie noteikumi attiecas uz tiesībām piekļuvei pārziņa vai apstrādātāja telpām, tā datu apstrādes iekārtām un turētajiem personas datiem, ja šādi personas dati ir saņemti tādas darbības gaitā, uz kuru attiecas konfidencialitātes pienākums. Tādējādi uzraudzības iestādēm, kam uzticēta datu aizsardzība, jāievēro dienesta noslēpuma glabāšanas pienākumi, kuri ir saistoši pārziņiem un apstrādātājiem. Turklāt uz pašiem uzraudzības iestāžu locekļiem attiecas dienesta noslēpums arī viņu pilnvaru laikā un pēc tā beigām. Pildot savus uzdevumus, uzraudzības iestāžu locekļi un darbinieki var iegūt konfidenciālu informāciju. Regulas 54. panta 2. punkts skaidri nosaka, ka viņiem ir pienākums glabāt dienesta noslēpumu attiecībā uz šādu konfidenciālu informāciju.

VDAR ir prasība dalībvalstīm informēt Komisiju par noteikumiem, ko tās pieņem, lai saskaņotu datu aizsardzību un regulā noteiktos principus ar dienesta noslēpuma glabāšanas pienākumu.

115 Vispārīgā datu aizsardzības regula, 9. panta 2. punkta h) apakšpunkts un 9. panta 3. punkts.

116 Turpat, 14. panta 5. punkta d) apakšpunkts.

117 Turpat, 164. apsvērums un 90. pants.

1.3.3. Reliģijas un ticības brīvība

Reliģijas un ticības brīvību aizsargā ECTK 9. pants (domas, apziņas un reliģijas brīvība) un ES Pamattiesību hartas 10. pants. Personas dati, kas atklāj reliģisko vai filozofisko pārliecību, tiek uzskatīti par "sensitīviem datiem" gan ES, gan Eiropas Padomes tiesību aktos, to apstrāde un izmantošana ir īpaši aizsargāta.

Piemērs. Prasītājs lietā *Sinak Isik pret Turciju*[118] bija alevītu reliģiskās kopienas loceklis, kuras uzskatus ietekmē sūfisms un citi pirmsislāma perioda uzskati. Daži zinātnieki to uzskata par atsevišķu reliģiju, savukārt citi par islāma reliģijas sastāvdaļu. Prasītājs sūdzējās, ka pret viņa vēlmēm personas apliecībā bija ailīte, kurā kā viņa reliģija norādīts "islāms", nevis "alēvisms". Valsts tiesas noraidīja viņa lūgumu mainīt ierakstu personas apliecībā uz "alēvismu", pamatojoties uz to, ka šis vārds apzīmē islāma apakšgrupu, nevis atsevišķu reliģiju. Tālāk prasītājs iesniedza sūdzību ECT par to, ka viņam bija pienākums izpaust viņa ticību bez viņa piekrišanas, jo personas apliecībā obligāti jānorāda personas reliģiskā piederība un tas pārkāpj viņa tiesības uz reliģijas un sirdsapziņas brīvību, jo īpaši ņemot vērā to, ka personas apliecībā ierakstītais apzīmējums "islāms" bija nepareizs.

ECT atkārtoti uzsvēra, ka reliģijas brīvība nozīmē brīvību paust personas reliģisko pārliecību kopienā ar citiem, publiski un tādu personu lokā, kuri pieder tādai pašai ticībai, kā arī vienatnē un privāti. Tajā laikā spēkā esošie valsts tiesību akti uzliek personām par pienākumu nēsāt personu apliecinošu dokumentu – dokumentu, kas jāuzrāda pēc jebkuras publiskas iestādes vai privāta uzņēmuma pieprasījuma, šis dokuments norāda viņu reliģisko piederību. Šāds pienākums bija pretrunā tam, ka tiesības paust savu reliģisko pārliecību piešķir arī pretējās tiesības, t. i., tiesības neatklāt savu pārliecību. Kaut arī valdība iebilda, ka valsts tiesību akti ir grozīti, lai personas varētu pieprasīt reliģijas ailīti personas apliecībās atstāt tukšu, pēc Tiesas domām, fakts, ka ir jāpieprasa informācijas par reliģiskās pārliecības dzēšana, varētu būt informācijas atklāšana par attieksmi pret reliģiju. Turklāt, ja personas apliecībās ir ailīte par reliģiju, atstājot to tukšu, tai tiek piešķirta īpaša nozīme, jo personas apliecības turētāji bez informācijas par reliģisko piederību izceltos attiecībā pret tiem, kuru apliecībās viņu pārliecība ir norādīta. ECT atzina, ka valsts tiesību akti pārkāpj ECTK 9. pantu.

118 ECT 2010. gada 2. februāra spriedums lietā *Sinan Işık pret Turciju*, Nr. 21924/05.

Baznīcu un reliģisko apvienību vai kopienu darbībai tomēr var būt nepieciešama biedru personiskās informācijas apstrāde, lai nodrošinātu draudzē saziņu un darbību organizēšanu. Tādēļ baznīcas un reliģiskās apvienības nereti ir ieviesušas noteikumus par personas datu apstrādi. Atbilstoši Vispārīgās datu aizsardzības regulas 91. pantam, ja šādi noteikumi ir visaptveroši, tie var būt spēkā arī turpmāk, ja ir saskaņoti ar šīs regulas noteikumiem. Baznīcām un reliģiskām apvienībām, kurām ir šādi noteikumi, jābūt pakļautām neatkarīgai uzraudzības iestādei, kas varētu būt īpaši tām paredzēta, ar nosacījumu, ka tās izpilda Vispārīgās datu aizsardzības regulas prasības šādām iestādēm[119].

Reliģiskās organizācijas var veikt personas datu apstrādi vairāku iemeslu dēļ – piemēram, lai uzturētu kontaktus ar savu draudzi vai sniegtu informāciju par organizētajiem reliģiskajiem vai labdarības pasākumiem un svētkiem. Dažās valstīs baznīcām nodokļu vajadzībām ir jāuztur savu biedru reģistri, jo dalība reliģiskajās iestādēs var ietekmēt privātpersonu maksājamo nodokļu apmēru. Jebkurā gadījumā saskaņā ar Eiropas tiesību aktiem dati, kas atklāj reliģisko pārliecību, ir sensitīvi, baznīcām ir jāatbild par darbībām ar šiem datiem un to apstrādi, jo īpaši tāpēc, ka reliģisko organizāciju apstrādātā informācija bieži attiecas uz bērniem, vecāka gadagājuma cilvēkiem vai citiem neaizsargātiem sabiedrības locekļiem.

1.3.4. Humanitāro un eksakto zinātņu brīvība

Vēl vienas tiesības, kas jālīdzsvaro ar tiesībām uz privātās dzīves neaizskaramību un datu aizsardzību, ir humanitāro un eksakto zinātņu brīvība, ko nepārprotami aizsargā ES Pamattiesību hartas 13. pants. Šīs tiesības galvenokārt izriet no tiesībām uz domas un vārda brīvību, tās jāīsteno, ņemot vērā Hartas 1. pantu (cilvēka cieņa). ECT uzskata, ka humanitāro zinātņu brīvību aizsargā ECTK 10. pants[120]. Uz tiesībām, ko garantē Hartas 13. pants, var attiekties arī ierobežojumi saskaņā ar Hartas 52. panta 1. punktu, ko var arī interpretēt, izmantojot ECTK 10. panta 2. punktu[121].

Piemērs. Lietā *Vereinigung bildender Künstler pret Austriju*[122] Austrijas tiesas aizliedza prasītājai apvienībai turpināt eksponēt gleznu, kurā bija fotogrāfijas ar dažādu publisku personu galvām seksuālās pozās. Austrijas parlamenta

119 Vispārīgā datu aizsardzības regula, 91. panta 2. punkts.

120 ECT 1988. gada 24. maija spriedums lietā *Müller un citi pret Šveici*, Nr. 10737/84.

121 Paskaidrojumi attiecībā uz Pamattiesību hartu, OV 2007 C 303.

122 ECT 2007. gada 25. janvāra spriedums lietā *Vereinigung bildender Künstler pret Austriju*, Nr. 68345/01, 26. un 34. punkts.

deputāts, kura fotoattēls tika izmantots gleznā, cēla prasību pret prasītāju apvienību, lūdzot izdot rīkojumu, ar ko aizliegtu gleznu izstādīt. Valsts tiesa izdeva rīkojumu par aizliegumu. ECT atkārtoti uzsvēra, ka ECTK 10. pants attiecas arī uz tādu ideju paušanu, kas aizvaino, šokē vai traucē valstij vai jebkurai iedzīvotāju daļai. Personas, kuras rada, izrāda, izplata vai izstāda mākslas darbus, veicina ideju un viedokļu apmaiņu, un valstij ir pienākums pārmērīgi neiejaukties viņu vārda brīvībā. Tā kā glezna bija kolāža un tajā tika izmantotas tikai personu galvu fotogrāfijas, savukārt viņu ķermeņi tika atainoti nereāli, pārspīlēti, tad acīmredzami mērķis nebija atspoguļot vai pat sniegt norādes uz realitāti. ECT tālāk norādīja, ka "gleznu diez vai varēja saprast, lai norādītu uz [attēlotās personas] privātās dzīves detaļām, bet drīzāk bija saistītas ar viņa publisko stāvokli kā politiķim" un to, ka "šajā amatā [attēlotajai personai] vajadzētu būt iecietīgākam pret kritiku". Izsverot dažādās iesaistītās intereses, ECT secināja, ka neierobežots aizliegums turpināt izstādīt gleznu bija nesamērīgs. Tiesa secināja, ka ir pārkāpts ECTK 10. pants.

Arī Eiropas tiesību aktos datu aizsardzības jomā atzīta zinātnes īpašā nozīme sabiedrībā. Saskaņā ar Vispārīgo datu aizsardzības regulu un modernizēto Konvenciju Nr. 108 datus ļauts saglabāt ilgāk ar nosacījumu, ka personas dati tiks apstrādāti vienīgi zinātniskās vai vēstures pētniecības nolūkos. Turklāt neatkarīgi no konkrētās apstrādes darbības sākotnējā mērķa turpmāku personas datu izmantošanu zinātniskiem pētījumiem neuzskata par nesaderīgu nolūku[123]. Tajā pašā laikā jāievieš šādai apstrādei piemēroti drošības pasākumi, lai aizsargātu datu subjektu tiesības un brīvības. ES vai dalībvalsts tiesību aktos var būt paredzētas atkāpes no datu subjekta tiesībām, piemēram, tiesībām piekļūt datiem, labot tos, ierobežot datu apstrādi un iebilst pret to, ja viņu personas dati tiek apstrādāti zinātniskās pētniecības, vēstures vai statistikas nolūkos (skatīt arī 6.1. iedaļu un 9.4. iedaļu).

1.3.5. Intelektuālā īpašuma aizsardzība

Tiesības uz īpašuma aizsardzību ir nostiprinātas ECTK Pirmā protokola 1. pantā, kā arī ES Pamattiesību hartas 17. panta 1. punktā. Viens svarīgs īpašumtiesību aspekts, kas jo īpaši attiecas uz datu aizsardzību, ir intelektuālā īpašuma aizsardzība, kas skaidri minēta Hartas 17. panta 2. punktā. Vairāku ES tiesību sistēmas direktīvu mērķis ir nodrošināt efektīvu intelektuālā īpašuma, jo īpaši autortiesību, aizsardzību. Intelektuālais īpašums ietver ne tikai literāro un mākslinieciskо īpašumu, bet arī patentus, preču zīmes un saistītās tiesības.

123 Vispārīgā datu aizsardzības regula, 5. panta 1. punkta b) apakšpunkts un modernizētā Konvencija Nr. 108, 5. panta 4. punkta b) apakšpunkts.

Kā skaidri noteikts EST judikatūrā, īpašuma pamattiesību aizsardzībai jābūt līdzsvarotai ar citu pamattiesību aizsardzību, jo īpaši tiesībām uz datu aizsardzību[124]. Ir bijuši gadījumi, kad autortiesību aizsardzības institūcijas pieprasījušas, lai interneta piekļuves sniedzēji atklātu interneta datņu koplietošanas platformu lietotāju identitāti. Šādas platformas interneta lietotājiem bieži ļauj mūzikas darbus lejupielādēt bez maksas, lai gan minētie darbi ir aizsargāti ar autortiesībām.

Piemērs. Lieta *Promusicae pret Telefónica de España*[125] attiecās uz Spānijas interneta piekļuves sniedzēja *Telefónica* atteikumu atklāt *Promusicae* – bezpeļņas asociācijai, kas apvieno mūzikas ierakstu, audiovizuālo ierakstu producentus un izdevējus, – atsevišķu personu, kam tā sniedza pakalpojumus piekļuvei internetam, personas datus. *Promusicae* lūdza sniegt minēto informāciju, lai varētu uzsākt civilprocesu pret attiecīgajām personām, kuras, kā apgalvoja *Promusicae*, izmanto arhīvu apmaiņas programmu, kas ļauj piekļūt fonogrammām, kuru izmantošanas tiesības ir *Promusicae* biedriem.

Spānijas tiesa lūdza EST sniegt prejudiciālu nolēmumu, jautājot, vai tādi personas dati ir jāpaziņo civilprocesā saskaņā ar Kopienas tiesību aktiem, lai nodrošinātu autortiesību efektīvu aizsardzību. Tā atsaucās uz Direktīvu 2000/31/EK, Direktīvu 2001/29/EK un Direktīvu 2004/48/EK, tās lasot arī kopsakarā ar Hartas 17. un 47. pantu. EST secināja, ka minētās trīs direktīvas, kā arī E-privātuma direktīva (Direktīva 2002/58/EK) neizslēdz iespēju dalībvalstīm paredzēt pienākumu civilprocesā izpaust personas datus, lai nodrošinātu autortiesību efektīvu aizsardzību.

EST norādīja, ka šī lieta tādējādi uzsver dažādo pamattiesību, proti, tiesību uz privātās dzīves respektēšanu un tiesību uz īpašuma aizsardzību un efektīvu tiesību aizsardzību prasību nepieciešamo saskaņošanu.

EST secināja, ka "dalībvalstīm, transponējot iepriekš minētās direktīvas, ir jārūpējas, lai tās būtu pamatotas ar tādu minēto direktīvu interpretāciju, kas ļauj nodrošināt atbilstošu līdzsvaru starp dažādajām Kopienu tiesību sistēmā aizsargātajām pamattiesībām. Līdz ar to, īstenojot šo direktīvu transponēšanas pasākumus, dalībvalstu iestādēm un tiesām ir ne tikai jāinterpretē savas valsts tiesības ar direktīvām saskanīgā veidā, bet arī jārūpējas par to, lai

124 EST 2008. gada 29. janvāra spriedums lietā C-275/06 *Productores de Música de España (Promusicae) pret Telefónica de España SAU* [GC], 62.–68. punkts.

125 Turpat, 54. un 60. punkts.

nepamatotos uz tādu šo direktīvu interpretāciju, kas nonāk konfliktā ar šīm pamattiesībām vai citiem Kopienu tiesību vispārējiem principiem – tādiem kā samērīguma princips"[126].

Piemērs. Lieta *Bonnier Audio AB un citi pret Perfect Communication Sweden AB*[127] skāra intelektuālā īpašuma tiesību un personas datu aizsardzības līdzsvarošanu. Prasītāji, pieci izdevēji, kuriem ir autortiesības uz 27 audiogrāmatām, cēla prasību Zviedrijas tiesā, apgalvojot, ka šīs autortiesības tika pārkāptas, izmantojot *FTP* serveri (datņu pārsūtīšanas protokolu, kas ļauj koplietot datnes un nosūtīt datus internetā). Prasītāji lūdza interneta pakalpojumu sniedzēju (*ISP*) atklāt tās personas vārdu un adresi, kura izmanto IP adresi, no kuras šīs datnes tika nosūtītas. *ISP*, *ePhone*, apstrīdēja pieteikumu, apgalvojot, ka tas pārkāpj Direktīvas 2006/24/EK (Datu saglabāšanas direktīvas, kas atcelta 2014. gadā) noteikumus.

Zviedrijas tiesa lūdza EST sniegt prejudiciālo nolēmumu, jautājot, vai Direktīva 2006/24/EK nepieļauj tādu valsts noteikumu piemērošanu, kuru pamatā ir Direktīvas 2004/48/EK (Intelektuālā īpašuma tiesību izpildes direktīvas) 8. pants, kas ļauj izdot rīkojumu, pieprasot IPS nodot autortiesību īpašniekiem informāciju par abonentiem, kuru IP adreses, iespējams, izmantotas pārkāpumu izdarīšanai. Jautājuma pamatā bija pieņēmums, ka prasītājs ir iesniedzis nepārprotamus pierādījumus par konkrēto autortiesību pārkāpumu un ka pasākums ir samērīgs.

EST norādīja, ka Direktīva 2006/24/EK attiecas vienīgi uz elektronisko komunikāciju pakalpojumu sniedzēju veikto datu apstrādi un saglabāšanu smagu noziegumu izmeklēšanas, atklāšanas un kriminālvajāšanas vajadzībām, kā arī to paziņošanu kompetentajām valsts iestādēm. Tādējādi valsts tiesību norma, ar kuru transponē Intelektuālā īpašuma tiesību izpildes direktīvu, neietilpst Direktīvas 2006/24/EK piemērošanas jomā, un tāpēc šī direktīva to neizslēdz[128].

126 Turpat, 65. un 68. punkts; skatīt arī EST 2012. gada 16. februāra spriedumu lietā C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) pret Netlog NV*.

127 EST 2012. gada 19. aprīļa spriedums lietā C-461/10 *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB pret Perfect Communication Sweden AB*.

128 Turpat, 40.–41. punkts.

Attiecībā uz prasītāja pieprasīto informāciju par vārdu un adresi EST sprieda, ka šāda rīcība ir personas datu apstrāde un ietilpst Direktīvas 2002/58/EK (E-privātuma direktīva) piemērošanas jomā. Tiesa arī atzīmēja, ka šo datu paziņošana bija nepieciešama civilprocesā autortiesību īpašnieka labā, lai nodrošinātu efektīvu autortiesību aizsardzību, un tādējādi tā pēc būtības ietilpst arī Direktīvas 2004/48/EK piemērošanas jomā[129].

EST secināja, ka Direktīvas 2002/58/EK un 2004/48/EK jāinterpretē tādējādi, ka tās neaizliedz tādus valsts tiesību aktus, kādi piemēroti pamata tiesvedībā, ciktāl šie tiesību akti ļauj valsts tiesai, pie kuras vēršas ar lūgumu izdot rīkojumu par personas datu izpaušanu, izsvērt iesaistītās konfliktējošās intereses, pamatojoties uz katras lietas faktiem, un pienācīgi ņemt vērā proporcionalitātes principa prasības.

1.3.6. Datu aizsardzība un ekonomiskās intereses

Digitālajā jeb lielo datu laikmetā dati tiek raksturoti kā ekonomikas jaunā nafta, veicinot inovācijas un radošumu[130]. Daudzi uzņēmumi, izmantojot datu apstrādi, ir izveidojuši spēcīgus uzņēmējdarbības modeļus, un šāda apstrāde bieži ietver personas datus. Daži uzņēmumi var uzskatīt, ka īpaši noteikumi par personas datu aizsardzību praksē var būt pārāk apgrūtinoši, ietekmējot viņu ekonomiskās intereses. Tādējādi rodas jautājums: vai pārziņu, apstrādātāju vai plašas sabiedrības ekonomiskās intereses būtu uztveramas kā attaisnojums tiesību uz datu aizsardzību ierobežošanai.

Piemērs. Lietā *Google Spain*[131] EST uzskatīja, ka noteiktos apstākļos indivīdiem ir tiesības pieprasīt meklētājprogrammām izņemt meklēšanas rezultātus no to meklēšanas indeksa. Savā argumentācijā EST norādīja uz to, ka meklētājprogrammu un uzrādīto meklēšanas rezultātu izmantošana var ļaut izveidot detalizētu personas profilu. Šī informācija var skart plašu personas privātās dzīves aspektu, un to nevarētu vienkārši atrast vai savstarpēji

129 Turpat, 52.–54. punkts. Skatīt arī EST 2008. gada 29. janvāra spriedumu lietā C-275/06 *Productores de Música de España (Promusicae) pret Telefónica de España SAU* [GC], 58. punkts.

130 Skatīt, piemēram, *Financial Times* (2016), "Data is the new oil ... who's going to own it?", 2016. gada 16. novembris.

131 EST 2014. gada 13. maija spriedums lietā C-131/12 *Google Spain SL un Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC].

savienot bez meklētājprogrammas palīdzības. Tādējādi tā ir potenciāli būtiska iejaukšanās datu subjektu pamattiesībās uz privātumu un personas datu aizsardzību.

Tālāk EST pārbaudīja, vai šāda iejaukšanās ir attaisnojama. Attiecībā uz meklētājprogrammu uzņēmuma ekonomiskajām interesēm veikt datu apstrādi, EST paziņoja, ka "ir jākonstatē, ka [iejaukšanās] nevar tikt attaisnota vienīgi ar šādas meklētājprogrammas pakalpojumu sniedzēja ekonomisko interesi šādā apstrādē", un ka "parasti" pamattiesības, kas noteiktas Hartas 7. un 8. pantā, ir svarīgākas par šādām ekonomiskām interesēm un plašas sabiedrības interesēm atrast šo informāciju, veicot meklēšanu saistībā ar datu subjekta vārdu[132].

Viens no galvenajiem apsvērumiem Eiropas tiesību aktos datu aizsardzības jomā ir nodrošināt indivīdiem lielāku kontroli pār viņu personas datiem. Jo īpaši digitālajā laikmetā pastāv nelīdzsvarotība starp uzņēmējdarbības struktūrām, kuras apstrādā lielu daudzumu personas datu un kurām ir pieeja šiem datiem, un to personu, kurām šie personas dati pieder, spēju kontrolēt viņu informāciju. EST izskata katru gadījumu individuāli, līdzsvarojot datu aizsardzību un ekonomiskās intereses, piemēram, trešo personu intereses saistībā ar akciju sabiedrībām un sabiedrībām ar ierobežotu atbildību, kā parādīts spriedumā *Manni* lietā.

Piemērs. Lieta *Manni*[133] attiecās uz indivīda personas datu iekļaušanu publiskajā komercreģistrā. *Manni* kungs bija lūdzis Lečes Tirdzniecības palātai dzēst viņa personas datus no šā reģistra, jo bija atklājis, ka potenciālie klienti izmanto reģistru, un redzēja, ka viņš ir bijis kāda uzņēmuma administrators, kas pirms vairāk nekā desmit gadiem tika pasludināts par bankrotējušu. Šī informācija negatīvi noskaņoja viņa potenciālos klientus, un tai varēja būt negatīva ietekme uz viņa komerciālajām interesēm.

EST tika lūgta noteikt, vai ES tiesību aktos šajā gadījumā tiek atzītas tiesības uz datu dzēšanu. Savā secinājumā tiesa izsvēra ES datu aizsardzības noteikumus un *Manni* kunga komerciālās intereses dzēst informāciju par viņa bijušā uzņēmuma bankrotu ar sabiedrības interesēm piekļūt informācijai. Tiesa

132 Turpat, 81. un 97. pants.

133 EST 2017. gada 9. marta spriedums lietā C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce pret Salvatore Manni*.

pienācīgi ņēma vērā faktu, ka informācijas publiskošana uzņēmumu reģistrā bija paredzēta tiesību aktos un jo īpaši ES direktīvā, kuras mērķis ir padarīt informāciju par uzņēmumiem vieglāk pieejamu trešām personām. Informācijas izpaušana bija svarīga, lai aizsargātu to trešo personu intereses, kuras varētu plānot uzņēmējdarbību ar konkrēto uzņēmumu, jo vienīgās garantijas, ko akciju sabiedrības un sabiedrības ar ierobežotu atbildību piedāvā trešām personām, ir to aktīvi. Tādēļ "attiecīgo sabiedrību pamatdokumentiem ir jābūt pieejamiem, lai trešās personas varētu iepazīties ar to saturu un citu informāciju, kas attiecas uz sabiedrību, īpaši ar sīkiem datiem par personām, kuras ir pilnvarotas uzņemties saistības sabiedrības vārdā"[134].

Ņemot vērā reģistra izvirzītā likumīgā mērķa nozīmi, EST uzskatīja, ka *Manni* kungam nebija tiesību pieprasīt savu personas datu dzēšanu, jo nepieciešamība aizsargāt trešo personu intereses saistībā ar akciju sabiedrībām un sabiedrībām ar ierobežotu atbildību un nodrošināt juridisko noteiktību, godīgu tirdzniecību un tādējādi arī iekšējā tirgus pareizu darbību prevalēja pār tiesību aktos noteiktajām viņa datu aizsardzības tiesībām. Tas jo īpaši bija tā, ņemot vērā faktu, ka personas, kuras izvēlas tirgoties ar akciju sabiedrības vai sabiedrības ar ierobežotu atbildību starpniecību, apzinās, ka tām ir pienākums izpaust informāciju par viņu identitāti un funkcijām.

Konstatējot, ka šajā gadījumā nav pamata panākt datu dzēšanu, EST atzina, ka pastāv tiesības iebilst pret datu apstrādi, un atzīmēja: "nevar (..) izslēgt, ka varētu pastāvēt īpašas situācijas, kurās ar attiecīgās personas konkrētu gadījumu saistīti nepārvarami un likumīgi iemesli izņēmuma kārtā pamato to, ka piekļuve reģistrā iekļautajiem personas datiem, kas skar attiecīgo personu, beidzoties pietiekami ilgam termiņam (..), tiek ierobežota, sniedzot to tikai trešām personām, kuras pamato savas īpašās intereses ar tiem iepazīties"[135].

EST norādīja, ka valsts tiesām katrā atsevišķā gadījumā jāizvērtē, ņemot vērā visus attiecīgos indivīda apstākļus, likumīgu un nepārvaramu iemeslu esamība vai neesamība, kas izņēmuma kārtā varētu attaisnot trešo personu piekļuves ierobežošanu uzņēmumu reģistros ietvertajiem personas datiem. Tomēr EST precizēja, ka *Manni* kunga gadījumā faktu, ka viņa personas datu izpaušana reģistrā, iespējams, ietekmēja viņa klientūru, nevar uzskatīt par

134 Turpat, 49. punkts.

135 Turpat, 60. punkts.

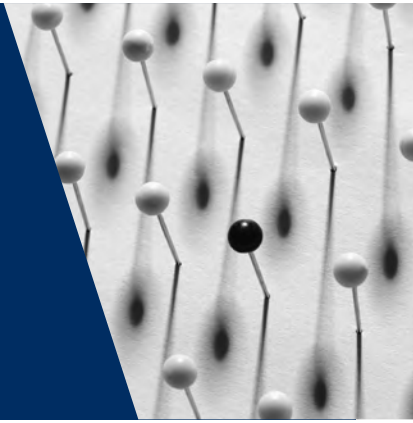
šādu likumīgu un nepārvaramu iemeslu. Potenciālajiem *Manni* kunga klientiem ir likumīgas intereses saņemt informāciju par viņa iepriekšējā uzņēmuma bankrotu.

Iejaukšanās *Manni* kunga un citu reģistrā iekļauto personu pamattiesībās uz privātās dzīves neaizskaramību un personas datu aizsardzību, ko garantē Hartas 7. un 8. pants, kalpoja vispārējas nozīmes mērķim un bija nepieciešama un samērīga.

Tāpēc *Manni* lietā EST uzskatīja, ka tiesības uz datu aizsardzību un privātumu neprevalē pār trešo personu interesēm piekļūt uzņēmumu reģistrā esošajai informācijai par akciju sabiedrībām un sabiedrībām ar ierobežotu atbildību.

2

Datu aizsardzības terminoloģija



ES	Aptvertie jautājumi	EP
Personas dati		
Vispārīgā datu aizsardzības regula, 4. panta 1. punkts Vispārīgā datu aizsardzības regula, 4. panta 5. punkts un 5. panta 1. punkta e) apakšpunkts Vispārīgā datu aizsardzības regula, 9. pants EST apvienotās lietas C-92/09 un C-93/09 *Volker und Markus Schecke GbR un Hartmut Eifert pret Land Hessen* [GC], 2010 EST lieta C-275/06 *Productores de Música de España (Promusicae) pret Telefónica de España SAU* [GC], 2008 EST lieta C-70/10 *Scarlet Extended SA pret Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 EST lieta C-582/14 *Patrick Breyer pret Vācijas Federatīvo Republiku*, 2016 EST apvienotās lietas C-141/12 un C-372/12 *YS pret Minister voor Immigratie, Integratie en Asiel* un *Minister voor Immigratie, Integratie en Asiel pret M un S*, 2014	**Datu aizsardzības juridiskā definīcija**	Modernizētā Konvencija Nr. 108, 2. panta a) punkts ECT lieta *Bernh Larsen Holding AS un citi pret Norvēģiju*, Nr. 24117/08, 2013 ECT lieta *Uzun pret Vāciju*, Nr. 35623/05, 2010 ECT lieta *Amann pret Šveici* [GC], Nr. 27798/95, 2000
EST lieta C-101/01 *Kriminālprocess pret Bodil Lindqvist*, 2003	**Īpašu kategoriju personas dati (sensitīvi dati)**	Modernizētā Konvencija Nr. 108, 6. panta 1. punkts

ES	Aptvertie jautājumi	EP
EST lieta C-434/16 *Peter Nowak pret Datu aizsardzības komisāru*, 2017	**Anonimizēti un pseidonimizēti personas dati**	Modernizētā Konvencija Nr. 108, 5. panta 4. punkta e) apakšpunkts Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 50. punkts
Datu apstrāde		
Vispārīgā datu aizsardzības regula, 4. panta 2. punkts EST lieta C-212/13 *František Ryneš pret Úřad pro ochranu osobních údajů*, 2014 EST lieta C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce pret Salvatore Manni*, 2017 EST lieta C-101/01 *Kriminālprocess pret Bodil Lindqvist*, 2003 EST lieta C-131/12 *Google Spain SL, Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	**Definīcijas**	Modernizētā Konvencija Nr. 108, 2. panta b) un c) punkts
Datu lietotāji		
Vispārīgā datu aizsardzības regula, 4. panta 7. punkts EST lieta C-212/13 *František Ryneš pret Úřad pro ochranu osobních údajů*, 2014 EST lieta C-1318/12 *Google Spain SL, Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	**Pārzinis**	Modernizētā Konvencija Nr. 108, 2. panta d) punkts Ieteikums par profilēšanu, 1. punkta g) apakšpunkts*
Vispārīgā datu aizsardzības regula, 4. panta 8. punkts	**Apstrādātājs**	Modernizētā Konvencija Nr. 108, 2. panta f) punkts Ieteikums par profilēšanu, 1. punkta h) apakšpunkts
Vispārīgā datu aizsardzības regula, 4. panta 9. punkts	**Saņēmējs**	Modernizētā Konvencija Nr. 108, 2. panta e) punkts
Vispārīgā datu aizsardzības regula, 4. panta 10. punkts	**Trešā persona**	

ES	Aptvertie jautājumi	EP
Piekrišana		
Vispārīgā datu aizsardzības regula, 4. panta 11. punkts un 7. pants EST lieta C-543/09 *Deutsche Telekom AG pret Vācijas Federatīvo Republiku*, 2011 EST lieta C-536/15 *Tele2 (Netherlands) BV un citi pret Autoriteit Consument en Markt (AMC)*, 2017	**Spēkā esošas piekrišanas definīcija un tai piemērojamās prasības**	Modernizētā Konvencija Nr. 108, 5. panta 2. punkts Medicīnisko datu ieteikums, 6. punkts, kā arī citi vēlākie ieteikumi ECT lieta *Elberte pret Latviju*, Nr. 61243/08, 2015

*Piezīme: * Eiropas Padomes Ministru komiteja (2010), Ministru komitejas Ieteikums CM/Rec(2010)13 dalībvalstīm par fizisko personu aizsardzību attiecībā uz personas datu automātisku apstrādi datu profilu veidošanas kontekstā (Ieteikums par profilēšanu), 2010. gada 23. novembris*

2.1. Personas dati

Svarīgākie aspekti

- Dati ir uzskatāmi par personas datiem, ja tie attiecas uz identificētu vai identificējamu personu – "datu subjektu".
- Lai noteiktu, vai fiziska persona ir identificējama, pārzinim vai citai personai ir jāņem vērā visi saprātīgie līdzekļi, ko iespējams izmantot, piemēram, izdalīšanu, lai tieši vai netieši identificētu fizisko personu.
- Autentifikācija nozīmē pierādīt, ka konkrētai personai piemīt konkrēta identitāte un/vai tā ir pilnvarota veikt noteiktas darbības.
- Ir īpašas datu kategorijas, tā sauktie sensitīvie dati, kas uzskaitīti modernizētajā Konvencijā Nr. 108 un ES tiesību aktos datu aizsardzības jomā, kuriem nepieciešama pastiprināta aizsardzība, tāpēc tie ir pakļauti īpašam tiesiskajam režīmam.
- Dati tiek anonimizēti, ja tie vairs neattiecas uz identificētu vai identificējamu personu.
- Pseidonimizācija ir pasākums, ar kuru personas datus nevar saistīt ar datu subjektu bez papildu informācijas, kas tiek turēta atsevišķi. "Atslēga", kas ļauj atkārtoti identificēt datu subjektus, ir jāuzglabā atsevišķi, tai jābūt drošai. Pseidonimizācijas procesam pakļautie dati joprojām ir personas dati. ES tiesību aktos nepastāv "pseidonimizētu datu" jēdziens.
- Datu aizsardzības principus un noteikumus nepiemēro anonimizētai informācijai. Taču tos piemēro pseidonimizētiem datiem.

2.1.1. Personas datu jēdziena galvenie aspekti

Saskaņā ar ES un **EP tiesību aktiem** "personas dati" tiek definēti kā informācija, kas attiecas uz identificētu vai identificējamu fizisku personu[136]. Tie attiecas uz informāciju par personu, kuras identitāte ir nepārprotami skaidra vai to var noteikt, izmantojot papildinformāciju. Lai noteiktu, vai persona ir identificējama, pārzinim vai citai personai ir jāņem vērā visi saprātīgie līdzekļi, kas, iespējams, tiek izmantoti tiešai vai netiešai personas identificēšanai, piemēram, izdalīšana, kas ļauj izturēties pret vienu personu savādāk nekā pret citu[137].

Ja tiek apstrādāti dati par šādu personu, šo personu sauc par "datu subjektu".

Datu subjekts

Saskaņā ar ES tiesību aktiem fiziskās personas ir vienīgie labuma guvēji no datu aizsardzības noteikumiem[138], un tikai dzīvas būtnes tiek aizsargātas saskaņā ar Eiropas tiesību aktiem datu aizsardzības jomā[139]. Vispārīgajā datu aizsardzības regulā (VDAR) personas dati ir definēti kā jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu.

EP tiesību aktos, jo īpaši modernizētajā Konvencijā Nr. 108, arī ir atsauce uz personu aizsardzību attiecībā uz viņu personas datu apstrādi. Arī šeit personas dati ir jebkura informācija par identificētu vai identificējamu indivīdu. Šī fiziskā persona jeb indivīds, kā minēts attiecīgi VDAR un modernizētajā Konvencijā Nr. 108, datu aizsardzības tiesību aktos ir zināms kā datu subjekts.

Arī juridiskajām personām tiek nodrošināta zināma aizsardzība. Pastāv ECT judikatūra ar spriedumiem par juridisko personu pieteikumiem attiecībā uz iespējamu tiesību uz aizsardzību pret to datu izmantošanu pārkāpumiem saskaņā ar ECTK 8. pantu. ECTK 8. pants attiecas gan uz tiesībām uz privātās un ģimenes dzīves neaizskaramību, gan uz dzīvokļa un korespondences neaizskaramību. Tādēļ Tiesa var izskatīt lietas, pamatojoties uz pēdējo minēto tiesību, nevis uz tiesību uz privāto dzīvi argumentu.

136 Vispārīgā datu aizsardzības regula, 4. panta 1. punkts un modernizētā Konvencija Nr. 108, 2. panta a) punkts.

137 Vispārīgā datu aizsardzības regula, 26. apsvērums.

138 Turpat, 1. pants.

139 Turpat, 27. apsvērums. Skatīt arī 29. panta darba grupas (2007) *Atzinumu 4/2007 par "personas datu" jēdzienu*, WP 136, 2007. gada 20. jūnijs, 22. lpp.

Piemērs. Lieta *Bernh Larsen Holding AS un citi pret Norvēģiju*[140] attiecās uz triju Norvēģijas uzņēmumu sūdzību par nodokļu iestādes lēmumu, ar kuru tiem tika uzdots nodokļu inspektoriem iesniegt visu to datu kopijas, kas glabājas uz to kopīgi izmantotā datora servera.

ECT secināja, ka šāda pienākuma piemērošana prasītājiem uzņēmumiem ir iejaukšanās viņu tiesībās uz "dzīvokļa" un "korespondences" neaizskaramību saskaņā ar ECTK 8. pantu. Taču Tiesa secināja, ka nodokļu administrācijas rīcībā bija efektīvi un atbilstoši aizsardzības pasākumi pret ļaunprātīgu izmantošanu, jo uzņēmumi, kas iesniedza pieteikumus, tika savlaicīgi informēti, bija klāt un varēja iesniegt pieteikumus veiktās izmeklēšanas laikā uz vietas, bet materiāli bija jāiznīcina pēc nodokļu pārbaudes pabeigšanas. Šādos apstākļos tika panākts taisnīgs līdzsvars starp prasītāju uzņēmumu tiesībām uz "dzīvokļa" un "korespondences" neaizskaramību un to interesēm aizsargāt viņu labā strādājošo personu privātumu, no vienas puses, un sabiedrības interesēm nodrošināt efektīvu pārbaudi nodokļu aprēķināšanas nolūkos, no otras puses. Attiecīgi Tiesa atzina, ka šajā lietā 8. pants nav pārkāpts.

Atbilstoši modernizētajai Konvencijai Nr. 108 datu aizsardzība galvenokārt nozīmē fizisku personu aizsardzību. Tomēr līgumslēdzējas puses savos tiesību aktos var paplašināt datu aizsardzību, attiecinot to arī uz juridiskām personām, piemēram, uzņēmumiem un apvienībām. Modernizētās Konvencijas skaidrojošajā ziņojumā ir teikts, ka valsts tiesību aktos var aizsargāt juridisko personu likumīgās intereses, paplašinot konvencijas piemērošanas jomu uz šādiem dalībniekiem[141]. **ES tiesību akti datu aizsardzības jomā** neattiecas uz datu apstrādi, kas skar juridiskās personas, un jo īpaši neattiecas uz uzņēmumiem, kas reģistrēti kā juridiskas personas, tostarp uz juridiskās personas nosaukumu un formu, kā arī to kontaktinformāciju[142]. Taču E-privātuma direktīva aizsargā komunikācijas konfidencialitāti un juridisko personu likumīgās intereses attiecībā uz pieaugošajām iespējām automātiski glabāt un apstrādāt datus saistībā ar abonentiem un lietotājiem[143]. Līdzīgi E-privātuma regulas projektā ir paredzēta arī juridisko personu aizsardzība.

140 ECT 2013. gada 14. marta spriedums lietā *Bernh Larsen Holding AS un citi pret Norvēģiju*, Nr. 24117/08. Tomēr skatīt arī ECT 2008. gada 1. jūlija spriedumu lietā *Liberty un citi pret Apvienoto Karalisti*, Nr. 58243/00.

141 Modernizētās konvencijas Nr. 108 skaidrojošais ziņojums, 30. punkts.

142 Vispārīgā datu aizsardzības regula, 14. apsvērums

143 E-privātuma direktīva, 7. apsvērums un 1. panta 2. punkts.

Piemērs. Lietā *Volker und Markus Schecke un Hartmut Eifert pret Land Hessen*[144] EST, atsaucoties uz personas datu publicēšanu par lauksaimniecības atbalsta saņēmējiem, uzskatīja, ka "juridiskas personas var atsaukties uz Hartas 7. un 8. panta aizsardzību attiecībā uz šādu identificēšanu tikai tad, ja ar juridiskas personas juridisko nosaukumu tiek identificētas viena vai vairākas fiziskas personas. (..) [T]iesības uz privātās dzīves neaizskaramību attiecībā uz personas datu apstrādi, kas atzītas Hartas 7. un 8. pantā, attiecas uz visu informāciju, kas skar identificētu vai identificējamu fizisku personu (..)"[145].

Līdzsvarojot ES intereses nodrošināt pārredzamību palīdzības piešķiršanā, no vienas puses, un to personu pamattiesības uz privātumu un datu aizsardzību, kuras saņēmušas atbalstu, no otras puses, EST uzskatīja, ka iejaukšanās šajās pamattiesībās ir nesamērīga. Tā uzskatīja, ka pārredzamības mērķi varēja efektīvi sasniegt ar pasākumiem, kas mazāk ierobežo attiecīgo personu tiesības. Tomēr, izskatot samērīgumu informācijas publicēšanai par juridiskām personām, kuras saņēmušas atbalstu, EST izdarīja atšķirīgu secinājumu, spriežot, ka šāda publicēšana nepārsniedz proporcionalitātes principa robežas. Tā norādīja, ka "tiesību uz personas datu aizsardzību aizskāruma smagums juridiskām personām izpaužas citādāk nekā fiziskām personām"[146]. Juridiskām personām ir noteikts daudz plašāks pienākums attiecībā uz ar tām saistītās informācijas publicēšanu. EST uzskatīja, ka prasība valsts iestādēm pirms datu publicēšanas pārbaudīt, vai dati par katru saņēmēju juridisko personu identificē saistītas fiziskas personas, uzliktu šīm iestādēm pārmērīgu administratīvo slogu. Tāpēc tiesību aktos, kas pieprasa vispārēju datu publicēšanu par juridiskām personām, bija ievērots taisnīgs līdzsvars starp attiecīgajām konkurējošajām interesēm.

Datu raksturs

Jebkāda veida informācija var būt personas dati, ja tā attiecas uz identificētu vai identificējamu personu.

144 EST 2010. gada 9. novembra spriedums apvienotajās lietās C-92/09 un C-93/09 *Volker und Markus Schecke GbR un Hartmut Eifert pret Land Hessen* [GC], 53. punkts.

145 Turpat, 52.–53. punkts.

146 Turpat, 87. punkts.

Piemērs. Vadītāja veiktais darbinieka snieguma novērtējums, kas tiek glabāts darbinieka personāla lietā, ir darbinieka personas dati. Tas uzskatāms par personas datiem arī tad, ja tas daļēji vai pilnībā atspoguļo vadītāja personīgo viedokli, piemēram: "darbinieks pietiekami nevelta sevi darbam", nevis faktus, piemēram: "darbinieks pēdējo sešu mēnešu laikā nav bijis darbā piecas nedēļas".

Personas dati ietver informāciju, kas attiecas uz personas privāto dzīvi, ietverot arī profesionālo darbību, kā arī informāciju par personas publisko dzīvi.

Lietā *Amann*[147] ECT interpretēja jēdzienu "personas dati" kā plašāk attiecināmu, ne tikai uz personas privātās sfēras jautājumiem. Šī termina "personas dati" nozīme attiecas arī uz VDAR.

Piemērs. Lietā *Volker und Markus Schecke un Hartmut Eifert pret Land Hessen*[148] EST paziņoja, ka "šajā sakarā nav nozīmes faktam, ka publicētās ziņas attiecas uz profesionālo darbību (..). Saistībā ar Konvencijas [ECTK] 8. panta interpretāciju Eiropas Cilvēktiesību tiesa šajā sakarībā ir nospriedusi, ka jēdziens "privātā dzīve" nav tulkojams sašaurināti un ka pamatā netiek pieļauta iespēja profesionālo darbību "izņemt no privātās dzīves" jēdziena (..)".

Piemērs. Apvienotajās lietās *YS pret Minister voor Immigratie, Integratie en Asiel* un *Minister voor Immigratie, Integratie en Asiel pret M un S*[149] EST paziņoja, ka Imigrācijas un naturalizācijas dienesta lēmuma projektā ietvertā juridiskā analīze par uzturēšanās atļauju piemērošanu pati par sevi nav personas dati, kaut arī tajā var būt ietverti daži personas dati.

ECT judikatūra attiecībā uz ECTK 8. pantu apstiprina, ka pilnībā nodalīt privātās un profesionālās dzīves jautājumus var būt sarežģīti[150].

147 Skatīt ECT 2000. gada 16. februāra spriedumu lietā *Amann pret Šveici*, Nr. 27798/95, 65. punkts.

148 EST 2010. gada 9. novembra spriedums apvienotajās lietās C-92/09 un C-93/09 *Volker und Markus Schecke GbR un Hartmut Eifert pret Land Hessen* [GC], 59. punkts.

149 EST 2014. gada 17. jūlija spriedums apvienotajās lietās C-141/12 un C-372/12 *YS pret Minister voor Immigratie, Integratie en Asiel* un *Minister voor Immigratie, Integratie en Asiel pret M un S*, 39. punkts.

150 Skatīt, piemēram, ECT 2000. gada 4. maija spriedumu lietā *Rotaru pret Rumāniju* [GC], Nr. 28341/95, 43. punkts; ECT 1992. gada 16. decembra spriedumu lietā *Niemietz pret Vāciju*, Nr. 13710/88, 29. punkts.

Piemērs. Lietā *Bărbulescu pret Rumāniju*[151] prasītājs tika atlaists par darba devēja interneta izmantošanu darba laikā, pārkāpjot iekšējos noteikumus. Darba devējs bija uzraudzījis šā darbinieka saziņu, un ieraksti, kas liecināja par pilnīgi privāta rakstura ziņojumiem, tika uzrādīti tiesvedības valsts tiesās gaitā. Konstatējusi 8. panta piemērojamību, ECT atstāja atklātu jautājumu, vai darba devēja ierobežojošie noteikumi ļāva prasītājam pamatoti cerēt uz privātuma ievērošanu, bet jebkurā gadījumā secināja, ka darba devēja norādījumi nevar samazināt privāto sociālo dzīvi darba vietā līdz nullei. Runājot pēc būtības, līgumslēdzējām valstīm bija jāpiešķir plaša rīcības brīvība, novērtējot nepieciešamību izveidot tiesisko regulējumu, kas reglamentē apstākļus, kādos darba devējs darba vietā var regulēt savu darbinieku ar darbu nesaistīto saziņu: gan elektronisku, gan cita veida. Tomēr valsts iestādēm bija jānodrošina, lai darba devēju ieviestie pasākumi korespondences un citas saziņas uzraudzībai neatkarīgi no šādu pasākumu apjoma un ilguma tiktu papildināti ar piemērotiem un pietiekamiem aizsardzības līdzekļiem pret to ļaunprātīgu izmantošanu. Samērīguma un procesuālo garantiju ievērošana ir būtiska, lai novērstu patvaļu, un ECT identificēja vairākus faktorus, kas bija būtiski šajos apstākļos. Šādi faktori ietvēra, piemēram, to, cik lielā mērā darba devējs uzrauga darbiniekus un kāds ir iejaukšanās līmenis darbinieka privātumā, sekas darbiniekam un to, vai pastāv atbilstoši drošības pasākumi. Turklāt valsts iestādēm bija jānodrošina, ka darbiniekam, kura saziņa tika uzraudzīta, ir iespēja izmantot tiesiskās aizsardzības līdzekļus tiesā, kas ir kompetenta vismaz pēc būtības noteikt, kā šie izklāstītie kritēriji tika ievēroti un vai apstrīdētie pasākumi bija likumīgi. Šajā gadījumā ECT konstatēja 8. panta pārkāpumu, jo valsts iestādes nebija nodrošinājušas pienācīgu aizsardzību prasītāja tiesībām uz viņa privātās dzīves un korespondences neaizskaramību un attiecīgi nebija panākušas taisnīgu līdzsvaru starp attiecīgajām interesēm.

Saskaņā ar ES un **EP tiesību aktiem** informācija satur datus par personu šādos gadījumos:

- indivīds šīs informācijas dēļ ir identificēts vai identificējams; vai
- indivīdu, lai arī tas nav identificēts, ar šo informāciju var izdalīt tādā veidā, kas ļauj noskaidrot, kurš ir datu subjekts, veicot papildu izpēti.

151 ECT 2017. gada 5. septembra spriedums lietā *Bărbulescu pret Rumāniju* [GC], Nr. 61496/08, 121. punkts.

Saskaņā ar Eiropas tiesību aktiem datu aizsardzības jomā abi informācijas veidi tiek vienādi aizsargāti. Personu tieša vai netieša identificēšana ir pastāvīgi jāizvērtē, "ņemot vērā apstrādes laikā pieejamo tehnoloģiju un tehnoloģiju attīstību"[152]. ECT vairākkārt ir atkārtojusi, ka jēdziens "personas dati" ECKT ir tāds pats kā Konvencijā Nr. 108, jo īpaši attiecībā uz nosacījumu par identificētām vai identificējamām personām[153].

VDAR noteikts, ka fiziska persona ir identificējama, ja viņu "var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem"[154]. Tādējādi identificēšanai ir nepieciešami elementi, kas personu raksturo tā, lai persona būtu atšķirama no visām citām personām un būtu atpazīstama kā indivīds. Personas vārds ir lielisks šādu apraksta elementu piemērs, un ar to var tieši identificēt personu. Dažos gadījumos citiem atribūtiem var būt līdzīga ietekme kā vārdam, padarot personu netieši identificējamu. Tālruņa numurs, sociālās apdrošināšanas numurs un transportlīdzekļa reģistrācijas numurs ir tādas informācijas piemēri, ar kuru starpniecību var identificēt indivīdu. Indivīdu izdalīšanai ir iespējams arī izmantot atribūtus, piemēram, datorizētus failus, sīkdatnes un tīmekļa plūsmas uzraudzības rīkus, identificējot viņu uzvedību un paradumus. Kā paskaidrots 29. panta datu aizsardzības darba grupas atzinumā, "[p]at neinteresējoties par indivīda vārdu vai adresi, ir iespējams kategorizēt šo personu, pamatojoties uz sociālekonomiskiem, psiholoģiskiem, filozofiskiem vai citiem kritērijiem un piedēvēt viņam vai viņai konkrētus lēmumus, jo indivīda kontaktpunkta (datora) dēļ viņa vai viņas identitātes atklāšana šā jēdziena sašaurinātā izpratnē vairs nav nepieciešama"[155]. Personas datu definīcija gan EP, gan ES tiesību aktos ir pietiekami plaša, lai ietvertu visas identifikācijas iespējas (un līdz ar to arī visas identificējamības pakāpes).

152 Vispārīgā datu aizsardzības regula, 26. apsvērums.

153 Skatīt ECT 2000. gada 16. februāra spriedumu lietā *Amann pret Šveici* [GC], Nr. 27798/95, 65. punkts.

154 Vispārīgā datu aizsardzības regula, 4. panta 1. punkts.

155 29. panta datu aizsardzības darba grupa, *Atzinums 4/2007 par "personas datu" jēdzienu* WP 136, 2007. gada 20. jūnijs, 15. lpp.

Piemērs. Lietā *Promusicae pret Telefónica de España*[156] EST paziņoja, ka "turklāt netiek apstrīdēts, ka *Promusicae* lūgtā noteiktu [konkrētas interneta datņu koplietošanas platformas] lietotāju vārdu un adrešu paziņošana netieši skar personas datu sniegšanu, proti, informāciju par identificētām vai identificējamām fiziskām personām saskaņā ar Direktīvas 95/46/EK 2. panta a) punktā esošo definīciju [pašlaik VDAR 4. panta 1. punkts]. Šī tās informācijas sniegšana, ko, kā norāda *Promusicae*, uzkrājusi *Telefónica*, – un ko pēdējā minētā nenoliedz – ir personas datu apstrāde"[157].

Piemērs. Lieta *Scarlet Extended SA pret Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[158] skāra interneta pakalpojumu sniedzēja *Scarlet* atteikumu uzstādīt sistēmu tādas elektroniskās komunikācijas filtrēšanai, kurā izmanto datņu koplietošanas programmatūras, lai novērstu tādu datņu koplietošanu, ar kurām pārkāpj autortiesības, ko aizsargā pārvaldības sabiedrība *SABAM*, kura pārstāv autorus, komponistus un redaktorus. EST uzskatīja, ka lietotāju IP adreses "ir aizsargātie personas dati tāpēc, ka tie ļauj precīzi identificēt minētos lietotājus".

Tā kā daudzi vārdi nav unikāli, personas identitātes noteikšanai var būt nepieciešami papildu atribūti, lai nodrošinātu, ka persona netiek sajaukta ar kādu citu. Dažreiz var nākties apvienot tiešos un netiešos atribūtus, lai identificētu personu, uz kuru attiecas informācija. Bieži tiek izmantots dzimšanas datums un vieta. Turklāt dažās valstīs ir ieviesti personalizēti numuri, kas ļauj labāk atšķirt pilsoņus. Nosūtītie nodokļu dati[159], dati par uzturēšanās atļaujas pieteikuma iesniedzēju administratīvā dokumentā[160] un dokumenti, kas attiecas uz banku un fiduciārajām attiecībām[161], var būt personas dati. Lai identificētu personas tehnoloģiskajā laikmetā, arvien vairāk izmanto biometriskos datus, piemēram, pirkstu nospiedumus, digitālās fotogrāfijas vai varavīksnenes skenēšanu, atrašanās vietas datus un tiešsaistes atribūtus.

156 EST 2008. gada 29. janvāra spriedums lietā C-275/06 *Productores de Música de España (Promusicae) pret Telefónica de España SAU* [GC], 45. punkts.

157 Iepriekšējā Direktīva 95/46/EK, 2. panta b) punkts, tagad Vispārīgā datu aizsardzības regula, 4. panta 2. punkts.

158 EST 2011. gada 24. novembra spriedums lietā C-70/10 *Scarlet Extended SA pret Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 51. punkts.

159 EST 2015. gada 1. oktobra spriedums lietā C-201/14 *Smaranda Bara un citi pret Casa Națională de Asigurări de Sănătate un citiem*.

160 EST 2014. gada 17. jūlija spriedums lietā *YS pret Minister voor Immigratie, Integratie en Asiel* un *Minister voor Immigratie, Integratie en Asiel pret M un S*.

161 ECT 2015. gada 7. jūlija spriedums lietā *M.N. un citi pret Sanmarīno*, Nr. 28005/12.

Tomēr, lai varētu piemērot Eiropas datu aizsardzības tiesību aktus, datu subjekta faktiska identificēšana nav nepieciešama. Pietiek ar to, ka attiecīgā persona ir identificējama. Personu uzskata par identificējamu, ja ir pieejams pietiekams daudzums elementu, ar kuru palīdzību personu var tieši vai netieši identificēt[162]. Atbilstoši VDAR 26. apsvērumam par kritēriju uzskata to, vai ir ticams, ka paredzamajiem informācijas lietotājiem būs pieejami un viņi saprātīgi pārvaldīs identifikācijas līdzekļus. Tas ietver informāciju, kura ir trešo personu saņēmēju rīcībā (skatīt 2.3.2. iedaļu).

Piemērs. Pašvaldības iestāde nolemj vākt datus par automašīnām, kas pārsniedz ātrumu vietējās apkaimes ielās. Tā fotografē automašīnas, automātiski reģistrējot laiku un vietu, lai datus nodotu kompetentajai iestādei sodīšanai par ātruma ierobežojumu pārkāpšanu. Datu subjekts iesniedz sūdzību, apgalvojot, ka pašvaldības iestādei saskaņā ar datu aizsardzības tiesību aktiem nav juridiska pamata šādai datu vākšanai. Pašvaldības iestāde apgalvo, ka tā nevāc personas datus. Tā apgalvo, ka reģistrācijas numura zīmes ir anonīmas. Pašvaldības iestādei nav juridisku pilnvaru piekļūt vispārējam transportlīdzekļu reģistram, lai noskaidrotu automašīnas īpašnieka vai vadītāja identitāti.

Šī argumentācija neatbilst VDAR 26. apsvērumam. Tā kā datu vākšanas mērķis nepārprotami ir identificēt un sodīt ātruma ierobežojumu pārkāpējus, ir paredzams, ka tiks veikti identificēšanas mēģinājumi. Lai arī pašvaldības iestāžu rīcībā nav tiešu identificēšanas līdzekļu, tās datus nodos kompetentajai iestādei, policijai, kuras rīcībā ir šādi līdzekļi. Nepārprotams scenārijs ir iekļauts 26. apsvērumā, paredzot, ka citi datu saņēmēji, bet ne tiešais datu lietotājs, var mēģināt identificēt personu. Ņemot vērā 26. apsvērumu, pašvaldības iestādes rīcība ir pielīdzināma datu vākšanai par identificējamām personām, un tāpēc ir nepieciešams juridiskais pamats saskaņā ar datu aizsardzības tiesību aktiem.

Lai "pārliecinātos, vai līdzekļus varētu pietiekami iespējami izmantot fiziskas personas identificēšanai, būtu jāņem vērā visi objektīvie faktori, piemēram, identificēšanai nepieciešamās izmaksas un laiks, ņemot vērā apstrādes laikā pieejamo tehnoloģiju un tehnoloģiju attīstību"[163].

162 Vispārīgā datu aizsardzības regula, 4. panta 1. punkts.

163 Turpat, 26. apsvērums.

Piemērs. Lietā *Breyer pret Bundesrepublik Deutschland*[164] EST aplūkoja datu subjektu netiešās identificējamības jēdzienu. Lieta skāra dinamiskās interneta protokola (IP) adreses, kuras mainās ik reizi, kad tiek izveidots jauns savienojums ar internetu. Vācijas federālo institūciju pārvaldītās vietnes reģistrēja un glabāja dinamiskās IP adreses, lai novērstu kiberuzbrukumus un vajadzības gadījumā uzsāktu kriminālprocesu. Tikai interneta pakalpojumu sniedzēja, kuru izmantoja *Breyer* kungs, rīcībā bija papildu nepieciešamā informācija, lai viņu identificētu.

EST uzskatīja, ka dinamiskā IP adrese, ko tiešsaistes multivides pakalpojumu sniedzējs reģistrē, personai piekļūstot vietnei, kuru pakalpojuma sniedzējs ir padarījis pieejamu sabiedrībai, ir personas dati, ja tikai trešās personas, šajā gadījumā – interneta pakalpojumu sniedzēja, rīcībā ir papildu dati, kas nepieciešami personas identificēšanai[165]. Tā nosprieda, ka, lai informācija būtu kvalificējama kā personas dati, "netiek prasīts, lai visa informācija, kas ļauj identificēt attiecīgo personu, atrastos tikai vienas personas rīcībā". Interneta pakalpojumu sniedzēja reģistrētas dinamiskas IP adreses lietotājus dažās situācijās var ļaut identificēt, piemēram, kriminālprocesa ietvaros kiberuzbrukumu gadījumā, izmantojot citu personu palīdzību[166]. Atbilstoši EST teiktajam, ja pakalpojumu sniedzēja rīcībā "ir tiesiski līdzekļi, kas tam ļauj likt identificēt attiecīgo personu, izmantojot šīs personas interneta piekļuves pakalpojumu sniedzēja rīcībā esošo papildu informāciju", tas ir "līdzeklis, kas saprātīgi var tikt izmantots, lai identificētu attiecīgo personu". Līdz ar to šādi dati ir uzskatāmi par personas datiem.

EP tiesību aktos identificējamība tiek saprasta līdzīgi. Modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā ir līdzīgs apraksts: jēdziens "identificējams" attiecas ne tikai uz personas civilo vai tiesisko identitāti kā tādu, bet arī uz to, kas var ļaut vienu personu "individualizēt" vai izdalīt no citām, un tā rezultātā iespējams izturēties pret šo personu atšķirīgi. Šo "individualizēšanu" var veikt, piemēram, atsaucoties konkrēti uz personu, uz ierīci vai ierīču kombināciju (datoru, mobilo tālruni, fotokameru, spēļu ierīcēm u. tml.), kas piesaistītas identifikācijas numuram,

164 EST 2016. gada 19. oktobra spriedums lietā C-582/14 *Patrick Breyer pret Vācijas Federatīvo Republiku*, 47.–48. punkts.

165 Iepriekšējā Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti, 2. panta a) punkts.

166 EST 2011. gada 24. novembra spriedums lietā C-70/10 *Scarlet Extended SA pret Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 47.–48. punkts.

pseidonīmam, biometriskiem vai ģenētiskiem datiem, atrašanās vietas datiem, IP adresei vai citam identifikatoram[167]. Indivīds netiek uzskatīts par "identificējamu", ja personas identificēšanai ir nepieciešams nesamērīgs laiks, pūles vai resursi, piemēram, ja datu subjekta identificēšanai būtu nepieciešams veikt pārāk sarežģītas, ilgas un dārgas darbības. Laika, pūļu vai resursu nepamatotība ir jāvērtē katrā gadījumā atsevišķi, ņemot vērā tādus faktorus kā apstrādes mērķis, identifikācijas izmaksas un ieguvumi, pārziņa tips un izmantotā tehnoloģija[168].

Runājot par personas datu glabāšanas vai izmantošanas veidu, ir svarīgi atzīmēt, ka tas nav būtiski datu aizsardzības tiesību aktu piemērojamībai. Rakstveida vai mutiska komunikācija var saturēt personas datus, kā arī attēlus[169], tostarp videonovērošanas sistēmas (*CCTV*) kadrus[170] vai skaņu[171]. Elektroniski ierakstīta informācija un informācija uz papīra arī var būt personas dati. Pat cilvēku audu šūnu paraugi, kas reģistrē personas DNS, var būt avoti, no kuriem var iegūt biometriskos datus[172], ja vien dati attiecas uz indivīda iedzimtām vai iegūtām ģenētiskām īpašībām, sniedz unikālu informāciju par indivīda veselību vai fizioloģiju un tiek iegūti šīs personas bioloģiskā parauga analīzes rezultātā[173].

Anonimizācija

Saskaņā ar glabāšanas ierobežojuma principu, kas ietverts gan VDAR, gan modernizētajā Konvencijā Nr. 108 (plašāk aplūkota 3. nodaļā), dati jāglabā "veidā, kas pieļauj datu subjektu identifikāciju ne ilgāk kā nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā"[174]. Rezultātā dati būtu jādzēš vai jāpadara anonīmi, ja pārzinis

167 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 18. punkts.

168 Turpat, 17. punkts.

169 ECT 2004. gada 24. jūnija spriedums lietā *Von Hannover pret Vāciju*, Nr. 59320/00; ECT 2005. gada 11. janvāra spriedums lietā *Sciacca pret Itāliju*, Nr. 50774/99; EST 2014. gada 11. decembra spriedums lietā C-212/13 *František Ryneš pret Úřad pro ochranu osobních údajů*.

170 ECT 2003. gada 28. janvāra spriedums lietā *Peck pret Apvienoto Karalisti*, Nr. 44647/98; ECT 2010. gada 5. oktobra spriedums lietā *Köpke pret Vāciju* (dec.), Nr. 420/07; EDAU (2010), *EDAU videonovērošanas vadlīnijas*, 2010. gada 17. marts.

171 ECT 2001. gada 25. septembra spriedums lietā *P.G. un J.H. pret Apvienoto Karalisti*, Nr. 44787/98, 59.–60. punkts; ECT 2005. gada 20. decembra spriedums lietā *Wisse pret Franciju*, Nr. 71611/01 (franču valodas versija).

172 Skatīt arī 29. panta darba grupas (2007) *Atzinumu 4/2007 par "personas datu" jēdzienu*, WP136, 2007. gada 20. jūnijs, 9. lpp.; Eiropas Padomes Ministru komitejas Ieteikumu Rec(2006)4 dalībvalstīm par cilvēka izcelsmes bioloģisko materiālu izpēti, 2006. gada 15. marts.

173 Vispārīgā datu aizsardzības regula, 4. panta 13. punkts.

174 Turpat, 5. panta 1. punkta e) apakšpunkts, modernizētā Konvencija Nr. 108, 5. panta 4. punkta e) apakšpunkts.

vēlas tos uzglabāt pēc tam, kad tie vairs nav nepieciešami un vairs nekalpo sākotnējam mērķim.

Datu anonimizācijas process nozīmē, ka visi identificējošie elementi tiek izslēgti no personas datu kopas, lai datu subjekts vairs nebūtu identificējams[175]. Savā Atzinumā 05/2014 29. panta darba grupa analizē dažādu anonimizācijas paņēmienu efektivitāti un robežas[176]. Tā atzīst šādu paņēmienu iespējamo vērtību, bet uzsver, ka noteikti paņēmieni ne vienmēr darbojas visos gadījumos. Lai attiecīgajā situācijā rastu optimālu risinājumu, katrā atsevišķā gadījumā ir jālemj par piemērotu anonimizācijas procesu. Neatkarīgi no izmantotās tehnikas identifikācija ir jānovērš neatgriezeniski. Tas nozīmē, ka, lai datus anonimizētu, informācijā nedrīkst atstāt nevienu elementu, kas, pieliekot pamatotas pūles, varētu palīdzēt atkārtoti identificēt attiecīgo(-ās) personu(-as)[177]. Atkārtotas identifikācijas risku var novērtēt, ņemot vērā "nepieciešamo laiku, pūles vai resursus, ievērojot datu raksturu, to izmantošanas kontekstu, pieejamās atkārtotas identifikācijas tehnoloģijas un saistītās izmaksas"[178].

Kad dati ir veiksmīgi anonimizēti, tie vairs nav personas dati, un tiesību aktus par datu aizsardzību nepiemēro.

Ar VDAR paredz, ka personai vai organizācijai, kas kontrolē personas datu apstrādi, nevar uzlikt par pienākumu uzturēt, iegūt vai apstrādāt papildu informāciju, lai identificētu datu subjektu tikai un vienīgi regulas ievērošanas nolūkā. Tomēr šim noteikumam ir ievērojams atbrīvojums: ja datu subjekts piekļuves, labošanas, dzēšanas, apstrādes un datu pārnesamības tiesību īstenošanas nolūkā sniedz pārzinim papildu informāciju, kas ļauj viņu identificēt, tad dati, kas iepriekš tikuši anonimizēti, atkal kļūst par personas datiem[179].

Pseidonimizācija

Personīgā informācija satur atribūtus, piemēram, vārdu, dzimšanas datumu, dzimumu, adresi vai citus elementus, kas varētu ļaut identificēt. Personas datu pseidonimizācijas process nozīmē, ka šos atribūtus aizstāj ar pseidonīmu.

175 Vispārīgā datu aizsardzības regula, 26. apsvērums.

176 29. panta darba grupa (2014), *Atzinums 05/2014 par anonimizācijas metodēm*, WP216, 2014. gada 10. aprīlis.

177 Vispārīgā datu aizsardzības regula, 26. apsvērums.

178 Eiropas Padomes Konvencijas Nr. 108 komitejas (2017) *Vadlīnijas personu aizsardzībai attiecībā uz personas datu apstrādi lielo datu pasaulē*, 2017. gada 23. janvāris, 6.2. punkts.

179 Vispārīgā datu aizsardzības regula, 11. pants.

ES tiesību aktos pseidonimizācija definēta kā "personas datu apstrāde, ko veic tādā veidā, lai personas datus vairs nav iespējams saistīt ar konkrētu datu subjektu bez papildu informācijas izmantošanas, ar noteikumu, ka šāda papildu informācija tiek turēta atsevišķi un tai piemēro tehniskus un organizatoriskus pasākumus, lai nodrošinātu, ka personas dati netiek saistīti ar identificētu vai identificējamu fizisku personu"[180]. Pretēji anonimizētiem datiem pseidonimizētie dati joprojām ir personas dati, un tāpēc uz tiem attiecas datu aizsardzības tiesību akti. Lai arī pseidonimizācija var samazināt riskus datu subjektu drošībai, tā joprojām ietilpst VDAR piemērošanas jomā.

VDAR atzīst dažādus pseidonimizēšanas lietojumus kā piemērotu tehnisko pasākumu datu aizsardzības uzlabošanai, un tā ir īpaši minēta datu apstrādes integrēšanas un drošības nolūkiem[181]. Tā ir arī piemērots aizsardzības līdzeklis, ko var izmantot, apstrādājot personas datus citiem mērķiem, nevis tiem, kam tie sākotnēji tika vākti[182].

Pseidonimizācija nav skaidri minēta **EP** modernizētās Konvencijas Nr. 108. juridiskajā definīcijā. Tomēr modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā ir skaidri noteikts, ka "pseidonīma vai jebkura digitālā identifikatora/digitālās identitātes izmantošana nerada datu anonimizāciju, jo datu subjektu joprojām var identificēt vai individualizēt"[183]. Viens no datu pseidonimizācijas veidiem ir datu šifrēšana. Kad dati ir pseidonimizēti, saite uz identitāti pastāv pseidonīma un atšifrēšanas atslēgas veidā. Bez šādas atslēgas ir grūti identificēt pseidonimizētus datus. Tomēr personām, kurām ir tiesības izmantot atšifrēšanas atslēgu, atkārtota identifikācija ir vienkārši izdarāma. Īpaši jānodrošinās pret to, ka nepilnvarotas personas izmanto šifrēšanas atslēgas. Tāpēc "[p]seidonimizētus datus (..) uzskata par personas datiem (..)", uz kuriem attiecas modernizētā Konvencija Nr. 108[184].

Autentifikācija

Tā ir procedūra, ar kuru persona var pierādīt, ka tai ir noteikta identitāte un/vai tā ir pilnvarota veikt konkrētas darbības, piemēram, iekļūt drošības zonā vai izņemt naudu no bankas konta. Autentifikāciju var panākt, salīdzinot biometriskos datus, piemēram, fotoattēlu vai pirkstu nospiedumus pasē, ar datiem, kurus pati persona

180 Turpat, 4. panta 5. punkts.

181 Turpat, 25. panta 1. punkts.

182 Turpat, 6. panta 4. punkts.

183 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 18. punkts.

184 Turpat.

uzrāda, piemēram, imigrācijas kontrolē[185], vai pieprasot informāciju, kas ir jāzina tikai personai ar noteiktu identitāti vai pilnvarām, piemēram, personas identifikācijas numuru (PIN) vai paroli, vai pieprasot uzrādīt noteiktu marķieri, kam vajadzētu būt tikai tās personas rīcībā, kurai ir noteikta identitāte vai pilnvaras, piemēram, īpašu čipkarti vai bankas seifa atslēgu. Papildus parolēm vai čipkartēm, elektroniskie paraksti, dažkārt kopā ar PIN, ir instruments, kas īpaši spēj identificēt un autentificēt personu elektroniskajā komunikācijā.

2.1.2. Īpašu kategoriju personas dati

Saskaņā ar ES un **EP tiesību aktiem** pastāv īpašas personas datu kategorijas, kuru rakstura dēļ apstrādē var tikt radīts risks datu subjektiem un kurām vajadzīga pastiprināta aizsardzība. Uz šādiem datiem attiecas aizlieguma princips, un pastāv ierobežots skaits nosacījumu, saskaņā ar kuriem šāda apstrāde ir likumīga.

Saskaņā ar modernizēto Konvenciju Nr. 108 (6. pants) un VDAR (9. pants) par sensitīviem datiem uzskata šādas kategorijas:

- personas datus, kas atklāj rasi vai etnisko izcelsmi;
- personas datus, kas atklāj politiskos uzskatus, reliģisko vai citu pārliecību, tostarp filozofisko pārliecību;
- personas datus, kas atklāj dalību arodbiedrībās;
- ģenētiskos datus un biometriskos datus, lai veiktu fiziskas personas unikālu identifikāciju;
- personas datus par veselību, dzimumdzīvi vai seksuālo orientāciju.

Piemērs. Lieta *Bodil Lindqvist*[186] skāra norādes tīmekļa vietnē uz dažādām personām, izmantojot vārdu vai citus līdzekļus, piemēram, tālruņa numuru vai informāciju par šo personu vaļaspriekiem. EST uzskatīja, ka "norāde uz faktu, ka persona ir guvusi pēdas savainojumu un atrodas daļējā slimības atvaļinājumā, ir personas dati par veselības stāvokli"[187].

185 Turpat, 56.–57. punkts.

186 EST 2003. gada 6. novembra spriedums lietā C-101/01 *Kriminālprocess pret Bodil Lindqvist*, 51. punkts.

187 Iepriekšējā Direktīva 95/46/EK, 8. panta 1. punkts, tagad Vispārīgā datu aizsardzības regula, 9. panta 1. punkts.

Personas dati par sodāmību un pārkāpumiem

Modernizētajā Konvencijā Nr. 108 personas datu īpašo kategoriju sarakstā ir iekļauti personas dati, kas attiecas uz pārkāpumiem, kriminālprocesiem un sodāmību, kā arī saistītajiem drošības pasākumiem[188]. VDAR ietvaros personas dati, kas attiecas uz sodāmību un pārkāpumiem vai ar tiem saistītajiem drošības pasākumiem, kā tādi nav minēti īpašo kategoriju datu sarakstā, bet tiek aplūkoti atsevišķā pantā. VDAR 10. pantā noteikts, ka šādus datus var apstrādāt tikai "oficiālas iestādes kontrolē vai tad, ja apstrādi atļauj Savienības vai dalībvalsts tiesību akti, paredzot atbilstošas garantijas datu subjektu tiesībām un brīvībām". No otras puses, visaptverošus reģistrus, kas satur informāciju par sodāmību, var uzglabāt tikai īpašu oficiālu iestāžu kontrolē[189]. ES personas datu apstrādi tiesībaizsardzības jomā regulē īpašs tiesību instruments – Direktīva (ES) 2016/680[190]. Direktīvā paredzēti īpaši datu aizsardzības noteikumi, kas ir saistoši kompetentajām iestādēm, apstrādājot personas datus, jo īpaši lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus un sauktu pie atbildības par tiem (skatīt 8.2.1. iedaļu).

2.2. Datu apstrāde

Svarīgākie aspekti

- "Datu apstrāde" attiecas uz jebkādām darbībām, kas tiek veiktas ar personas datiem.
- Termins "apstrāde" ietver automatizētu un neautomatizētu apstrādi.
- Saskaņā ar ES tiesību aktiem "apstrāde" attiecas arī uz manuālu apstrādi strukturētās kartotēkās.
- Saskaņā ar EP tiesību aktiem jēdziena "apstrāde" nozīmi var paplašināt ar valsts tiesību aktiem, iekļaujot tajā manuālu apstrādi.

188 Modernizētā Konvencija Nr. 108, 6. panta 1. punkts.

189 Vispārīgā datu aizsardzības regula, 10. pants

190 Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Direktīva (ES) 2016/680 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI, OV 2016 L 119.

2.2.1. Datu apstrādes jēdziens

Personas datu apstrādes jēdziens ir visaptverošs **gan ES, gan EP tiesību aktos**: "personas datu apstrāde (..) ir jebkura darbība (..), piemēram, [personas datu] vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana"[191]. Modernizētajā Konvencijā Nr. 108 definīcija papildināta ar personas datu saglabāšanu[192].

Piemērs. Lietā *František Ryneš*[193] *Ryneš* kungs, izmantojot mājas videonovērošanas sistēmu, ko viņš bija uzstādījis sava īpašuma aizsardzībai, iemūžināja attēlā divas personas, kuras izsita logus viņa mājoklī. EST secināja, ka videonovērošana, ietverot personas datu ierakstīšanu un glabāšanu, ir automatizēta datu apstrāde, kas ietilpst ES datu aizsardzības tiesību aktu darbības jomā.

Piemērs. Lietā *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce pret Salvatore Manni*[194] *Manni* kungs lūdza izņemt no reitingu kompānijas reģistra viņa personas datus, kas viņu saistīja ar nekustamā īpašuma uzņēmuma likvidāciju, tādējādi negatīvi ietekmējot reputāciju. EST sprieda, ka, "minēto informāciju ievadot un saglabājot reģistrā un attiecīgā gadījumā pēc pieprasījuma to paziņojot trešām personām, iestāde, kas ir atbildīga par reģistru, veic "personas datu apstrādi", par kuru tā ir "pārzinis"".

Piemērs. Darba devēji vāc un apstrādā datus par saviem darbiniekiem, tostarp informāciju par viņu algām. Viņu darba līgumi nodrošina likumīgu pamatu likumīgai rīcībai.

Darba devējiem jānosūta nodokļu iestādēm informācija par darbinieku algām. Šī datu pārsūtīšana arī būs "apstrāde" šā termina izpratnē modernizētajā Konvencijā Nr. 108 un VDAR. Tomēr šādas informācijas izpaušanas juridiskais

191 Vispārīgā datu aizsardzības regula, 4. panta 2. punkts. Skatīt arī modernizētās Konvencijas Nr. 108 2. panta b) punktu.

192 Modernizētā Konvencija Nr. 108, 2. panta b) punkts.

193 EST 2014. gada 11. decembra spriedums lietā C-212/13 *František Ryneš pret Úřad pro ochranu osobních údajů*, 25. punkts.

194 EST 2017. gada 9. marta spriedums lietā C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce pret Salvatore Manni*, 35. punkts.

pamats nav darba līgumi. Apstrādes darbībām, kuru rezultātā darba devējs nodokļu iestādēm pārsūta informāciju par algām, nepieciešams papildu juridiskais pamats. Šis juridiskais pamats parasti ir atrodams valstu nodokļu likumos. Bez šādiem noteikumiem un cita likumīga pamata apstrādei šāda personas datu pārsūtīšana būtu nelikumīga apstrāde.

2.2.2. Automatizēta datu apstrāde

Datu aizsardzība saskaņā ar modernizēto Konvenciju Nr. 108 un VDAR pilnībā attiecināma uz automatizētu datu apstrādi.

Saskaņā ar **ES tiesību aktiem** automatizēta datu apstrāde skar darbības, kas personas datiem "pilnībā vai daļēji veikta ar automatizētiem līdzekļiem"[195]. Modernizētajā Konvencijā Nr. 108 ir iekļauta līdzīga definīcija[196]. Praktiski tas nozīmē, ka uz jebkuru personas datu apstrādi, izmantojot automatizētus līdzekļus, piemēram, personālo datoru, mobilo ierīci vai maršrutētāju, attiecas gan ES, gan EP datu aizsardzības noteikumi.

Piemērs. Lieta *Bodil Lindqvist*[197] attiecās uz norādi tīmekļa vietnē uz dažādām personām, izmantojot vārdu vai citus līdzekļus, piemēram, tālruņa numuru vai informāciju par šo personu vaļaspriekiem. EST sprieda, ka "darbība, kuras ietvaros interneta mājaslapā tiek norādītas vairākas personas un tās identificētas vai nu norādot viņu uzvārdu, vai citā veidā, piemēram, norādot viņu tālruņa numuru vai informāciju par viņu darba apstākļiem un vaļaspriekiem, ir uzskatāma par "personas datu apstrādi pilnībā vai daļēji ar automatizētiem līdzekļiem" Direktīvas 95/46/EK 3. panta 1. punkta izpratnē"[198].

Piemērs. Lietā *Google Spain SL, Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González*[199] *González* kungs pieprasīja noņemt vai izmainīt saiti starp viņa vārdu *Google* meklētājā un divām laikrakstu lapām ar sludinājumiem par nekustamā īpašuma izsoli sociālās apdrošināšanas parādu piedziņai. EST paziņoja, ka, "automatizēti, konstanti

195 Vispārīgā datu aizsardzības regula, 2. panta 1. punkts un 4. panta 2. punkts.

196 Modernizētā Konvencija Nr. 108, 2. panta b) un c) punkts, modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 21. punkts.

197 EST 2003. gada 6. novembra spriedums lietā C-101/01 *Kriminālprocess pret Bodil Lindqvist*, 27. punkts.

198 Vispārīgā datu aizsardzības regula, 2. panta 1. punkts.

199 EST 2014. gada 13. maija spriedums lietā C-131/12 *Google Spain SL un Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC].

un sistemātiski izmantojot internetu tajā publicētās informācijas meklēšanai, meklētājprogrammas pakalpojumu sniedzējs "vāc" šādus datus, kurus tas pēc tam "atgūst", "reģistrē" un "organizē" savu indeksācijas programmu ietvaros, "saglabā" savos serveros un attiecīgajā gadījumā "atklāj" vai "padara tos pieejamus" saviem lietotājiem to meklējumu rezultātu sarakstu formā"[200]. EST secināja, ka šādas darbības ir "apstrāde", "un nav svarīgi, ka meklētājprogrammas pakalpojumu sniedzējs piemēro tās pašas darbības cita veida informācijai un nenošķir šo informāciju no personas datiem".

2.2.3. Neautomatizēta datu apstrāde

Arī datu manuālai apstrādei nepieciešama datu aizsardzība.

Datu aizsardzība saskaņā ar ES tiesību aktiem nekādā gadījumā neattiecas tikai uz automatizētu datu apstrādi. Attiecīgi saskaņā ar ES tiesību aktiem datu aizsardzība attiecas uz personas datu apstrādi manuālā kartotēkā, tas ir, īpaši strukturētā papīra kartotēkā[201]. Strukturēta kartotēka ir tāda, kurā personas dati tiek klasificēti, padarot tos pieejamus atbilstoši noteiktiem kritērijiem. Piemēram, ja darba devējs uztur papīra kartotēku ar nosaukumu "darbinieku atvaļinājums", kas satur visu informāciju par atvaļinājumiem, ko darbinieki ir izņēmuši pēdējā gada laikā, un tā ir sakārtota alfabēta secībā, datne ir manuāla kartotēka, uz kuru attiecas ES dati aizsardzības noteikumi. Šādas datu aizsardzības paplašināšanas iemesls ir tāds, ka:

- papīra dokumentus var strukturēt veidā, kas ļauj ātri un viegli atrast informāciju;
- personas datu glabāšana strukturētās papīra kartotēkās ļauj viegli apiet likumos noteiktos ierobežojumus automatizētai datu apstrādei[202].

Saskaņā ar **EP tiesību aktiem** automātiskās apstrādes definīcijā atzīts, ka starp automatizētām darbībām var būt nepieciešami daži personas datu manuālas izmantošanas posmi[203]. Modernizētās Konvencijas Nr. 108 2. panta c) punktā noteikts, ka "ja neizmanto automatizētu apstrādi, datu apstrāde ir darbība vai darbību kopums, kas veikts ar personas datiem strukturētā šādu datu kopā, kas ir pieejams vai izgūstams saskaņā ar īpašiem kritērijiem".

200 Turpat, 28. punkts.

201 Vispārīgā datu aizsardzības regula, 2. panta 1. punkts.

202 Vispārīgā datu aizsardzības regula, 15. apsvērums.

203 Modernizētā Konvencija Nr. 108, 2. panta b) un c) punkts.

2.3. Personas datu lietotāji

Svarīgākie aspekti

- Tas, kurš nosaka citu personu personas datu apstrādes līdzekļus un mērķus, saskaņā ar datu aizsardzības tiesību aktiem ir "pārzinis". Ja vairākas personas pieņem šo lēmumu kopā, viņi var būt "kopīgi pārziņi".
- "Apstrādātājs" ir fiziska vai juridiska persona, kura apstrādā personas datus pārziņa vārdā.
- Apstrādātājs kļūst par pārzini, ja tas pats nosaka datu apstrādes līdzekļus un mērķus.
- Jebkura persona, kurai tiek izpausti personas dati, ir "saņēmējs".
- "Trešā persona" ir fiziska vai juridiska persona, kura nav datu subjekts, pārzinis, apstrādātājs un personas, kuras ir pilnvarotas apstrādāt personas datus tiešā pārziņa vai apstrādātāja pakļautībā.
- Piekrišanai kā juridiskam pamatam personas datu apstrādei ir jābūt sniegtai no brīvas gribas, apzinātai, konkrētai un nepārprotami jānorāda uz vēlmēm ar skaidru apstiprinošu aktu, kas apliecina piekrišanu apstrādei.
- Lai apstrādātu īpašas datu kategorijas, pamatojoties uz piekrišanu, ir nepieciešama nepārprotama piekrišana.

2.3.1. Pārziņi un apstrādātāji

Vissvarīgākās sekas pārziņa vai apstrādātāja statusam ir juridiskā atbildība par attiecīgo datu aizsardzības tiesību aktos noteikto pienākumu izpildi. Privātajā sektorā tā parasti ir fiziska vai juridiska persona, valsts sektorā tā parasti ir iestāde. Starp datu pārzini un datu apstrādātāju ir būtiska atšķirība: pirmā ir fiziska vai juridiska persona, kura nosaka apstrādes mērķus un līdzekļus, savukārt otrā ir fiziska vai juridiska persona, kura apstrādā datus pārziņa vārdā, ievērojot stingrus norādījumus. Parasti datu apstrādi kontrolē datu pārzinis un uzņemas par to atbildību, tostarp juridisko atbildību. Tomēr līdz ar datu aizsardzības noteikumu reformu apstrādātājiem tagad ir pienākums ievērot daudzas prasības, kas attiecas uz pārziņiem. Piemēram, saskaņā ar VDAR apstrādātājiem jāreģistrē visu kategoriju apstrādes darbības, lai pierādītu savu saistību izpildi saskaņā ar regulu[204]. Apstrādātājiem ir arī pienākums īstenot attiecīgus tehniskos un organizatoriskos pasākumus, lai nodrošinātu apstrādes drošību[205],

204 Vispārīgā datu aizsardzības regula, 30. panta 2. punkts.

205 Turpat, 32. pants.

noteiktās situācijās iecelt datu aizsardzības speciālistu[206] un informēt pārzini par datu aizsardzības pārkāpumiem[207].

Personas spēja izlemt un noteikt apstrādes mērķi un līdzekļus būs atkarīga no lietas faktiskajiem elementiem vai apstākļiem. Atbilstoši VDAR sniegtai pārziņa definīcijai pārzinis var būt gan fiziskas, gan juridiskas personas vai citas struktūras. Tomēr 29. panta darba grupa ir uzsvērusi, ka, lai nodrošinātu indivīdiem stabilāku organizāciju viņu tiesību īstenošanai, "priekšroka būtu jādod uzņēmumam vai struktūrai kā tādai kā pārzinim, nevis konkrētai personai uzņēmumā vai struktūrā"[208]. Piemēram, uzņēmums, kas pārdod veselības aprūpes preces praktizējošiem ārstiem, ir visu praktizējošo ārstu izplatīšanas saraksta sastādīšanas un uzturēšanas pārzinis noteiktā apgabalā, nevis pārdošanas vadītājs, kurš šo sarakstu faktiski izmanto un uztur.

Piemērs. Kad uzņēmuma *Sunshine* mārketinga nodaļa plāno apstrādāt datus tirgus izpētei, tieši uzņēmums *Sunshine*, nevis mārketinga nodaļas darbinieki, būs šādas apstrādes pārzinis. Mārketinga nodaļa nevar būt pārzinis, jo tai nav savas atsevišķas identitātes.

Fiziskas personas var būt pārziņi gan saskaņā ar ES, gan EP tiesību aktiem. Tomēr, apstrādājot datus par citiem attiecībā uz tīri personīgām vai mājsaimniecības darbībām, uz privātpersonām neattiecas VDAR un modernizētās Konvencijas Nr. 108 noteikumi un tās netiek uzskatītas par pārziņiem[209]. Personu, kura uztur korespondenci, personīgo dienasgrāmatu, kurā aprakstīti incidenti ar draugiem un kolēģiem un ģimenes locekļu medicīniskā informācija, var atbrīvot no datu aizsardzības noteikumiem, jo šīs darbības ir tīri personiskas vai tikai mājsaimniecības darbības. VDAR arī precizēts, ka personiskās vai mājsaimniecības darbībās varētu ietvert arī sociālo tīklošanos un aktivitātes tiešsaistē, ja tās tiek veiktas šādu darbību kontekstā[210]. Savukārt datu aizsardzības noteikumi pilnībā attiecas uz pārziņiem un

206 Turpat, 37. pants.

207 Turpat, 33. panta 2. punkts.

208 29. panta darba grupa (2010), *Atzinums 1/2010 par "personas datu apstrādātāja" un "apstrādātāja" jēdzienu*, WP 169, Brisele, 2010. gada 16. februāris.

209 Vispārīgā datu aizsardzības regula, 18. apsvērums un 2. panta 2. punkta c) apakšpunkts; modernizētā Konvencija Nr. 108, 3. panta 2. punkts.

210 Vispārīgā datu aizsardzības regula, 18. apsvērums.

apstrādātājiem, kuri nodrošina līdzekļus personas datu apstrādei personiskām vai mājsaimniecības darbībām (piemēram, sociālās tīklošanās platformas).[211]

Iedzīvotāju piekļuve internetam un iespēja izmantot e-komercijas platformas, sociālos tīklus un emuāru veidošanas vietnes, lai apmainītos ar personisko informāciju par sevi un citām personām, arvien apgrūtina personīgas apstrādes nodalīšanu no apstrādes, kas nav personīga[212]. Tas, vai darbības ir tīri personiskas vai mājsaimniecības, ir atkarīgs no apstākļiem[213]. Darbībām, kam ir profesionāli vai komerciāli aspekti, nevar piemērot uz mājsaimniecībām attiecināmo atbrīvojumu[214]. Tādējādi, ja datu apstrādes mērogs un biežums liecina par profesionālu vai pilna laika darbību, privātpersonu var uzskatīt par pārzini. Papildus apstrādes darbības profesionālajam vai komerciālajam raksturam vēl viens faktors, kas jāņem vērā, ir, vai personas dati ir pieejami lielam skaitam personu, kuras acīmredzami ir ārpus personas privātās sfēras. Judikatūrā saskaņā ar Datu aizsardzības direktīvu ir konstatēts, ka tiesību akti datu aizsardzības jomā ir piemērojami, ja privātpersona, izmantojot internetu, publiskā tīmekļa vietnē publicē datus par citiem. EST vēl nav pieņēmusi lēmumu par līdzīgiem faktiem saskaņā ar VDAR, kurā sniedz vairāk norāžu par tēmām, ko varētu uzskatīt par ārpus datu aizsardzības tiesību aktu darbības jomas esošām atbilstoši "mājsaimniecības atbrīvojumam", piemēram, sociālo mediju izmantošanu personīgos nolūkos.

Piemērs. Lieta *Bodil Lindqvist*[215] skāra norādes tīmekļa vietnē uz dažādām personām, izmantojot vārdu vai citus līdzekļus, piemēram, tālruņa numuru vai informāciju par šo personu vaļaspriekiem. EST noteica, ka "darbība, kuras ietvaros interneta mājaslapā tiek norādītas vairākas personas un tās identificētas vai nu norādot viņu uzvārdu, vai citā veidā", ir uzskatāma par "personas datu apstrādi pilnībā vai daļēji ar automatizētiem līdzekļiem" Datu aizsardzības direktīvas 3. panta 1. punkta izpratnē[216].

211 Turpat, 18. apsvērums; modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 29. punkts.

212 Skatīt 29. panta darba grupas paziņojumu attiecībā uz diskusijām par datu aizsardzības reformu pakotni (2013), *2. pielikums: Priekšlikumi un grozījumi attiecībā uz atbrīvojumiem personiska vai mājsaimnieciska rakstura darbībām* , 2013. gada 27. februāris.

213 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 28. punkts.

214 Skatīt Vispārīgās datu aizsardzības regulas 18. apsvērumu un modernizētās Konvencijas Nr. 108 skaidrojošā ziņojuma 27. punktu.

215 EST 2003. gada 6. novembra spriedums lietā C-101/01 *Kriminālprocess pret Bodil Lindqvist*.

216 Turpat, 27. punkts; iepriekšējā Direktīva 95/46/EK, 3. panta 1. punkts, tagad Vispārīgā datu aizsardzības regula, 2. panta 1. punkts.

Šāda personas datu apstrāde neietilpst tīri personisku vai mājsaimniecības darbību ietvaros, uz kurām neattiecas ES datu aizsardzības noteikumi, jo šis izņēmums "(..) jāinterpretē tādējādi, ka tas attiecas vienīgi uz darbībām, kas ietilpst personu privātajā vai ģimenes dzīvē, kā tas acīmredzami nav gadījumā, kad personas dati tiek apstrādāti, tos publicējot internetā, un tādējādi šie dati tiek padarīti pieejami nenoteiktam personu skaitam"[217].

Saskaņā ar EST viedokli ES datu aizsardzības tiesību akti var attiekties arī uz privāti uzstādītas drošības kameras vizuālajiem ierakstiem noteiktos apstākļos.

Piemērs. Lietā *František Ryneš*[218] *Ryneš* kungs, izmantojot mājas videonovērošanas sistēmu, ko viņš bija uzstādījis sava īpašuma aizsardzībai, iemūžināja attēlā divas personas, kuras izsita logus viņa mājoklī. Pēc tam ieraksts tika nodots policijai un izmantots kriminālprocesā.

EST paziņoja, ka "[c]iktāl tāda videonovērošana (..) kaut vai daļēji aptver publisko telpu un tādēļ ir vērsta uz personas, kura ar šo līdzekli veic datu apstrādi, privātās sfēras ārpusi, to nevar uzskatīt par darbību tikai un vienīgi personiskām vai sadzīviskām vajadzībām (..)"[219].

Pārzinis

Saskaņā ar ES tiesību aktiem pārzinis tiek definēts kā persona, kura "viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus"[220]. Pārziņa lēmums nosaka, kāpēc un kā dati tiek apstrādāti.

Saskaņā ar EP tiesību aktiem modernizētajā Konvencijā Nr. 108 definē "pārzini" kā "fizisku vai juridisku personu, publisku institūciju, dienestu, aģentūru vai jebkuru citu struktūru, kurai vienai vai kopā ar citiem ir lēmumu pieņemšanas tiesības attiecībā uz datu apstrādi"[221]. Šādas lēmumu pieņemšanas pilnvaras attiecas uz apstrā-

217 EST 2003. gada 6. novembra spriedums lietā C-101/01 *Kriminālprocess pret Bodil Lindqvist*, 47. punkts.

218 EST 2014. gada 11. decembra spriedums lietā C-212/13 *František Ryneš pret Úřad pro ochranu osobních údajů*, 33. punkts.

219 Iepriekšējā Direktīva 95/46/EK, 3. panta 2. punkta otrais ievilkums, tagad Vispārīgā datu aizsardzības regula, 2. panta 2. punkta c) apakšpunkts.

220 Vispārīgā datu aizsardzības regula, 4. panta 7. punkts.

221 Modernizētā Konvencija Nr. 108, 2. panta d) punkts.

des mērķiem un līdzekļiem, kā arī uz apstrādājamo datu kategorijām un piekļuvi datiem[222]. Par to, vai šīs pilnvaras izriet no tiesiska nozīmējuma vai no faktiskajiem apstākļiem, jālemj katrā gadījumā atsevišķi[223].

Piemērs. Lietu *Google Spain*[224] ierosināja Spānijas pilsonis, kurš vēlējās no *Google* izņemt vecu laikraksta ziņojumu par viņa finanšu vēsturi.

EST tika jautāts, vai *Google* kā meklētājprogrammas operators ir datu "pārzinis" Datu aizsardzības direktīvas 2. panta d) punkta izpratnē[225]. EST aplūkoja jēdziena "pārzinis" plašu definīciju, lai nodrošinātu "efektīvu un pilnīgu datu subjektu aizsardzību"[226]. EST konstatēja, ka meklētājprogrammas operators ir noteicis darbības mērķus un līdzekļus un sniedz tīmekļa vietnēs datus, kurus izvietojuši vietņu izdevēji un kuri ir pieejami jebkuram interneta lietotājam, veicot meklēšanu, pamatojoties uz datu subjekta vārdu[227]. Tādēļ EST lēma, ka *Google* ir uzskatāms par "pārzini"[228].

Ja pārzinis vai apstrādātājs ir reģistrēts ārpus ES, šim uzņēmumam rakstiski jāieceļ pārstāvis ES teritorijā[229]. VDAR uzsvērts, ka pārstāvis veic uzņēmējdarbību "vienā no tām dalībvalstīm, kur atrodas datu subjekti, kuru personas datus apstrādā saistībā ar preču vai pakalpojumu piedāvāšanu tiem vai kuru uzvedība tiek novērota"[230]. Ja pārstāvis nav iecelts, pret pašu pārzini vai apstrādātāju joprojām var celt tiesiskās prasības[231].

222 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 22. punkts

223 Turpat.

224 EST 2014. gada 13. maija spriedums lietā C-131/12 *Google Spain SL un Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC].

225 Vispārīgā datu aizsardzības regula, 4. panta 7. punkts; EST 2014. gada 13. maija spriedums lietā C-131/12 *Google Spain SL, Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 21. punkts.

226 EST 2014. gada 13. maija spriedums lietā C-131/12 *Google Spain SL un Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 34. punkts.

227 Turpat, 35.–40. punkts.

228 Turpat, 41. punkts.

229 Vispārīgā datu aizsardzības regula, 27. panta 1. punkts.

230 Turpat, 27. panta 3. punkts.

231 Turpat, 27. panta 5. punkts.

Kopīga kontrole

VDAR noteikts, ka tad, ja divi vai vairāki pārziņi kopīgi nosaka apstrādes mērķi un līdzekļus, tos uzskata par kopīgiem pārziņiem. Tas nozīmē, ka viņi kopā lemj veikt datu apstrādi kopīgam mērķim[232]. Modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā noteikts, ka **EP tiesību aktu** ietvaros ir iespējami arī vairāki pārziņi vai kopīgi pārziņi[233].

29. panta darba grupa norāda, ka kopējai kontrolei var būt dažādas formas un ka dažādu pārziņu dalība kontroles darbībās var būt nevienlīdzīga[234]. Šāda elastība ļauj apkalpot arvien sarežģītāku datu apstrādes realitāti[235]. Tādēļ kopīgiem pārziņiem īpašā nolīgumā jānosaka viņu atbildība par šajā regulā noteikto saistību izpildi[236].

Kopīga kontrole rada kopīgu atbildību par apstrādes darbībām[237]. Saskaņā ar **ES tiesību aktiem** tas nozīmē, ka katrs pārzinis vai apstrādātājs var būt pilnībā atbildīgs par visu kaitējumu, kas nodarīts apstrādes rezultātā kopējas kontroles ietvaros, lai nodrošinātu datu subjektam efektīvu kompensāciju[238].

> Piemērs. Datubāze par klientiem, kuri nepilda saistības, ko kopīgi pārvalda vairākas kredītiestādes, ir izplatīts kopīgas kontroles piemērs. Ja kāda persona pieprasa kredītlīniju bankā, kas ir viens no kopīgajiem pārziņiem, bankas pārbauda datubāzi, lai palīdzētu tām pieņemt apzinātus lēmumus par pieteikuma iesniedzēja kredītspēju.

Tiesību aktos nav skaidri noteikts, vai kopējai kontrolei ir nepieciešams, lai kopējais mērķis būtu vienāds visiem pārziņiem, vai arī pietiek, ja to mērķi tikai daļēji pārklājas. Pagaidām Eiropas mērogā nav pieejama atbilstoša judikatūra. Savā 2010. gada atzinumā par pārziņiem un apstrādātājiem 29. panta darba grupa norāda, ka kopīgajiem pārziņiem var būt kopīgi visi apstrādes mērķi un līdzekļi, kā arī tiem var

232 Turpat, 4. panta 7. punkts un 26. pants.

233 Modernizētā Konvencija Nr. 108, 2. panta d) punkts, modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 22. punkts.

234 29. panta darba grupa (2010), *Atzinums 1/2010 par "personas datu apstrādātāja" un "apstrādātāja" jēdzienu*, WP 169, Brisele, 2010. gada 16. februāris, 19. lpp.

235 Turpat.

236 Vispārīgā datu aizsardzības regula, 79. apsvērums.

237 Turpat, 21. punkts.

238 Turpat, 82. panta 4. punkts.

būt kopīgi tikai daži mērķi, līdzekļi vai to daļa[239]. Kamēr pirmais variants nozīmētu ļoti ciešas attiecības starp dažādiem dalībniekiem, pēdējais norādītu uz brīvākām attiecībām.

29. panta darba grupa atbalsta plašāku kopīgas kontroles jēdziena interpretāciju ar mērķi nodrošināt zināmu elastību, lai ņemtu vērā pašreizējās datu apstrādes realitātes pieaugošo sarežģītību[240]. Lieta, kurā iesaistīta Vispasaules Starpbanku finanšu telekomunikāciju sabiedrība (*SWIFT*), atspoguļo darba grupas nostāju.

Piemērs. Tā sauktajā *SWIFT* lietā Eiropas banku iestādes piesaistīja *SWIFT* sākotnēji kā apstrādātāju datu nosūtīšanai banku darījumu gaitā. *SWIFT* šādus banku darījumu datus, kas glabājas skaitļošanas pakalpojumu centrā Amerikas Savienotajās Valstīs (ASV), atklāja ASV Valsts kases departamentam bez nepārprotama Eiropas banku iestāžu, kas to piesaistīja, pieprasījuma. Novērtējot šīs situācijas likumību, 29. panta darba grupa nonāca pie secinājuma, ka Eiropas banku iestādes, kas izmanto *SWIFT*, kā arī pati *SWIFT* ir jāuzskata par kopīgiem pārziņiem, kuriem ir atbildība pret Eiropas klientiem attiecībā uz viņu datu izpaušanu ASV iestādēm[241].

Apstrādātājs

Apstrādātājs **saskaņā ar ES tiesību aktiem** ir definēts kā persona, kura apstrādā personas datus pārziņa vārdā[242]. Apstrādātājam uzticētās darbības var būt tikai ļoti konkrēts uzdevums vai konteksts, kā arī tās var būt diezgan vispārīgas un visaptverošas.

Saskaņā ar EP tiesību aktiem apstrādātājam ir tāda pati nozīme kā ES tiesību aktos[243].

Apstrādātāji ne tikai apstrādā datus citu uzdevumā, bet arī paši būs datu pārziņi saistībā ar apstrādi, ko viņi veic pašu mērķiem, piemēram, savu darbinieku administrēšanai, pārdošanas un klientu administrēšanai.

239 29. panta darba grupa (2010), *Atzinums 1/2010 par "personas datu apstrādātāja" un "apstrādātāja" jēdzienu*, WP 169, Brisele, 2010. gada 16. februāris, 19. lpp.

240 Turpat.

241 29. panta darba grupa (2006), *Atzinums 10/2006 par personas datu apstrādi, ko veic Vispasaules Starpbanku finanšu telekomunikāciju sabiedrība (SWIFT),* WP 128, Brisele, 2006. gada 22. novembris.

242 Vispārīgā datu aizsardzības regula, 4. panta 8. punkts.

243 Modernizētā Konvencija Nr. 108, 2. panta f) punkts.

Piemērs. Uzņēmums *Everready* specializējas datu apstrādē, administrējot cilvēkresursu datus citiem uzņēmumiem. Veicot šo funkciju, *Everready* ir apstrādātājs. Tomēr, ja *Everready* apstrādā savu darbinieku datus, tas ir datu apstrādes darbību pārzinis, pildot savus pienākumus kā darba devējs.

Attiecības starp pārzini un apstrādātāju

Kā redzējām, pārzinis tiek definēts kā tas, kurš nosaka apstrādes mērķus un līdzekļus. VDAR skaidri norādīts, ka apstrādātājs personas datus drīkst apstrādāt tikai saskaņā ar pārziņa norādījumiem, ja vien ES vai dalībvalsts tiesību aktos nav noteikts pienākums to darīt apstrādātājam[244]. Līgums starp pārzini un apstrādātāju ir būtisks viņu savstarpējo attiecību elements un ir juridiska prasība[245].

Piemērs. Uzņēmuma *Sunshine* direktors nolemj, ka uzņēmumam *Cloud*, kas ir mākoņdatošanas datu glabāšanas speciālists, vajadzētu pārvaldīt *Sunshine* klientu datus. Uzņēmums *Sunshine* joprojām ir pārzinis, savukārt uzņēmums *Cloud* ir tikai apstrādātājs, jo atbilstoši līgumam *Cloud* drīkst izmantot *Sunshine* uzņēmuma klientu datus tikai tiem mērķiem, kādus nosaka *Sunshine*.

Ja pilnvaras noteikt apstrādes veidus tiek deleģētas apstrādātājam, pārzinim tomēr jāspēj pienācīgi kontrolēt apstrādātāja lēmumus par apstrādes līdzekļiem. Vispārējo atbildību joprojām uzņemas pārzinis, kuram ir jāpārrauga apstrādātāji, lai pārliecinātos par viņu lēmumu atbilstību datu aizsardzības tiesību aktiem un pārziņa norādījumiem.

Turklāt, ja apstrādātājs neievēros pārziņa sniegtos datu apstrādes nosacījumus, apstrādātājs būs kļuvis par pārzini vismaz tādā mērā, kādā tiek pārkāpti pārziņa norādījumi. Tādējādi apstrādātājs, visticamāk, kļūs par pārzini, kurš rīkojas nelikumīgi. Savukārt sākotnējam pārzinim būs jāsniedz paskaidrojums, kā apstrādātājam bija iespējams pārkāpt tā pilnvaras[246]. Patiešām, 29. panta darba grupai ir tendence

244 Vispārīgā datu aizsardzības regula, 29. apsvērums.

245 Turpat, 28. panta 3. punkts.

246 Turpat, 82. panta 2. punkts.

pieņemt kopīgu kontroli šādos gadījumos, jo tā vislabāk nodrošina datu subjektu interešu aizsardzību[247].

Var rasties problēmas arī ar atbildības sadalījumu, ja pārzinis ir mazs uzņēmums, savukārt apstrādātājs ir liels korporatīvais uzņēmums, kas spēj diktēt savu pakalpojumu nosacījumus. Šādos apstākļos 29. panta darba grupa tomēr apgalvo, ka atbildības līmeni nedrīkst pazemināt ekonomiskās nelīdzsvarotības dēļ un ka jāsaglabā pārziņa jēdziena izpratne[248].

Skaidrības un pārredzamības nolūkā ziņas par pārziņa un apstrādātāja attiecībām jāreģistrē rakstiskā līgumā[249]. Līgumā jo īpaši jāietver apstrādes priekšmets, raksturs, mērķis un apstrādes ilgums, personas datu tips, kā arī datu subjektu kategorijas. Tajā ir jānosaka arī pārziņa un apstrādātāja pienākumi un tiesības, piemēram, prasības attiecībā uz konfidencialitāti un drošību. Šāda līguma neesamība ir pārziņa pienākuma sniegt rakstisku savstarpējās atbildības dokumentāciju pārkāpums, kā rezultātā var tikt piemērotas sankcijas. Ja kaitējums tiek nodarīts, rīkojoties ārpus pārziņa likumīgiem norādījumiem vai tos neievērojot, pie atbildības var saukt ne tikai pārzini, bet arī apstrādātāju[250]. Apstrādātājam jāreģistrē visu kategoriju apstrādes darbības, ko tas veic pārziņa vārdā[251]. Šie ieraksti ir jādara pieejami uzraudzības iestādei pēc tās pieprasījuma, jo gan pārzinim, gan apstrādātājam ar to ir jāsadarbojas, pildot savus uzdevumus[252]. Pārzinim un apstrādātājiem ir arī iespēja ievērot apstiprinātu rīcības kodeksu vai sertifikācijas mehānismu, lai apliecinātu viņu atbilstību VDAR prasībām[253].

Apstrādātāji var vēlēties deleģēt noteiktus uzdevumus papildu apakšapstrādātājiem. Juridiski tas ir pieļaujams, ja starp pārzini un apstrādātāju pastāv attiecīgi līguma nosacījumi, tostarp tas, vai ir nepieciešama pārziņa atļauja katrā atsevišķā gadījumā vai arī pietiek tikai ar informēšanu. VDAR ir noteikts, ka sākotnējais

247 29. panta darba grupa (2010), Atzinums 1/2010 par "personas datu apstrādātāja" un "apstrādātāja" jēdzienu, WP 169, Brisele, 2010. gada 16. februāris, 25. lpp.; 29. panta darba grupa (2006), *Atzinums 10/2006 par personas datu apstrādi, ko veic Vispasaules Starpbanku finanšu telekomunikāciju sabiedrība (SWIFT)*, WP 128, Brisele, 2006. gada 22. novembris.

248 29. panta darba grupa (2010), *Atzinums 1/2010 par "personas datu apstrādātāja" un "apstrādātāja" jēdzienu*, WP 169, Brisele, 2010. gada 16. februāris, 26. lpp.

249 Vispārīgā datu aizsardzības regula, 28. panta 3. un 9. punkts.

250 Turpat, 82. panta 2. punkts.

251 Turpat, 30. panta 2. punkts.

252 Turpat, 30. panta 4. punkts un 31. pants.

253 Turpat, 28. panta 5. punkts un 42. panta 4. punkts.

apstrādātājs ir pilnībā atbildīgs attiecībā pret pārzini, ja apakšapstrādātājs nepilda savus datu aizsardzības pienākumus[254].

Saskaņā ar EP tiesību aktiem pārziņa un apstrādātāja jēdzienu interpretācija, kā paskaidrots iepriekš, ir pilnībā piemērojama[255].

2.3.2. Saņēmēji un trešās personas

Atšķirība starp šīm divām personu vai vienību kategorijām, kas ieviestas ar Datu aizsardzības direktīvu, galvenokārt ir saistīta ar viņu attiecībām ar pārzini un attiecīgi ar viņu pilnvarām piekļūt pārziņa rīcībā esošajiem personas datiem.

"Trešā persona" ir persona, kura nav pārzinis vai apstrādātājs. Atbilstoši VDAR 4. panta 10. punktam trešā persona ir "fiziska vai juridiska persona, publiska iestāde, aģentūra vai struktūra, kura nav datu subjekts, pārzinis, apstrādātājs un personas, kuras pārziņa vai apstrādātāja tiešā pakļautībā ir pilnvarotas apstrādāt personas datus". Tas nozīmē, ka personas, kuras strādā organizācijā, kas nav pārzinis, pat ja tā pieder tai pašai grupai vai kontrolakciju sabiedrībai, būs (vai skaitīsies) "trešā persona". No otras puses, banku filiāles, kuras apstrādā klienta kontus tiešā galvenā biroja pakļautībā, nebūs "trešās personas"[256].

"Saņēmējs" ir plašāks termins nekā "trešā persona". VDAR 4. panta 9. punkta nozīmē saņēmējs ir "fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kurai izpauž personas datus – neatkarīgi no tā, vai tā ir trešā persona vai nav". Šis saņēmējs var būt vai nu persona, kura nav pārzinis vai apstrādātājs, tātad trešā persona, vai arī persona pārziņa vai apstrādātāja iekšienē, piemēram, darbinieks vai cita nodaļa tajā pašā uzņēmumā vai iestādē.

Atšķirība starp saņēmējiem un trešām personām ir svarīga tikai datu likumīgas izpaušanas nosacījumu kontekstā. Pārziņa vai apstrādātāja darbinieki var būt personas datu saņēmēji, uz kuriem attiecas papildu juridiskās prasības, ja viņi ir iesaistīti pārziņa vai apstrādātāja apstrādes darbībās. Turpretī trešai personai, kas ir nodalīta no pārziņa vai apstrādātāja, nav atļauts izmantot personas datus, kurus apstrādā apstrādātājs, ja vien tas nav paredzēts īpašos gadījumos uz īpaša likumīga pamata.

254 Turpat, 28. panta 4. punkts.

255 Skatīt, piemēram, modernizētās Konvencijas Nr. 108 2. panta b) un f) punktu, Ieteikuma par profilēšanu 1. punktu.

256 29. panta darba grupa (2010), Atzinums 1/2010 par "personas datu apstrādātāja" un "apstrādātāja" jēdzienu, WP 169, Brisele, 2010. gada 16. februāris, 31. lpp.

Piemērs. Pārziņa darbinieks, kurš izmanto personas datus darba devēja uzticēto uzdevumu ietvaros, ir datu saņēmējs, bet ne trešā persona, jo viņš/viņa datus izmanto pārziņa vārdā un saskaņā ar tā norādījumiem. Piemēram, ja darba devējs izpauž personāla informāciju par saviem darbiniekiem cilvēkresursu departamentam, ņemot vērā gaidāmos snieguma novērtējumus, cilvēkresursu komanda būs personas datu saņēmēji, jo šie dati tai tika atklāti pārziņa uzdevumā veiktas apstrādes laikā.

Savukārt, ja organizācija sniedz datus par saviem darbiniekiem apmācību uzņēmumam, kas tos izmantos, lai pielāgotu darbinieku apmācības programmu, šis apmācības uzņēmums ir trešā persona. Iemesls ir tāds, ka apmācības uzņēmumam nav īpašu likumīgu tiesību vai atļaujas (kas "cilvēkresursu" gadījumā izriet no darba attiecībām ar pārzini) šo personas datu apstrādei. Citiem vārdiem sakot, tas nav saņēmis informāciju, esot darba attiecībās ar datu pārzini.

2.4. Piekrišana

Svarīgākie aspekti

- Piekrišanai kā juridiskam pamatam personas datu apstrādei ir jābūt sniegtai no brīvas gribas, apzinātai, konkrētai un nepārprotami jānorāda uz vēlmēm ar skaidru apstiprinošu aktu, kas apliecina piekrišanu apstrādei.
- Lai apstrādātu īpašas datu kategorijas, ir nepieciešama nepārprotama piekrišana.

Kā plašāk aplūkots 4. nodaļā, piekrišana ir viens no sešiem leģitīmiem personas datu apstrādes pamatiem. Piekrišana ir "jebkura brīvi sniegta, konkrēta, apzināta un vienozīmīga norāde uz datu subjekta vēlmēm"[257].

ES tiesību aktos ir noteikti vairāki derīgas piekrišanas elementi, un to mērķis ir garantēt, ka datu subjekti snieguši patiesu piekrišanu viņu datu konkrētam izmantojumam[258]:

257 Vispārīgā datu aizsardzības regula, 4. panta 11. punkts. Skatīt arī modernizēto Konvenciju Nr. 108, 5. panta 2. punkts.

258 Vispārīgā datu aizsardzības regula, 7. pants.

- Piekrišana ir jāsniedz ar skaidru apstiprinošu darbību, ar ko dod brīvi sniegtu, konkrētu, apzinātu un nepārprotamu norādi par datu subjekta piekrišanu viņa/viņas personas datu apstrādei. Šāda rīcība var būt darbība vai paziņojums.

- Datu subjektam jābūt tiesībām jebkurā laikā atsaukt piekrišanu.

- Saistībā ar rakstisku deklarāciju, kas skar arī citus jautājumus, piemēram, "pakalpojumu sniegšanas noteikumus", piekrišanas pieprasījumiem jābūt skaidrā un vienkāršā valodā, saprotamā un viegli pieejamā formā, skaidri izdalot piekrišanu no citiem jautājumiem. Ja daļa šīs deklarācijas pārkāpj VDAR, tā nav saistoša.

Piekrišana būs spēkā datu aizsardzības tiesību aktu kontekstā tikai tad, ja būs izpildītas visas šīs prasības. Pārziņa pienākums ir pierādīt, ka datu subjekts ir piekritis viņa/viņas datu apstrādei[259]. Spēkā esošas piekrišanas elementi tiks sīkāk aplūkoti 4.1.1. iedaļā par leģitīmiem personas datu apstrādes pamatiem.

Konvencijā Nr. 108 nav ietverta piekrišanas definīcija. Tā ir jāparedz valsts tiesību aktos. Tomēr **saskaņā ar EP tiesību aktiem** derīgas piekrišanas elementi atbilst iepriekš izskaidrotajiem[260].

Civiltiesībās paredzētās papildu prasības par derīgu piekrišanu, piemēram, rīcībspēja, protams, attiecas arī uz datu aizsardzību, jo šādas prasības ir būtisks juridiskais priekšnoteikums. Nederīga tādu personu piekrišana, kurām nav rīcībspējas, radīs juridiska pamata neesamību datu apstrādei par šādām personām. Attiecībā uz nepilngadīgo tiesībspēju slēgt līgumus, VDAR paredzēts, ka tās noteikumi par minimālo vecumu derīgas piekrišanas iegūšanai neskar dalībvalstu vispārējās līgumtiesības[261].

Piekrišana ir jāsniedz skaidri, lai neradītu šaubas par datu subjekta nodomu[262]. Piekrišanai jābūt nepārprotamai, ja tā attiecas uz sensitīvu datu apstrādi, un to var sniegt mutiski vai rakstiski[263]. Pēdējo var sniegt, izmantojot elektroniskos līdzekļus[264]. Gan **ES,** gan **EP tiesību aktu** ietvaros piekrišana personas datu apstrādei ir jāsniedz ar

259 Turpat, 7. panta 1. punkts.

260 Modernizētā Konvencija Nr. 108, 5. panta 2. punkts; modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 42.–45. punkts.

261 Vispārīgā datu aizsardzības regula, 8. panta 3. punkts.

262 Turpat, 6. panta 1. punkta a) apakšpunkts un 9. panta 2. punkta a) apakšpunkts.

263 Turpat, 32. apsvērums.

264 Turpat.

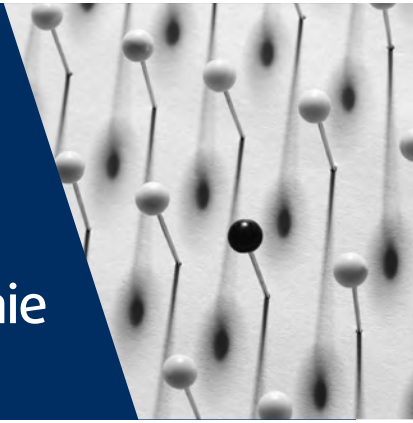
paziņojumu vai ar skaidru apstiprinošu darbību[265]. Tādējādi piekrišanu nevar iegūt, pamatojoties uz klusēšanu, iepriekš atzīmētām rūtiņām, iepriekš aizpildītām veidlapām vai rīcības neesamību[266].

265 Turpat 4. panta 11. punkts; modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 42. punkts.

266 Vispārīgā datu aizsardzības regula, 32. apsvērums; modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 42. punkts.

3

Eiropas tiesību aktu datu aizsardzības jomā galvenie principi



ES	Aptvertie jautājumi	EP
Vispārīgā datu aizsardzības regula, 5. panta 1. punkta a) apakšpunkts	**Likumības princips**	Modernizētā Konvencija Nr. 108, 5. panta 3. punkts
Vispārīgā datu aizsardzības regula, 5. panta 1. punkta a) apakšpunkts	**Godprātības princips**	Modernizētā Konvencija Nr. 108, 5. panta 4. punkta a) apakšpunkts ECT lieta *K.H. un citi pret Slovākiju*, Nr. 32881/04, 2009
Vispārīgā datu aizsardzības regula, 5. panta 1. punkta a) apakšpunkts EST lieta C-201/14 *Smaranda Bara un citi pret Casa Națională de Asigurări de Sănătate un citiem*, 2015	**Pārredzamības princips**	Modernizētā Konvencija Nr. 108, 5. panta 4. punkta a) apakšpunkts un 8. pants ECT lieta *Haralambie pret Rumāniju*, Nr. 21737/03, 2009
Vispārīgā datu aizsardzības regula, 5. panta 1. punkta b) apakšpunkts	**Nolūka ierobežojuma princips**	Modernizētā Konvencija Nr. 108, 5. panta 4. punkta b) apakšpunkts
Vispārīgā datu aizsardzības regula, 5. panta 1. punkta c) apakšpunkts EST apvienotās lietas C-293/12 un C-594/12 *Digital Rights Ireland* un Kärntner Landesregierung un citi [GC], 2014	**Datu minimizēšanas princips**	Modernizētā Konvencija Nr. 108, 5. panta 4. punkta c) apakšpunkts

ES	Aptvertie jautājumi	EP
Vispārīgā datu aizsardzības regula, 5. panta 1. punkta d) apakšpunkts EST lieta C-553/07 *College van burgemeester en wethouders van Rotterdam pret M. E. E. Rijkeboer*, 2009	**Datu precizitātes princips**	Modernizētā Konvencija Nr. 108, 5. panta 4. punkta d) apakšpunkts
Vispārīgā datu aizsardzības regula, 5. panta 1. punkta e) apakšpunkts EST apvienotās lietas C-293/12 un C-594/12 *Digital Rights Ireland* un Kärntner Landesregierung un citi [GC], 2014	**Glabāšanas ierobežojuma princips**	Modernizētā Konvencija Nr. 108, 5. panta 4. punkta e) apakšpunkts ECT lieta *S. un Marper pret Apvienoto Karalisti* [GC], Nr. 30562/04 un Nr. 30566/04, 2008
Vispārīgā datu aizsardzības regula, 5. panta 1. punkta f) apakšpunkts un 32. pants	**Datu drošības (integritātes un konfidencialitātes) princips**	Modernizētā Konvencija Nr. 108, 7. pants
Vispārīgā datu aizsardzības regula, 5. panta 2. punkts	**Pārskatatbildības princips**	Modernizētā Konvencija Nr. 108, 10. pants

Vispārīgās datu aizsardzības regulas 5. pantā ir noteikti principi, kas reglamentē personas datu apstrādi. Šie principi aptver:

- likumību, godprātību un pārredzamību;
- nolūka ierobežojumu;
- datu minimizēšanu;
- datu precizitāti;
- glabāšanas ierobežojumu;
- integritāti un konfidencialitāti.

Šie principi kalpo par sākumpunktu detalizētākiem noteikumiem, kas izklāstīti turpmākajos regulas pantos. Tie parādās arī modernizētās Konvencijas Nr. 108 5., 7., 8. un 10. pantā. Visiem vēlāk pieņemtiem datu aizsardzības tiesību aktiem EP vai ES mērogā jāatbilst šiem principiem, un tie jāņem vērā, interpretējot šādus tiesību

aktus. Saskaņā ar ES tiesību aktiem apstrādes principu ierobežojumi ir atļauti tikai tiktāl, ciktāl tie atbilst tiesībām un pienākumiem, kas paredzēti 12. līdz 22. pantā, un tiem ir jāievēro pamattiesību un brīvību būtība. Jebkādus atbrīvojumus no šiem pamatprincipiem un ierobežojumus var paredzēt ES vai valstu mērogā[267]. Tie jāparedz likumos, tiem jātiecas sasniegt leģitīmu mērķi, un tie ir nepieciešami un samērīgi pasākumi demokrātiskā sabiedrībā. [268] Visiem trim priekšnosacījumiem ir jābūt izpildītiem.

3.1. Apstrādes principu likumība, godprātība un pārredzamība

Svarīgākie aspekti

- Likumības, godprātības un pārredzamības principus piemēro visai personas datu apstrādei.
- Saskaņā ar VDAR likumības nodrošināšanai nepieciešami šādi elementi:
  - datu subjekta piekrišana;
  - nepieciešamība noslēgt līgumu;
  - juridisks pienākums;
  - nepieciešamība aizsargāt datu subjekta vai citas personas vitālas intereses;
  - nepieciešamība veikt uzdevumu sabiedrības interešu dēļ;
  - nepieciešamība pārziņa vai trešās personas likumīgo interešu nodrošināšanai, ja datu subjekta intereses un tiesības nav svarīgākas.
- Personas datu apstrāde ir jāveic godprātīgi.
  - Datu subjekts ir jāinformē par risku, lai nodrošinātu, ka apstrādei nav neparedzamas negatīvas ietekmes.
- Personas datu apstrāde ir jāveic pārredzamā veidā.

267 Modernizētā Konvencija Nr. 108, 11. panta 1. punkts; Vispārīgā datu aizsardzības regula, 23. panta 1. punkts.

268 Vispārīgā datu aizsardzības regula, 23. panta 1. punkts.

- Pārziņiem pirms datu apstrādes cita starpā jāinformē datu subjekti par apstrādes mērķi un par pārziņa identitāti un adresi.
- Informācija par apstrādes darbībām ir jāsniedz skaidrā un vienkāršā valodā, lai datu subjekti varētu viegli izprast ar to saistītos noteikumus, riskus, aizsardzības pasākumus un tiesības.
- Datu subjektiem ir tiesības piekļūt saviem datiem neatkarīgi no tā, kur tie tiek apstrādāti.

3.1.1. Apstrādes likumīgums

ES un EP tiesību aktos datu aizsardzības jomā pieprasīts personas datu apstrādi veikt likumīgi[269]. Likumīgai apstrādei nepieciešama datu subjekta piekrišana vai cits leģitīms pamats, kas paredzēts datu aizsardzības tiesību aktos[270]. VDAR 6. panta 1. punktā ir iekļauti pieci likumīgi apstrādes pamati papildus piekrišanai, t. i., ja personas datu apstrāde ir nepieciešama līguma izpildei, lai izpildītu uzdevumu, ko veic, īstenojot piešķirtās oficiālās pilnvaras, lai izpildītu uz pārzini attiecināmu juridisku pienākumu vai trešās personas leģitīmo interešu ievērošanai, vai, ja nepieciešams, lai aizsargātu datu subjekta vitālas intereses. Tas tiks plašāk aplūkots 4.1. iedaļā.

3.1.2. Apstrādes godprātība

Papildus likumīgai apstrādei ES un EP tiesību aktos datu aizsardzības jomā pieprasīts personas datu apstrādi veikt godprātīgi[271]. Godprātīgas apstrādes princips galvenokārt regulē attiecības starp pārzini un datu subjektu.

Pārziņiem ir jāinformē datu subjekti un plašāka sabiedrība, ka viņi datus apstrādā likumīgā un pārredzamā veidā, un viņiem jāspēj pierādīt apstrādes darbību atbilstība VDAR. Apstrādes darbības nedrīkst tikt veiktas slepeni, un datu subjektiem jābūt informētiem par iespējamiem riskiem. Turklāt pārziņiem, ciktāl iespējams, ir jārīkojas tā, lai tie nekavējoties izpildītu datu subjekta vēlmes, jo īpaši, ja datu apstrādes juridiskais pamats ir piekrišana.

269 Modernizētā Konvencija Nr. 108, 5. panta 3. punkts; Vispārīgā datu aizsardzības regula, 5. panta 1. punkta a) apakšpunkts.

270 Eiropas Savienības Pamattiesību harta, 8. panta 2. punkts; Vispārīgā datu aizsardzības regula, 40. apsvērums un 6.–9. pants; modernizētā Konvencija Nr. 108, 5. panta 2. punkts, modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 41. punkts.

271 Vispārīgā datu aizsardzības regula, 5. panta 1. punkts a) apakšpunkts; modernizētā Konvencija Nr. 108, 5. panta 4. punkta a) apakšpunkts.

Piemērs. Lietā *K.H. un citi pret Slovākiju*[272] prasītājas – romu tautības sievietes – grūtniecības un dzemdību laikā tika ārstētas divās slimnīcās Slovākijas austrumos. Pēc tam neviena no viņām nespēja vēlreiz ieņemt bērnu, kaut mēģinājumi bija atkārtoti. Valsts tiesas uzdeva slimnīcām ļaut prasītājām un viņu pārstāvjiem iepazīties ar medicīnisko dokumentāciju un veikt ar roku rakstītus izrakstus no tās, taču noraidīja viņu lūgumu atļaut kopēt dokumentus, domājams, lai novērstu to ļaunprātīgu izmantošanu. Valstu pozitīvās saistības saskaņā ar ECTK 8. pantu obligāti ietver pienākumu darīt datu subjektam pieejamus viņa vai viņas datu dosjē kopijas. Valsts pārziņā bija noteikt personas datu dosjē kopēšanas kārtību, vai attiecīgā gadījumā tai jāuzrāda pārliecinoši atteikuma iemesli. Prasītāju gadījumā valsts tiesas attaisnoja aizliegumu prasītājām kopēt viņu medicīniskās kartes, galvenokārt pamatojot ar nepieciešamību aizsargāt attiecīgo informāciju no ļaunprātīgas izmantošanas. Tomēr ECT nespēja saskatīt, kā prasītājas, kurām jebkurā gadījumā bija ļauts piekļūt visiem viņu medicīniskajiem dokumentiem, varētu ļaunprātīgi izmantot informāciju par sevi. Turklāt šādas ļaunprātīgas izmantošanas risku varēja novērst, izmantojot citus līdzekļus, nevis liedzot prasītājām iespēju veikt dokumentu kopijas, piemēram, ierobežojot to personu loku, kurām ir tiesības piekļūt dokumentiem. Valsts nav sniegusi pietiekami pārliecinošu iemeslu, lai liegtu prasītājām efektīvu piekļuvi informācijai par viņu veselību. Tiesa atzina, ka šajā lietā ticis pārkāpts 8. pants.

Saistībā ar interneta pakalpojumiem datu apstrādes sistēmu īpašībām ir jābūt tādām, lai datu subjekti varētu patiešām saprast, kas tiek darīts ar viņu datiem. Jebkurā gadījumā godprātības princips ir plašāks par pārredzamības pienākumu, un to varētu saistīt arī ar personas datu apstrādi ētiskā veidā.

Piemērs. Universitātes pētniecības nodaļa veic eksperimentu, kurā analizē 50 dalībnieku garastāvokļa izmaiņas. Viņiem katru stundu noteiktā laikā jāreģistrē savas domas elektroniskā datnē. Piekrišanu šim konkrētajam projektam un tam, ka universitāte izmanto šos datus konkrēti šim nolūkam ir devušas 50 personas. Pētniecības nodaļa drīz atklāj, ka elektroniski reģistrētas domas būtu ļoti noderīgas citam projektam, kas pievēršas garīgajai veselībai, citas komandas vadībā. Kaut arī universitāte kā pārzinis varēja izmantot tos pašus datus citas komandas darbam bez turpmākiem pasākumiem šo

272 ECT 2009. gada 28. aprīļa spriedums lietā *K.H. un citi pret Slovākiju*, Nr. 32881/04.

datu apstrādes likumības nodrošināšanai, ņemot vērā mērķu savietojamību, universitāte informēja šīs personas un lūdza jaunu piekrišanu atbilstoši tās pētījumu ētikas kodeksam un godīgas apstrādes principam.

3.1.3. Apstrādes pārredzamība

ES un EP tiesību aktos datu aizsardzības jomā ir noteikts, ka personas datu apstrāde jāveic "datu subjektam pārredzamā veidā"[273].

Šis princips nosaka pārziņa pienākumu īstenot visus attiecīgos pasākumus, lai datu subjekti, kuri var būt lietotāji, patērētāji vai klienti, tiktu informēti par to, kā tiek izmantoti viņu dati[274]. Pārredzamība var attiekties uz informāciju, kas indivīdam tiek sniegta pirms apstrādes uzsākšanas[275], informāciju, kurai apstrādes laikā vajadzētu būt viegli pieejamai datu subjektiem[276], kā arī informāciju, ko datu subjektiem sniedz pēc pieprasījuma sniegt piekļuvi viņu pašu datiem[277].

Piemērs. Lietā *Haralambie pret Rumāniju*[278] prasītājam tika piešķirta piekļuve slepenā dienesta rīcībā esošajai informācijai par viņu tikai piecus gadus pēc viņa pieprasījuma. ECT atkārtoti uzsvēra, ka piekļuve personas lietām, kas ir publisko iestāžu rīcībā, ir šīs personas vitālas intereses. Iestādēm bija pienākums nodrošināt efektīvu procedūru, lai iegūtu piekļuvi šādai informācijai. ECT uzskatīja, ka ne pārsūtīto dokumentu daudzums, ne arhīva sistēmas nepilnības neattaisno aizkavēšanos piecu gadu garumā izsniegt prasītājam piekļuvi viņa dosjē. Iestādes nebija nodrošinājušas prasītājam efektīvu un pieejamu procedūru, kas ļautu saprātīgā laikā piekļūt viņa personas lietai. Tiesa secināja, ka ir pārkāpts ECTK 8. pants.

Apstrādes darbības datu subjektiem jāpaskaidro viegli pieejamā veidā, nodrošinot, ka viņi saprot, kas tiks darīts ar viņu datiem. Tas nozīmē, ka personas datu vākšanas

273 Vispārīgā datu aizsardzības regula, 5. panta 1. punkts a) apakšpunkts; modernizētā Konvencija Nr. 108, 5. panta 4. punkta a) apakšpunkts un 8. pants.

274 Vispārīgā datu aizsardzības regula, 12. pants.

275 Turpat, 13. panta 14. pants.

276 29. panta darba grupa, *Atzinums 2/2017 par datu apstrādi darbā*, 23. lpp.

277 Vispārīgā datu aizsardzības regula, 15. pants.

278 ECT 2009. gada 27. oktobra spriedums lietā *Haralambie pret Rumāniju*, Nr. 21737/03.

brīdī datu subjektam ir jāzina konkrētais personas datu apstrādes mērķis[279]. Apstrādes pārredzamība prasa skaidras un vienkāršas valodas lietojumu[280]. Iesaistītajām personām ir jābūt skaidrībai, kādi ir riski, noteikumi, aizsardzības pasākumi un tiesības attiecībā uz viņu personas datu apstrādi[281].

EP tiesību aktos ir arī noteikts, ka pārzinim ir obligāti jāsniedz datu subjektiem noteikta būtiskā informācija. Informāciju par pārziņa (vai kopīgo pārziņu) vārdu un adresi, datu apstrādes juridisko pamatu un mērķiem, apstrādāto datu kategorijām un saņēmējiem, kā arī par tiesībām izmantot līdzekļus var sniegt jebkurā piemērotā formātā (izmantojot tīmekļa vietni, personālo ierīču tehnoloģiskos rīkus u. tml.) ar nosacījumu, ka informācija datu subjektam tiek sniegta godīgi un efektīvi. Sniegtajai informācijai jābūt viegli pieejamai, salasāmai, saprotamai un pielāgotai attiecīgajiem datu subjektiem (piemēram, bērniem draudzīgā valodā attiecīgos gadījumos). Ir jāsniedz arī jebkura papildu informācija, kas nepieciešama, lai nodrošinātu godprātīgu datu apstrādi, vai kas ir noderīga šādiem nolūkiem, piemēram, glabāšanas periods, informācija par datu apstrādes pamatojumu vai informācija par datu nosūtīšanu saņēmējam, kas ir citā dalībvalstī vai ārpus tās (tostarp, vai šī konkrētā trešā valsts nodrošina attiecīgu aizsardzības līmeni vai pārzinis veic pasākumus, lai garantētu šādu attiecīgu datu aizsardzības līmeni). [282]

Saskaņā ar piekļuves tiesībām[283] datu subjektam ir tiesības saņemt informāciju no pārziņa, vai viņa dati tiek apstrādāti, un, ja tā, kādi dati tiek šādi apstrādāti[284]. Turklāt saskaņā ar tiesībām uz informāciju[285] pārziņiem vai apstrādātājiem principā ir jāinformē personas, kuru dati tiek apstrādāti, pirms apstrādes darbības sākuma cita starpā par apstrādes mērķiem, ilgumu, līdzekļiem.

Piemērs. Lieta *Smaranda Bara un citi pret Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF)*[286] skāra nodokļu datu par pašnodarbinātu personu ienākumiem pārsūtīšanu no Valsts

279 Vispārīgā datu aizsardzības regula, 39. apsvērums.

280 Turpat.

281 Turpat.

282 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 68. punkts.

283 Vispārīgā datu aizsardzības regula, 15. pants.

284 Modernizētā Konvencija Nr. 108, 8. pants un 9. panta 1. punkta b) apakšpunkts.

285 Vispārīgā datu aizsardzības regula, 13. un 14. pants.

286 EST 2015. gada 1. oktobra spriedums lietā C-201/14 *Smaranda Bara un citi pret Casa Naţională de Asigurări de Sănătate un citiem*. 28.–46. punkts.

nodokļu administrācijas aģentūras uz Nacionālo veselības apdrošināšanas fondu Rumānijā, uz kā pamata tika pieprasīts apmaksāt parādu par veselības apdrošināšanas iemaksām. EST tika lūgts noteikt, vai bija pienākums pirms šo datu apstrādes Nacionālajā veselības apdrošināšanas fondā sniegt datu subjektam iepriekšēju informāciju par datu pārziņa identitāti un datu pārsūtīšanas mērķi. EST nosprieda, ka tad, ja dalībvalsts publiskās pārvaldes iestāde pārsūta personas datus citai publiskās pārvaldes iestādei, kas šos datus tālāk apstrādā, datu subjekti par šo pārsūtīšanu vai apstrādi jāinformē.

Dažās situācijās ir pieļaujamas atkāpes no pienākuma informēt datu subjektus par datu apstrādi, un tās sīkāk tiks aplūkotās 6.1. iedaļā par datu subjekta tiesībām.

3.2. Nolūka ierobežojuma princips

Svarīgākie aspekti

- Datu apstrādes nolūks ir jādefinē pirms apstrādes sākšanas.
- Nedrīkst turpināt datu turpmāku apstrādi veidā, kas nav savienojams ar sākotnējo mērķi, lai gan Vispārīgajā datu aizsardzības regulā paredzēti izņēmumi no šā noteikuma, lai datus arhivētu sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, kā arī statistikas nolūkos.
- Faktiski nolūka ierobežojuma princips nozīmē, ka jebkura personas datu apstrāde jāveic konkrētam skaidri noteiktam mērķim un tikai tādiem papildu, konkrētiem mērķiem, kas ir saderīgi ar sākotnējo.

Nolūka ierobežojuma princips ir viens no Eiropas datu aizsardzības tiesību aktu pamatprincipiem. Tas ir cieši saistīts ar pārredzamību, paredzamību un lietotāju kontroli: ja apstrādes nolūks ir pietiekami konkrēts un skaidrs, indivīdi zina, ko sagaidīt, un tiek uzlabota pārredzamība un juridiskā noteiktība. Tajā pašā laikā ir svarīgi skaidri definēt nolūku, lai datu subjekti varētu efektīvi īstenot savas tiesības, piemēram, tiesības iebilst pret apstrādi[287].

Šis princips paredz, ka jebkura personas datu apstrāde jāveic konkrētam skaidri noteiktam mērķim un tikai tādiem papildu nolūkiem, kas ir saderīgi ar sākotnējo[288].

287 29. panta darba grupa (2013), *Atzinums 3/2013 par nolūka ierobežojumu*, WP 203, 2013. gada 2. aprīlis.

288 Vispārīgā datu aizsardzības regula, 5. panta 1. punkta b) apakšpunkts.

Tādējādi personas datu apstrāde nenoteiktiem un/vai neierobežotiem nolūkiem ir nelikumīga. Personas datu apstrāde bez noteikta nolūka, balstoties tikai uz apsvērumiem, ka nākotnē dati varētu būt noderīgi, arī nav likumīga. Personas datu apstrādes leģitimitāte ir atkarīga no apstrādes nolūka, kam jābūt skaidram, konkrētam un leģitīmam.

Katram jaunam datu apstrādes nolūkam, kas nav savietojams ar sākotnējo, jābūt savam īpašam juridiskajam pamatam, un nav pieļaujams atsaukties uz faktu, ka dati sākotnēji tika iegūti vai apstrādāti citam likumīgam nolūkam. Savukārt likumīgai apstrādei ir tikai tās sākotnēji noteiktais nolūks, bet jebkuram jaunam apstrādes nolūkam nepieciešams atsevišķs jauns juridiskais pamats. Piemēram, rūpīgi jāapsver personas datu izpaušana trešām personām jaunajam nolūkam, jo šādai izpaušanai, iespējams, ir vajadzīgs papildu juridiskais pamats, kas atšķiras no datu vākšanas pamatā esošā.

Piemērs. Aviosabiedrība vāc datus no saviem pasažieriem, veicot rezervācijas, lai pareizi izpildītu lidojumu. Aviosabiedrībai nepieciešami šādi dati: pasažieru sēdvietu numuri; īpaši fiziski ierobežojumi, piemēram, nepieciešamība pēc ratiņkrēsla; un īpašas pārtikas prasības, piemēram, košera vai halāla pārtika. Ja aviosabiedrībām lūdz pārsūtīt šos datus, kas ir iekļauti Pasažieru datu reģistrā, imigrācijas iestādēm nolaišanās lidostā, šie dati tiek izmantoti imigrācijas kontroles nolūkos, kas atšķiras no sākotnējā datu vākšanas nolūka. Tādēļ šo datu nosūtīšanai imigrācijas iestādei ir nepieciešams jauns, atsevišķs juridiskais pamats.

Apskatot konkrēta nolūka piemērošanas jomu un ierobežojumus, modernizētā Konvencija Nr. 108 un Vispārīgā datu aizsardzības regula atsaucas uz savietojamības jēdzienu: datu izmantošana savietojamiem nolūkiem ir atļauta, pamatojoties uz sākotnējo juridisko pamatu. Tāpēc turpmāku datu apstrādi nedrīkst veikt negaidīti, nepiemēroti vai veidā, pret kuru datu subjekts varētu iebilst[289]. Lai novērtētu, vai turpmākā apstrāde ir uzskatāma par savietojamu, pārzinim (cita starpā) ir jāņem vērā šādi aspekti:

- "jebkura saikne starp minētajiem nolūkiem un paredzētās turpmākās apstrādes nolūkiem;

289 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 49. punkts.

- konteksts, kādā personas dati ir vākti, jo īpaši saprātīgas datu subjektu gaidas, kuru pamatā ir to attiecības ar pārzini, attiecībā uz datu turpmāku izmantošanu;
- personas datu raksturs;
- sekas, ko paredzētā turpmākā apstrāde rada datu subjektiem; kā arī
- atbilstošu garantiju esamība gan sākotnējās, gan paredzētajās turpmākās apstrādes darbībās"[290]. Tas izdarāms, piemēram, izmantojot šifrēšanu vai pseidonimizāciju.

Piemērs. Uzņēmums *Sunshine* datus par klientiem iegūst klientu attiecību pārvaldības (*CRM*) gaitā. Pēc tam šie dati tiek pārsūtīti tiešās tirgvedības uzņēmumam *Moonlight*, kurš vēlas izmantot šos datus, lai palīdzētu trešo uzņēmumu tirgvedības kampaņās. Uzņēmuma *Sunshine* veiktā datu nodošana citiem uzņēmumiem tirgvedības nolūkos ir datu turpmāka izmantošana jaunam nolūkam, kurš nav savietojams ar *CRM*, kas ir uzņēmuma *Sunshine* sākotnējais klientu datu vākšanas nolūks. Tāpēc datu nosūtīšanai uzņēmumam *Moonlight* ir nepieciešams atsevišķs juridiskais pamats.

Turpretī uzņēmuma *Sunshine CRM* datu izmantošana saviem mārketinga nolūkiem, proti, mārketinga ziņojumu nosūtīšana saviem klientiem par saviem produktiem, parasti tiek atzīta par savietojamu mērķi.

Vispārīgajā datu aizsardzības regulā un modernizētajā Konvencijā Nr. 108 noteikts, ka "turpmāka apstrāde arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, vai statistikas nolūkos" *a priori* uzskatāma par savietojamu ar sākotnējo nolūku[291]. Taču, turpinot personas datu turpmāku apstrādi, ir jāievieš piemēroti drošības pasākumi, piemēram, datu anonimizācija, šifrēšana vai pseidonimizācija un piekļuves ierobežojums datiem[292]. Vispārīgajā datu aizsardzības regulā papildus noteikts, ka gadījumos, "[j]a datu subjekts ir devis piekrišanu

290 Vispārīgā datu aizsardzības regula, 50. apsvērums un 6. panta 4. punkts; modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 49. punkts.

291 Vispārīgā datu aizsardzības regula, 5. panta 1. punkta b) apakšpunkts; modernizētā Konvencija Nr. 108, 5. panta 4. punkta b) apakšpunkts. Piemērs šādai valsts tiesību aktu normai sniegts Austrijas datu aizsardzības likumā (*Datenschutzgesetz*), *Federal Law Gazette* I Nr. 165/1999, 46. punkts.

292 Vispārīgā datu aizsardzības regula, 6. panta 4. punkts; modernizētā Konvencija Nr. 108, 5. panta 4. punkta b) apakšpunkts; modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 50. punkts.

vai ja apstrāde balstās uz Savienības vai dalībvalsts tiesību aktiem, kas demokrātiskā sabiedrībā ir vajadzīgs un samērīgs pasākums, lai jo īpaši aizsargātu svarīgus vispārējo sabiedrības interešu mērķus, būtu jāļauj pārzinim turpināt personas datu apstrādi neatkarīgi no saderības ar nolūkiem[293]". Tāpēc, veicot turpmāku apstrādi, datu subjekts ir jāinformē par tās nolūkiem, kā arī par viņa tiesībām, piemēram, tiesībām iebilst[294].

Piemērs. Uzņēmums *Sunshine* ir apkopojis un glabā klientu attiecību pārvaldības (*CRM*) datus par saviem klientiem. Tālāk šos datus *Sunshine* izmanto savu klientu pirkšanas paradumu statistiskai analīzei, jo statistika ir savietojams nolūks. Nav nepieciešams papildu juridiskais pamats, piemēram, datu subjektu piekrišana. Tomēr personas datu turpmākai apstrādei statistikas nolūkos uzņēmumam *Sunshine* ir jāievieš attiecīgi datu subjekta tiesību un brīvību aizsardzības pasākumi. Tehniskie un organizatoriskie pasākumi, kas uzņēmumam *Sunshine* jāveic, var ietvert pseidonimizāciju.

3.3. Datu minimizēšanas princips

Svarīgākie aspekti

- Datu apstrāde jāierobežo līdz nepieciešamajam, lai sasniegtu likumīgu mērķi.
- Personas datu apstrādei ir jānotiek tikai tad, ja apstrādes mērķi nav iespējams saprātīgi sasniegt ar citiem līdzekļiem.
- Datu apstrāde nedrīkst nesamērīgi ierobežot intereses, tiesības un brīvības.

Jāapstrādā tikai tādi dati, kas ir "adekvāti, atbilstīgi un ietver tikai to, kas nepieciešams to apstrādes nolūkos"[295]. Apstrādei izvēlētajām datu kategorijām jābūt nepieciešamām, lai sasniegtu deklarēto kopējo apstrādes darbību mērķi, un pārzinim datu vākšana ir stingri jāierobežo līdz informācijai, kas tieši saistīta ar konkrēto apstrādes nolūku.

293 Vispārīgā datu aizsardzības regula, 50. apsvērums.

294 Turpat.

295 Modernizētā Konvencija Nr. 108, 5. panta 4. punkta c) apakšpunkts; Vispārīgā datu aizsardzības regula, 5. panta 1. punkta c) apakšpunkts.

Piemērs. Lietā *Digital Rights Ireland*[296] EST aplūkoja Datu saglabāšanas direktīvas spēkā esamību, kuras mērķis bija saskaņot valstu noteikumus par tādu personas datu glabāšanu, ko ģenerējuši vai apstrādājuši publiski pieejami elektronisko komunikāciju pakalpojumi vai tīkli, lai tos varētu pārsūtīt kompetentajām iestādēm smagu noziegumu, piemēram, organizētās noziedzības un terorisma, apkarošanai. Lai gan tas tika uzskatīts par mērķi, kas patiesībā atbilst vispārējas nozīmes mērķim, vispārīgais veids, kādā direktīva aptver "visas personas un visus elektroniskās komunikācijas līdzekļus, kā arī visu informāciju par datu plūsmu bez kādām atšķirībām, ierobežojumiem vai izņēmumiem saistībā ar mērķi cīnīties pret smagiem noziegumiem", tika uzskatīts par problemātisku[297].

Turklāt, izmantojot īpašu privātumu uzlabojošu tehnoloģiju, dažreiz ir iespējams vispār izvairīties no personas datu izmantošanas vai izmantot pasākumus, lai samazinātu iespēju attiecināt datus uz datu subjektu (piemēram, izmantojot pseidonimizāciju), iegūstot privātumam draudzīgu risinājumu. Tas ir īpaši piemēroti plašākās apstrādes sistēmās.

Piemērs. Pilsētas dome par noteiktu samaksu piedāvā mikroshēmas karti pilsētas sabiedriskā transporta pastāvīgajiem lietotājiem. Uz kartes ir rakstīts lietotāja vārds, mikroshēmā tas ierakstīts elektroniskā formā. Ikreiz, kad tiek izmantots autobuss vai tramvajs, mikroshēmas karte ir jānovieto pie nolasīšanas ierīces, kas uzstādīta, piemēram, autobusos un tramvajos. Ierīces nolasītie dati tiek elektroniski pārbaudīti, izmantojot datubāzi ar to personu vārdiem, kuras iegādājušās braukšanas karti.

Šajā sistēmā optimāli neievēro datu samazināšanas principu. Ir jārod iespēja veikt pārbaudi, vai personai ir atļauts izmantot transportu, nesalīdzinot personas datus kartes mikroshēmā ar datubāzi. Pietiktu, piemēram, ja kartes mikroshēmā ir īpašs elektronisks attēls, piemēram, svītrkods, kurš, novietots pie nolasīšanas ierīces, apstiprinātu, vai karte ir derīga vai nē. Šāda sistēma nereģistrēs, kurš un kad izmantojis transportu. Tas būtu optimālais risinājums minimizācijas principa izpratnē, jo no šā principa izriet pienākums samazināt datu vākšanu līdz minimumam.

296 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C-293/12 un C-594/12 *Digital Rights Ireland Ltd pret Minister for Communications, Marine and Natural Resources un citiem* un Kärntner Landesregierung un citiem [GC].

297 Turpat, 44. un 57. pants.

Modernizētās Konvencijas Nr. 108 5. panta 1. punktā ir ietverta proporcionalitātes prasība personas datu apstrādei saistībā ar leģitīmo mērķi. Visos apstrādes posmos jāievēro līdzsvars starp visām attiecīgajām interesēm. Tas nozīmē, ka "[p]ersonas dati, kas ir adekvāti un atbilstīgi, bet izraisītu nesamērīgu iejaukšanos attiecīgajās pamattiesībās un brīvībās, ir jāuzskata par pārmērīgiem[298]".

3.4. Datu precizitātes princips

Svarīgākie aspekti

- Pārzinim visās apstrādes darbībās jāievēro datu precizitātes princips.
- Neprecīzi dati nekavējoties jādzēš vai jālabo.
- Iespējams, dati ir regulāri jāpārbauda un jāatjaunina, lai nodrošinātu to precizitāti.

Pārzinis, kura rīcībā ir personiska informācija, nedrīkst izmantot šo informāciju, neveicot pasākumus, kas sniegtu pietiekamu pārliecību, ka dati ir precīzi un atjaunināti[299].

Pienākums nodrošināt datu precizitāti jāskata datu apstrādes nolūka kontekstā.

Piemērs. Lietā *Rijkeboer*[300] EST izskatīja Nīderlandes valstspiederīgā lūgumu saņemt informāciju no Amsterdamas pilsētas vietējās pārvaldes iestādes par to personu identitāti, kurām divos iepriekšējos gados tika izsniegti vietējas iestādes rīcībā esošie ieraksti par viņu, kā arī par izpausto datu saturu. EST norādīja, ka "tiesības uz privātās dzīves neaizskaramību nozīmē, ka attiecīgajai personai ir jābūt iespējai pārliecināties, ka tās personas dati ir apstrādāti pareizi un likumīgi, proti, it īpaši, ka tās pamatdati ir pareizi un ka tie ir izpausti likumīgiem saņēmējiem". Tālāk EST atsaucās uz Datu aizsardzības direktīvas preambulu, kurā teikts, ka datu subjektiem ir jābūt tiesībām piekļūt saviem personas datiem, lai varētu pārbaudīt, vai dati ir pareizi[301].

298 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 52. punkts; Vispārīgā datu aizsardzības regula, 5. panta 1. punkta c) apakšpunkts.

299 Vispārīgā datu aizsardzības regula, 5. panta 1. punkta d) apakšpunkts; modernizētā Konvencija Nr. 108, 5. panta 4. punkta d) apakšpunkts.

300 EST 2009. gada 7. maija spriedums lietā C-553/07 *College van burgemeester en wethouders van Rotterdam pret M. E. E. Rijkeboer*.

301 Iepriekšējais 41. apsvērums, Direktīvas 95/46/EK preambula.

Var būt arī gadījumi, kad uzglabāto datu atjaunināšana ir juridiski aizliegta, jo datu glabāšanas mērķis pamatā ir notikumu dokumentēšana vēsturiskā "momentuzņēmumā".

Piemērs. Operācijas medicīniskos ierakstus nedrīkst mainīt, citiem vārdiem sakot, "atjaunināt", pat ja vēlāk ierakstā minētie konstatējumi izrādās nepareizi. Šādos apstākļos ierakstā var izdarīt tikai papildinājumus, ja vien tie ir skaidri atzīmēti kā vēlāk izdarīti pieraksti.

Tajā pašā laikā var būt situācijas, kad ir absolūti nepieciešams atjaunināt un regulāri pārbaudīt datu precizitāti iespējamā kaitējuma dēļ, kas varētu tikt nodarīts datu subjektam, ja dati netiktu precizēti.

Piemērs. Ja persona vēlas noslēgt aizdevuma līgumu ar banku, banka parasti pārbauda potenciālā klienta kredītspēju. Šim nolūkam ir pieejamas īpašas datubāzes, kurās ir dati par privātpersonu kredītvēsturi. Ja šāda datubāze sniedz nepareizus vai novecojušus datus par personu, tas var negatīvi ietekmēt šo personu. Tādēļ šādu datubāzu pārziņiem ir jāpieliek īpašas pūles, lai ievērotu precizitātes principu.

3.5. Glabāšanas ierobežojuma princips

Svarīgākie aspekti

- Glabāšanas ierobežojuma princips nozīmē, ka personas dati ir jādzēš vai jāpadara anonīmi, tiklīdz tie vairs nav nepieciešami nolūkiem, kādiem tie tika vākti.

VDAR 5. panta 1. punkta e) apakšpunkts un tāpat arī modernizētās Konvencijas Nr. 108 5. panta 4. punkta e) apakšpunkts pieprasa, lai personas dati tiktu "glabāti veidā, kas pieļauj datu subjektu identifikāciju, ne ilgāk, kā nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā". Tāpēc šie dati ir jādzēš vai jāpadara anonīmi, kad šie nolūki ir sasniegti. Šajā nolūkā "pārzinim būtu jānosaka termiņi, kad dati ir jādzēš vai periodiski jāpārskata", lai pārliecinātos, ka dati netiek glabāti ilgāk, kā tas ir nepieciešams[302].

302 Vispārīgā datu aizsardzības regula, 39. apsvērums.

Lietā *S. un Marper* ECT secināja, ka attiecīgo Eiropas Padomes instrumentu un citu līgumslēdzēju pušu tiesību un prakses pamatprincipi prasa, lai datu saglabāšana ir samērīga attiecībā uz datu vākšanas nolūku un ierobežota laikā, jo īpaši policijas darbā[303].

Piemērs. Lietā *S. un Marper*[304] ECT lēma, ka abu prasītāju pirkstu nospiedumu, šūnu paraugu un DNS profilu glabāšana uz nenoteiktu laiku ir nesamērīga un nav nepieciešama demokrātiskā sabiedrībā, uzskatot, ka kriminālprocess pret abiem prasītājiem tika izbeigts attiecīgi ar attaisnojošu spriedumu un atteikšanos no prasības.

Personas datu glabāšanas termiņš attiecas tikai uz datiem, ko glabā tādā formā, kura ļauj identificēt datu subjektus. Tādēļ datu, kas vairs nav nepieciešami, likumīgu glabāšanu varētu panākt, anonimizējot datus.

Arhivējot datus sabiedrības interesēs, zinātniskos vai vēsturiskos nolūkos vai statistikas vajadzībām, tos var uzglabāt ilgāk, ja šie dati tiks izmantoti tikai iepriekšminētajiem nolūkiem[305]. Personas datu pastāvīgai glabāšanai un izmantošanai jāīsteno attiecīgi tehniski un organizatoriski pasākumi, lai aizsargātu datu subjekta tiesības un brīvības.

Modernizētā Konvencija Nr. 108 pieļauj arī izņēmumus no glabāšanas ierobežojuma principa ar nosacījumu, ka tie ir paredzēti likumā, tiek ievērota pamattiesību un brīvību būtība, kā arī tie ir nepieciešami un samērīgi ierobežota skaita likumīgu mērķu sasniegšanai[306]. Tie cita starpā ietver valsts drošības aizsardzību, noziedzīgu nodarījumu izmeklēšanu un kriminālvajāšanu par tiem, kriminālsodu izpildi, datu subjekta aizsardzību, kā arī citu personu tiesību un pamatbrīvību aizsardzību.

303 ECT 2008. gada 4. decembra spriedums lietā *S. un Marper pret Apvienoto Karalisti* [GC], Nr. 30562/04 un Nr. 30566/04, skatīt arī, piemēram: ECT 2012. gada 13. novembra spriedumu lietā *M.M. pret Apvienoto Karalisti*, Nr. 24029/07.

304 ECT 2008. gada 4. decembra spriedums lietā *S. un Marper pret Apvienoto Karalisti* [GC], Nr. 30562/04 un Nr. 30566/04.

305 Vispārīgā datu aizsardzības regula, 5. panta 1. punkta e) apakšpunkts; modernizētā Konvencija Nr. 108, 5. panta 4. punkta b) apakšpunkts un 11. panta 2. punkts.

306 Modernizētā Konvencija Nr. 108, 11. panta 1. punkts; modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 91.–98. punkts.

Piemērs. Lietā *Digital Rights Ireland*[307] EST pārskatīja spēkā esamību Datu saglabāšanas direktīvai, kuras mērķis bija saskaņot valstu noteikumus par to personas datu saglabāšanu, ko ģenerē vai apstrādā publiski pieejami elektronisko komunikāciju pakalpojumi vai tīkli, lai apkarotu smagus noziegumus, piemēram, organizēto noziedzību un terorismu. Datu saglabāšanas direktīvā noteikts datu saglabāšanas periods "vismaz sešus mēnešus, nenosakot nekādas atšķirības starp šīs direktīvas 5. pantā paredzētajām datu kategorijām atkarībā no to iespējamā noderīguma izvirzītā mērķa sasniegšanai vai personām, uz kurām tie attiecas"[308]. EST arī izvirzīja jautājumu par objektīvu kritēriju neesamību Datu saglabāšanas direktīvā, pamatojoties uz kuriem ir jānosaka precīzs datu saglabāšanas periods, kas var svārstīties no vismaz sešiem mēnešiem līdz ne vairāk kā 24 mēnešiem, lai nodrošinātu, ka šāds laika posms nepārsniedz nepieciešamo termiņu[309].

3.6. Datu drošības princips

Svarīgākie aspekti

- Personas datu drošība un konfidencialitāte ir būtiski, lai novērstu nelabvēlīgu ietekmi uz datu subjektu.
- Drošības pasākumiem var būt tehnisks un/vai organizatorisks raksturs.
- Pseidonimizācija ir process, ar ko iespējams aizsargāt personas datus.
- Drošības pasākumu piemērotība jānosaka katrā gadījumā atsevišķi, un tā regulāri jāpārskata.

Saskaņā ar datu drošības principu, apstrādājot personas datus, jāievieš attiecīgi tehniski vai organizatoriski pasākumi, lai aizsargātu datus pret nejaušu vai nelikumīgu piekļuvi, izmantošanu, pārveidošanu, izpaušanu, nozaudēšanu, iznīcināšanu vai bojājumu[310]. VDAR norādīts, ka pārzinim un apstrādātājam, īstenojot šādus pasā-

307 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C-293/12 un C-594/12 *Digital Rights Ireland Ltd pret Minister for Communications, Marine and Natural Resources un citiem* un Kärntner Landesregierung un citiem [GC].

308 Turpat, 63. punkts.

309 Turpat, 64. punkts.

310 Vispārīgā datu aizsardzības regula, 39. apsvērums un 5. panta 1. punkta f) apakšpunkts; modernizētā Konvencija Nr. 108, 7. pants.

kumus, jāņem vērā "tehnikas līmenis, īstenošanas izmaksas un apstrādes raksturs, apmērs, konteksts un nolūki, kā arī dažādas iespējamības un smaguma pakāpes risks attiecībā uz fizisku personu tiesībām un brīvībām"[311]. Atkarībā no katra gadījuma īpašiem apstākļiem attiecīgie tehniskie un organizatoriskie pasākumi varētu ietvert, piemēram, personas datu pseidonimizēšanu un šifrēšanu un/vai regulāru pasākumu efektivitātes pārbaudi un novērtēšanu, lai nodrošinātu datu apstrādes drošību[312].

Kā paskaidrots 2.1.1. iedaļā, pseidonimizācija nozīmē personas datu atribūtu, kas ļauj identificēt datu subjektu, aizstāšanu ar pseidonīmu un šo atribūtu saglabāšanu atsevišķi, piemērojot tehniskus vai organizatoriskus pasākumus. Pseidonimizācijas procesu nedrīkst jaukt ar anonimizācijas procesu, kurā visas saites ar personas identificēšanu tiek pārtrauktas.

Piemērs. Teikumu "Čārlzs Spensers, dzimis 1967. gada 3. aprīlī, ir tēvs četriem bērniem – diviem zēniem un divām meitenēm", piemēram, var pseidonimizēt šādi:

"Č.S. 1967. ir tēvs četriem bērniem – diviem zēniem un divām meitenēm"; vai

"324 ir tēvs četriem bērniem – diviem zēniem un divām meitenēm"; vai

"YESz320l ir tēvs četriem bērniem – diviem zēniem un divām meitenēm".

Lietotājiem, kuri piekļūst pseidonimizētiem datiem, parasti nav iespējas identificēt "Čarlzu Spenseru, dzimušu 1967. gada 3. aprīlī" ar "324" vai "YESz3201" palīdzību. Tādēļ šādi dati, visticamāk, ir droši pasargāti no nepareizas lietošanas.

Pirmais piemērs tomēr ir mazāk drošs. Ja teikumu "Č.S. 1967 ir tēvs četriem bērniem – diviem zēniem un divām meitenēm" izmantotu ciematā, kur dzīvo Čārlzs Spensers, Spensera kungu varētu viegli atpazīt. Pseidonimizācijas metode var ietekmēt datu aizsardzības efektivitāti.

Personas dati ar šifrētiem vai atsevišķi turētiem atribūtiem daudzos gadījumos tiek izmantoti kā līdzeklis personas identitātes slepenības nodrošināšanai. Tas ir īpaši noderīgi gadījumos, kad datu pārziņiem ir jāpārliecinās, ka viņiem ir darīšana ar tiem

311 Vispārīgā datu aizsardzības regula, 32. panta 1. punkts.

312 Turpat.

pašiem datu subjektiem, bet viņiem nav nepieciešamas vai nevajadzētu būt nepieciešamām datu subjektu patiesajām identitātēm. Tas attiecas, piemēram, uz gadījumiem, kad pētnieks pēta slimības gaitu ar pacientiem, kuru identitāte ir zināma tikai slimnīcai, kur viņi tiek ārstēti, un no kuras pētnieks iegūst pseidonimizētas slimības vēstures. Tādēļ pseidonimizācija veido spēcīgu saikni ar privātumu uzlabojošām tehnoloģijām. Tā var darboties kā svarīgs elements, ieviešot integrētu privātuma aizsardzību. Tas nozīmē, ka datu aizsardzība ir jāiekļauj datu apstrādes sistēmu struktūrā.

VDAR 25. pantā, kurā runa par integrētu datu aizsardzību, skaidri norādīts uz pseidonimizāciju kā attiecīgu tehnisko un organizatorisko pasākumu, kas pārziņiem ir jāveic, lai ievērotu datu aizsardzības principus un integrētu nepieciešamos aizsardzības pasākumus. To darot, pārziņi izpildīs regulas prasības un aizsargās datu subjektu tiesības, apstrādājot viņu personas datus.

Apstiprināta rīcības kodeksa vai apstiprināta sertifikācijas mehānisma ievērošana var palīdzēt pierādīt atbilstību apstrādes drošības prasībām[313]. Eiropas Padome savā atzinumā par pasažieru datu reģistra apstrādes ietekmi uz datu aizsardzību sniedz citus piemērotu drošības pasākumu piemērus personas datu aizsardzībai pasažieru vārdu reģistru sistēmās. Tie ietver datu glabāšanu drošā fiziskā vidē, piekļuves kontroles ierobežošanu, izmantojot daudzslāņu pierakstīšanos, un datu paziņošanas aizsardzību ar spēcīgu kriptogrāfiju[314].

> Piemērs. Sociālo tīklu vietnes un e-pasta pakalpojumu sniedzēji ļauj lietotājiem pievienot papildu datu drošības līmeni sniegtajiem pakalpojumiem, ieviešot divlīmeņu autentifikāciju. Papildus personīgās paroles ievadīšanai lietotājiem ir jāveic arī otrā pierakstīšanās, lai piekļūtu savam personīgajam kontam. Pēdējais varētu būt, piemēram, drošības koda, kas nosūtīts uz personīgajam kontam piesaistīto mobilā tālruņa numuru, ievadīšana. Tādā veidā divpakāpju verifikācija nodrošina labāku personiskās informācijas aizsardzību pret neatļautu piekļuvi personīgajiem kontiem, tos uzlaužot.

Modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā ir sniegti attiecīgu drošības pasākumu papildu piemēri, piemēram, dienesta noslēpuma glabāšanas pienākuma ieviešana vai kvalificētu tehniskās drošības pasākumu, piemēram, datu šifrēšanas,

313 Turpat, 32. panta 3. punkts.

314 Eiropas Padomes Konvencijas Nr. 108 komiteja, *Atzinums par Pasažieru datu reģistra apstrādes datu aizsardzības sekām*, T-PD(2016)18rev, 2016. gada 19. augusts, 9. lpp.

pieņemšana[315]. Ieviešot īpašus drošības pasākumus, pārzinim vai, attiecīgā gadījumā, apstrādātājam ir jāņem vērā vairāki elementi, piemēram, apstrādāto personas datu raksturs un apjoms, iespējamās nelabvēlīgās sekas datu subjektiem, kā arī nepieciešamība ierobežot piekļuvi datiem[316]. Īstenojot attiecīgus drošības pasākumus, jāņem vērā pašreizējais datu drošības metožu un datu apstrādes paņēmienu tehnikas līmenis. Šādu pasākumu izmaksām jābūt proporcionālām potenciālo risku nopietnībai un iespējamībai. Drošības pasākumi ir regulāri jāpārskata, lai vajadzības gadījumā tos varētu atjaunināt[317].

Gadījumos, kad notiek personas datu aizsardzības pārkāpums, gan modernizētajā Konvencijā Nr. 108, gan VDAR tiek prasīts, lai pārzinis bez nepamatotas kavēšanās informētu kompetento uzraudzības iestādi par pārkāpumu, kas rada risku personu tiesībām un brīvībām[318]. Līdzīgs paziņošanas datu subjektam pienākums pastāv, ja personas datu aizsardzības pārkāpums, iespējams, rada lielu risku viņa tiesībām un brīvībām[319]. Par šādiem pārkāpumiem datu subjekts jāinformē skaidri un saprotami[320]. Ja apstrādātājs uzzina par personas datu aizsardzības pārkāpumu, par to nekavējoties jāpaziņo pārzinim[321]. Noteiktās situācijās var piemērot izņēmumus paziņošanas pienākumam. Piemēram, pārzinim nav jāziņo uzraudzības iestādei, ja "ir maz ticams, ka personas datu aizsardzības pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām"[322]. Nav arī jāpaziņo datu subjektam gadījumos, ja īstenotie drošības pasākumi padara datus nepilnvarotām personām nesaprotamus vai ja turpmākie pasākumi nodrošina, ka liels risks visticamāk vairs nepastāv[323]. Ja personīga pārkāpuma paziņošana datu subjektiem pārziņa vārdā sagādātu nesamērīgas pūles, publiska saziņa vai līdzīgs pasākums var nodrošināt, ka "datu subjekti tiek informēti vienlīdz efektīvā veidā"[324].

315 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 56. punkts.

316 Turpat, 62. punkts.

317 Turpat, 63. punkts.

318 Modernizētā Konvencija Nr. 108, 7. panta 2. punkts; Vispārīgā datu aizsardzības regula, 33. panta 1. punkts.

319 Modernizētā Konvencija Nr. 108, 7. panta 2. punkts; Vispārīgā datu aizsardzības regula, 34. panta 1. punkts.

320 Vispārīgā datu aizsardzības regula, 34. panta 2. punkts.

321 Turpat, 33. panta 1. punkts.

322 Turpat, 32. panta 1. punkts.

323 Turpat, 34. panta 3. punkta a) un b) apakšpunkts.

324 Turpat, 34. panta 3. punkta c) apakšpunkts.

3.7. Pārskatatbildības princips

Svarīgākie aspekti

- Pārskatatbildība uzliek pārziņiem un apstrādātājiem pienākumu aktīvi un nepārtraukti īstenot pasākumus, lai veicinātu un nodrošinātu datu aizsardzību savās apstrādes darbībās.
- Pārziņi un apstrādātāji ir atbildīgi par to veikto apstrādes darbību atbilstību datu aizsardzības tiesību aktiem un katra attiecīgajiem pienākumiem.
- Pārziņiem jāspēj jebkurā laikā pierādīt datu subjektiem, plašākai sabiedrībai un uzraudzības iestādēm sava atbilstība datu aizsardzības noteikumiem. Apstrādātājiem jāievēro arī daži pienākumi, kas ir cieši saistīti ar pārskatatbildību (piemēram, apstrādes operāciju uzskaite un datu aizsardzības speciālista iecelšana).

VDAR un modernizētajā Konvencijā Nr. 108 ir noteikts, ka pārzinis atbild par šajā nodaļā aprakstītajiem personas datu apstrādes principiem un viņam jāspēj pierādīt savu atbilstību tiem[325]. Šajā nolūkā pārzinim ir jāievieš attiecīgi tehniski un organizatoriski pasākumi[326]. Kaut arī VDAR 5. panta 2. punktā noteiktais pārskatatbildības princips ir vērsts tikai uz pārziņiem, tiek sagaidīts, ka arī apstrādātāji būs atbildīgi, ņemot vērā, ka viņiem ir jāpilda vairāki pienākumi un ka tie ir cieši saistīti ar pārskatatbildību.

ES un EP datu aizsardzības tiesību aktos arī noteikts, ka pārzinis ir atbildīgs par datu aizsardzības principu, kas apspriesti 3.1.–3.6. iedaļā, ievērošanu, un viņam jāspēj to nodrošināt[327]. 29. panta darba grupa norāda, ka "procedūru un mehānismu veids var atšķirties atkarībā no riskiem, kādus rada datu apstrāde, un no datu rakstura"[328].

Pārziņi var veicināt šīs prasības izpildi dažādos veidos, tostarp:

- reģistrēt apstrādes darbības un pēc pieprasījuma padarīt tās pieejamas uzraudzības iestādei[329];

325 Turpat, 5. panta 2. punkts, modernizētā Konvencija Nr. 108, 10. panta 1. punkts.

326 Vispārīgā datu aizsardzības regula, 24. pants.

327 Turpat, 5. panta 2. punkts, modernizētā Konvencija Nr. 108, 10. panta 1. punkts.

328 29. panta darba grupa, Atzinums 3/2010 par pārskatatbildības principu, WP 173, Brisele, 2010. gada 13. jūlijs, 12. punkts.

329 Vispārīgā datu aizsardzības regula, 30. pants.

- noteiktās situācijās iecelt datu aizsardzības speciālistu, kurš ir iesaistīts visos ar personas datu aizsardzību saistītajos jautājumos[330];

- veikt datu aizsardzības ietekmes novērtējumus apstrādes veidiem, kas varētu radīt lielu risku fizisko personu tiesībām un brīvībām[331];

- nodrošināt integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma[332];

- ieviest kārtību un procedūras datu subjektu tiesību īstenošanai[333];

- ievērot apstiprinātos rīcības kodeksus vai sertifikācijas mehānismus[334].

Kaut arī VDAR 5. panta 2. punktā noteiktais pārskatatbildības princips nav vērsts īpaši uz apstrādātājiem, pastāv ar pārskatatbildību saistītas normas, kas ietver arī uz viņiem attiecināmus pienākumus, piemēram, apstrādes darbību uzskaiti un datu aizsardzības speciālista iecelšanu jebkurām apstrādes darbībām, kurām tāds ir nepieciešams[335]. Apstrādātājiem arī jānodrošina, ka tiek īstenoti visi datu drošības garantēšanai nepieciešamie pasākumi[336]. Juridiski saistošā līgumā starp pārzini un apstrādātāju jāparedz, ka apstrādātājs palīdz pārzinim izpildīt dažas atbilstības prasības, piemēram, veicot datu aizsardzības ietekmes novērtējumu vai informējot pārzini par visiem personas datu aizsardzības pārkāpumiem, tiklīdz viņiem tādi kļūst zināmi[337].

Ekonomiskās sadarbības un attīstības organizācija (ESAO) 2013. gadā pieņēma privātuma pamatnostādnes, kurās tika uzsvērts, ka pārziņiem ir svarīga funkcija datu aizsardzības nodrošināšanai praksē. Pamatnostādnēs ir ietverts pārskatatbildības princips, saskaņā ar kuru "datu pārzinim jāuzņemas atbildība par to pasākumu ieviešanu, ar kuriem tiek īstenoti iepriekš minētie [būtiskie] principi"[338].

330 Turpat, 37.–39. punkts.

331 Turpat, 35. pants, modernizētā Konvencija Nr. 108, 10. panta 2. punkts.

332 Vispārīgā datu aizsardzības regula, 25. pants; modernizētā Konvencija Nr. 108, 10. panta 2. un 3. punkts.

333 Turpat, 12. un 24. pants.

334 Turpat, 40. un 42. pants.

335 Turpat, 5. panta 2. punkts, 30. un 37. pants.

336 Turpat, 28. panta 3. punkta c) apakšpunkts.

337 Turpat, 28. panta 3. punkta d) apakšpunkts.

338 ESAO (2013) *Pamatnostādnes par privātās dzīves aizsardzību un personas datu pārrobežu plūsmu*, 14. pants.

Piemērs. Likumdošanas piemērs, kurā uzsvērts pārskatatbildības princips, ir 2009. gada grozījumi[339] E-privātuma direktīvā 2002/58/EK. Atbilstoši grozītajam 4. pantam direktīva uzliek pienākumu "nodrošināt, ka tiek īstenota drošības politika saistībā ar personas datu apstrādi". Tādējādi, ciktāl tas attiecas uz šīs direktīvas drošības noteikumiem, likumdevējs lēma, ka ir jāievieš viennozīmīga prasība par drošības politikas izstrādi un ieviešanu.

Atbilstoši 29. panta darba grupas atzinumam[340] pārskatatbildības būtība ir šādi pārziņa pienākumi:

- īstenot pasākumus, kas normālos apstākļos garantētu datu aizsardzības noteikumu ievērošanu apstrādes darbību kontekstā; un

- sagatavot dokumentāciju, ar ko datu subjektiem un uzraudzības iestādēm parāda pasākumus, kas veikti, lai panāktu atbilstību datu aizsardzības noteikumiem.

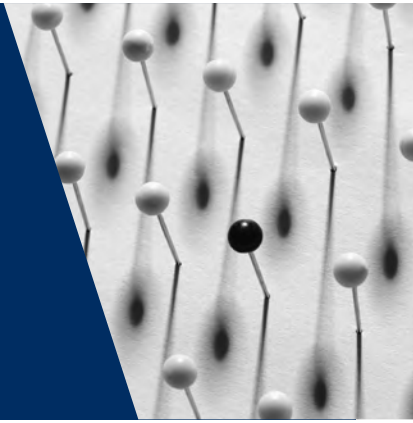
Tādējādi pārskatatbildības princips uzliek pārziņiem pienākumu aktīvi pierādīt atbilstību, nevis tikai gaidīt, kamēr datu subjekti vai uzraudzības iestādes norāda trūkumus.

339 Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīva 2009/136/EK, ar ko groza Direktīvu 2002/22/EK par universālo pakalpojumu un lietotāju tiesībām attiecībā uz elektronisko sakaru tīkliem un pakalpojumiem, Direktīvu 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē un Regulu (EK) Nr. 2006/2004 par sadarbību starp valstu iestādēm, kas atbildīgas par tiesību aktu īstenošanu patērētāju tiesību aizsardzības jomā, OV 2009 L 337, 11. lpp.

340 29. panta darba grupa, *Atzinums 3/2010 par pārskatatbildības principu*, WP 173, Brisele, 2010. gada 13. jūlijs.

4

Eiropas tiesību aktu datu aizsardzības jomā noteikumi



ES	Aptvertie jautājumi	EP
Likumīgas datu apstrādes noteikumi		
Vispārīgā datu aizsardzības regula, 6. panta 1. punkta a) apakšpunkts EST lieta C-543/09 *Deutsche Telekom AG pret Vācijas Federatīvo Republiku*, 2011 EST lieta C-536/15 *Tele2 (Netherlands) BV un citi pret Autoriteit Consument en Markt (AMC)*, 2017	**Piekrišana**	Ieteikums par profilēšanu, 3.4. punkta b) apakšpunkts un 3.6. punkts Modernizētā Konvencija Nr. 108, 5. panta 2. punkts
Vispārīgā datu aizsardzības regula, 6. panta 1. punkta b) apakšpunkts	**Pirmslīgumiskās attiecības**	Ieteikums par profilēšanu, 3.4. punkta b) apakšpunkts
Vispārīgā datu aizsardzības regula, 6. panta 1. punkta c) apakšpunkts	**Pārziņa juridiskie pienākumi**	Ieteikums par profilēšanu, 3.4. punkta a) apakšpunkts
Vispārīgā datu aizsardzības regula, 6. panta 1. punkta d) apakšpunkts	**Datu subjekta vitālās intereses**	Ieteikums par profilēšanu, 3.4. punkta b) apakšpunkts
Vispārīgā datu aizsardzības regula, 6. panta 1. punkta e) apakšpunkts EST lieta C-524/06 *Huber pret Vācijas Federatīvo Republiku* [GC], 2008	**Sabiedrības intereses un oficiālo pilnvaru īstenošana**	Ieteikums par profilēšanu, 3.4. punkta b) apakšpunkts

ES	Aptvertie jautājumi	EP
Vispārīgā datu aizsardzības regula, 6. panta 1. punkta f) apakšpunkts EST lieta C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde pret Rīgas pašvaldības SIA "Rīgas satiksme"*, 2017 EST apvienotās lietas C-468/10 un C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) un Federación de Comercio Electrónico y Marketing Directo (FECEMD) pret Administración del Estado*, 2011	**Citu leģitīmās intereses**	Ieteikums par profilēšanu, 3.4. punkta b) apakšpunkts ECT lieta *Y pret Turciju*, Nr. 648/10, 2015
Vispārīgā datu aizsardzības regula, 6. panta 4. punkts	**Nolūka ierobežojuma izņēmumi: tālāka apstrāde citiem nolūkiem**	Modernizētā Konvencija Nr. 108, 5. panta 4. punkta b) apakšpunkts
Sensitīvu datu likumīgas apstrādes noteikumi		
Vispārīgā datu aizsardzības regula, 9. panta 1. punkts	**Vispārējs aizliegums veikt apstrādi**	Modernizētā Konvencija Nr. 108, 6. pants
Vispārīgā datu aizsardzības regula, 9. panta 2. punkts	**Vispārējā aizlieguma izņēmumi**	Modernizētā Konvencija Nr. 108, 6. pants
Drošas apstrādes noteikumi		
Vispārīgā datu aizsardzības regula, 32. pants	**Pienākums nodrošināt drošu apstrādi**	Modernizētā Konvencija Nr. 108, 7. panta 1. punkts ECT lieta *I. pret Somiju*, Nr. 20511/03, 2008
Vispārīgā datu aizsardzības regula, 28. pants, 32. panta 1. punkta b) apakšpunkts	**Pienākums ievērot konfidencialitāti**	Modernizētā Konvencija Nr. 108, 7. panta 1. punkts
Vispārīgā datu aizsardzības regula, 34. pants Direktīva par privāto dzīvi un elektronisko komunikāciju, 4. panta 2. punkts	**Paziņojumi par datu aizsardzības pārkāpumiem**	Modernizētā Konvencija Nr. 108, 7. panta 2. punkts
Pārskatatbildības un atbilstības veicināšanas noteikumi		
Vispārīgā datu aizsardzības regula, 12., 13. un 14. pants	**Pārredzamība kopumā**	Modernizētā Konvencija Nr. 108, 8. pants
Vispārīgā datu aizsardzības regula, 37., 38. un 39. pants	**Datu aizsardzības speciālisti**	Modernizētā Konvencija Nr. 108, 10. panta 1. punkts

ES	Aptvertie jautājumi	EP
Vispārīgā datu aizsardzības regula, 30. pants	Apstrādes darbību reģistrēšana	
Vispārīgā datu aizsardzības regula, 35. un 36. pants	Ietekmes novērtējums un iepriekšēja apspriešanās	Modernizētā Konvencija Nr. 108, 10. panta 2. punkts
Vispārīgā datu aizsardzības regula, 33. un 34. pants	Paziņojumi par datu aizsardzības pārkāpumiem	Modernizētā Konvencija Nr. 108, 7. panta 2. punkts
Vispārīgā datu aizsardzības regula, 40. un 41. pants	Rīcības kodeksi	
Vispārīgā datu aizsardzības regula, 42. un 43. pants	Sertifikācija	
Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma		
Vispārīgā datu aizsardzības regula, 25. panta 1. punkta a) apakšpunkts	Integrēta datu aizsardzība	Modernizētā Konvencija Nr. 108, 10. panta 2. punkts
Vispārīgā datu aizsardzības regula, 25. panta 1. punkta b) apakšpunkts	Datu aizsardzība pēc noklusējuma	Modernizētā Konvencija Nr. 108, 10. panta 3. punkts

Principiem vienmēr ir vispārējs raksturs. To piemērošana konkrētās situācijās atstāj zināmu interpretācijas un līdzekļu izvēles iespēju. Saskaņā ar **EP tiesību aktiem** modernizētās Konvencijas Nr. 108 dalībvalstīm ir pienākums skaidrot šīs interpretācijas robežas savos tiesību aktos. **ES tiesību aktos** ir atšķirīga pieeja: lai izveidotu datu aizsardzību iekšējā tirgū, tika uzskatīts par nepieciešamu ES mērogā ieviest detalizētākus noteikumus, lai saskaņotu datu aizsardzības līmeni dalībvalstu tiesību aktos. Ar Vispārīgo datu aizsardzības regulu izveido detalizēti izstrādātus noteikumus saskaņā ar tās 5. pantā izklāstītajiem principiem, kas ir tieši piemērojami valsts tiesību sistēmā. Turpmāk sniegtās piezīmes par detalizētiem datu aizsardzības noteikumiem Eiropas mērogā galvenokārt attiecas uz ES tiesību aktiem.

4.1. Likumīgas apstrādes noteikumi

Svarīgākie aspekti

- Personas datus var likumīgi apstrādāt, ja tie atbilst vienam no šiem kritērijiem:
  - apstrādes pamatā ir datu subjekta piekrišana;
  - personas datu apstrāde ir nepieciešama līgumattiecību īstenošanai;
  - apstrāde ir nepieciešama, lai pārzinis varētu izpildīt savus juridiskos pienākumus;
  - datu subjektu vai citas personas vitālo interešu nodrošināšanai ir nepieciešama viņu datu apstrāde;
  - apstrāde ir vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs;
  - apstrādes iemesls ir pārziņu vai trešo personu likumīgās intereses, taču tikai tiktāl, ciktāl datu subjektu intereses vai pamattiesības nav svarīgākas.
- Sensitīvu personas datu likumīgai apstrādei piemēro īpašu stingrāku režīmu.

4.1.1. Datu apstrādes likumīgais pamats

Vispārīgās datu aizsardzības regulas II nodaļā "Principi" ir noteikts, ka, veicot personas datu apstrādi, pirmkārt, jāievēro principi, kas attiecas uz datu kvalitāti, kā noteikts VDAR 5. pantā. Viens no principiem ir tāds, ka personas dati ir jāapstrādā "likumīgi, godprātīgi un pārskatāmi". Otrkārt, lai dati tiktu apstrādāti likumīgi, apstrādei ir jāatbilst vienam no datu apstrādes likumīgajiem pamatiem, kuri uzskaitīti 6. pantā[341] attiecībā uz personas datiem, kas nav sensitīvi, un 9. pantā attiecībā uz īpašām datu kategorijām (jeb sensitīviem datiem). Tāpat modernizētās Konvencijas Nr. 108 II nodaļā, kurā izklāstīti "personas datu aizsardzības pamatprincipi", noteikts, ka datu apstrādei, lai tā būtu likumīga, ir jābūt "samērīgai attiecībā uz izvirzīto likumīgo mērķi".

341 EST 2003. gada 20. maija spriedums apvienotajās lietās C-465/00, C-138/01 un C-139/01 *Rechnungshof pret Österreichischer Rundfunk un citiem* un *Christa Neukomm un Jospeh Lauermann pret Österreichischer Rundfunk*, 65. punkts; EST 2008. gada 16. decembra spriedums lietā C-524/06 *Heinz Huber pret Vācijas Federatīvo Republiku* [GC], 48. punkts; EST 2011. gada 24. novembra spriedums apvienotajās lietās C-468/10 un C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) un Federación de Comercio Electrónico y Marketing Directo (FECEMD) pret Administración del Estado*, 26. punkts.

Neatkarīgi no apstrādes likumīgā pamata, uz kuru pārzinis atsaucas, lai uzsāktu personas datu apstrādes darbību, pārzinim jāpiemēro arī drošības pasākumi, kas paredzēti vispārējā datu aizsardzības likuma režīmā.

Piekrišana

EP tiesību aktos piekrišana ir minēta modernizētās Konvencijas Nr. 108 5. panta 2. punktā. Tā ir minēta arī ECT judikatūrā un vairākos EP ieteikumos[342]. **ES tiesību aktos** piekrišana kā likumīgs datu apstrādes pamats ir cieši nostiprināta VDAR 6. pantā, kā arī skaidri minēta Hartas 8. pantā. Derīgas piekrišanas pazīmes ir izskaidrotas piekrišanas definīcijā 4. pantā, savukārt derīgas piekrišanas iegūšanas nosacījumi ir detalizēti izklāstīti 7. pantā, savukārt īpašie noteikumi bērna piekrišanai attiecībā uz informācijas sabiedrības pakalpojumiem noteikti VDAR 8. pantā.

Kā paskaidrots 2.4. iedaļā, piekrišanai jābūt labprātīgi sniegtai, apzinātai, konkrētai un nepārprotamai. Piekrišanai ir jābūt paziņojumam vai skaidri apstiprinošai rīcībai, kas nozīmē piekrišanu apstrādei, un personai ir tiesības jebkurā laikā atsaukt šo piekrišanu. Pārziņiem ir pienākums turēt pārbaudāmu piekrišanas reģistru.

Labprātīga piekrišana

EP modernizētās Konvencijas Nr. 108 ietvaros datu subjekta piekrišanai "ir jāatspoguļo apzinātas izvēles brīva izpausme"[343]. Brīvi sniegta piekrišana ir spēkā tikai tad, "kad datu subjektam ir reālas izvēles iespējas bez maldināšanas, iebiedēšanas, piespiešanas vai ievērojamu negatīvu seku riska, ja persona nepiekrīt datu apstrādei"[344]. Šajā sakarībā **ES tiesību aktos** noteikts, ka piekrišana netiek uzskatīta par labprātīgi sniegtu, "ja datu subjektam nav īstas vai brīvas izvēles vai viņš nevar atteikties vai atsaukt savu izvēli bez nelabvēlīgām sekām"[345]. VDAR uzsvērts, ka "novērtējot to, vai piekrišana ir dota brīvi, maksimāli ņem vērā to, vai cita starpā līguma izpilde, tostarp pakalpojuma sniegšana, ir atkarīga no piekrišanas tādai

342 Skatīt, piemēram, Eiropas Padome, Ministru komiteja, (2010) Ministru komitejas Ieteikums CM/Rec(2010)13 dalībvalstīm par fizisko personu aizsardzību attiecībā uz personas datu automātisku apstrādi datu profilu veidošanas kontekstā (Ieteikums par profilēšanu), 2010. gada 23. novembris, 3.4. punkta b) apakšpunkts.

343 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 42. punkts.

344 Skatīt arī 29. panta darba grupas (2011) *Atzinumu 15/2011 par jēdziena "piekrišana" definīciju*, WP 187, Brisele, 2011. gada 13. jūlijs, 12. lpp.

345 Vispārīgā datu aizsardzības regula, 42. apsvērums.

personas datu apstrādei, kura nav nepieciešama minētā līguma izpildei"[346]. Modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā teikts, ka "uz datu subjektu var tikt izdarīta nepamatota tieša vai netieša ietekme vai spiediens (kam var būt ekonomisks vai cits raksturs), un piekrišana nav jāuzskata par labprātīgi sniegtu. ja datu subjektam nav īstas izvēles vai viņam nav iespējas atteikties vai atsaukt piekrišanu bez nelabvēlīgām sekām"[347].

Piemērs. Dažas A valsts pašvaldības nolēma izstrādāt uzturēšanās atļaujas ar iebūvētu mikroshēmu. Iedzīvotājiem šīs elektroniskās kartes nav obligātas. Tomēr iedzīvotājiem, kuriem nav kartes, nav piekļuves virknei svarīgu administratīvo pakalpojumu, piemēram, iespējai tiešsaistē samaksāt pašvaldības nodokļus, elektroniski iesniegt sūdzības, izmantojot iestāžu atbilžu sniegšanai noteikto trīs dienu termiņu, un bez rindas apmeklēt pašvaldības koncertzāli, nopirkt biļetes ar atlaidi un pie ieejas izmantot skenerus.

Pašvaldību veiktā personas datu apstrāde šajā piemērā nevar būt balstīta uz piekrišanu. Tā kā pastāv vismaz netiešs spiediens uz iedzīvotājiem saņemt elektronisko karti un piekrist apstrādei, piekrišana nav sniegta labprātīgi. Tādējādi pašvaldību elektronisko karšu sistēmas izstrādei jābūt balstītai uz citu likumīgu pamatu, kas attaisno apstrādi. Piemēram, tās varētu atsaukties uz to, ka apstrāde ir nepieciešama, lai izpildītu uzdevumu, ko veic sabiedrības interesēs, kas ir likumīgs pamats apstrādei saskaņā ar VDAR 6. panta 1. punkta e) apakšpunktu[348].

Par labprātīgu piekrišanu var būt šaubas arī pakļautības situācijās, kad pastāv ievērojama ekonomiska vai cita nelīdzsvarotība starp pārzini, kurš nodrošina piekrišanu, un datu subjektu, kurš sniedz piekrišanu[349]. Tipisks šādas nelīdzsvarotības un pakļautības piemērs ir darba devēja veikta personas datu apstrāde darba attiecību

346 Turpat, 7. panta 4. punkts.

347 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 42. punkts.

348 29. panta darba grupa (2011), *Atzinums 15/2011 par jēdziena "piekrišana" definīciju*, WP 187, Brisele, 2011. gada 13. jūlijs, 16. lpp. Papildu piemēri gadījumiem, kad datu apstrāde nevar balstīties uz piekrišanu un ir nepieciešams atšķirīgs juridiskais pamats apstrādes likumīgumam, ir atrodami atzinuma 14. un 17. lpp.

349 Skatīt 29. gada darba grupas (2001) *Atzinumu 8/2001 par personas datu apstrādi nodarbinātības kontekstā*, WP 48, Brisele, 2001. gada 13. septembris; 29. panta darba grupas (2005) Darba dokumentu par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta vienotu interpretāciju, WP 114, Brisele, 2005. gada 25. novembris; 29. panta darba grupas (2017) *Atzinumu 2/2017 par datu apstrādi darbā*, WP 249, Brisele, 2017. gada 8. jūnijs.

kontekstā. Atbilstoši 29. panta darba grupas teiktajam "darba ņēmēji gandrīz nekad nevar labprātīgi sniegt, atteikt vai atsaukt piekrišanu, ņemot vērā atkarību, kas izriet no darba devēja/darbinieka attiecībām. Ņemot vērā varas nelīdzsvarotību, darbinieki var sniegt labprātīgu piekrišanu tikai izņēmuma gadījumos, kad piedāvājuma pieņemšana vai noraidīšana nerada nekādas sekas"[350].

Piemērs. Liels uzņēmums plāno izveidot direktoriju, kurā būtu iekļauti visu darbinieku vārdi, viņu funkcijas uzņēmumā un viņu darba adreses, lai uzlabotu uzņēmuma iekšējo komunikāciju. Personāla vadītājs ierosina direktorijā pievienot katra darbinieka fotoattēlu, lai sanāksmēs būtu vieglāk atpazīt kolēģus. Darbinieku pārstāvji pieprasa, lai tas tiktu darīts tikai tad, ja katrs atsevišķais darbinieks tam piekrīt.

Šādā situācijā darbinieka piekrišana ir jāatzīst par juridisko pamatu fotoattēlu apstrādei direktorijā, jo visticamāk darbiniekam neiestāsies nekādas sekas neatkarīgi no tā, vai viņš nolemj piekrist sava fotoattēla publicēšanai direktorijā.

Piemērs. Uzņēmums A plāno tikšanos, kurā piedalīsies trīs tā darbinieki un uzņēmuma B direktori, lai pārrunātu iespējamo turpmāko sadarbību projektā. Sanāksme notiks uzņēmuma B telpās, un tas lūdz uzņēmumu A pa e-pastu nosūtīt sapulces dalībnieku vārdus, CV un fotoattēlus. Uzņēmums B apgalvo, ka tam nepieciešami dalībnieku vārdi un fotoattēli, lai apsardzes darbinieki pie ēkas ieejas varētu pārbaudīt, vai tās ir īstās personas, savukārt CV palīdzēs direktoriem labāk sagatavoties sapulcei. Šajā gadījumā uzņēmuma A personas datu pārsūtīšana nevar būt balstīta uz piekrišanu. Piekrišanu nevar uzskatīt par "labprātīgi sniegtu", jo pastāv iespēja, ka darbinieki saskarsies ar negatīvām sekām, noraidot piedāvājumu (piemēram, viņus var aizstāt cits kolēģis, ne tikai apmeklējot sanāksmi, bet arī sazinoties ar uzņēmumu B un strādājot pie projekta kopumā). Tāpēc apstrādei jābalstās uz citu likumīgo pamatu.

Tas tomēr nenozīmē, ka piekrišana nevar būt derīga apstākļos, kad piekrišanas nepiešķiršanai būtu kādas negatīvas sekas. Piemēram, ja, nesniedzot piekrišanu lielveikala klienta kartei, netiek saņemts tikai neliels cenu samazinājums atsevišķām precēm, piekrišana varētu būt derīgs juridiskais pamats to klientu personas datu

350 29. panta darba grupa, *Atzinums 2/2017 par datu apstrādi darbā*, WP 249, Brisele, 2017. gada 8. jūnijs.

apstrādei, kuri piekrita šādas kartes saņemšanai. Starp uzņēmumu un klientu nav pakļautības attiecību, un piekrišanas nesniegšanas sekas nav pietiekami nopietnas, lai neļautu datu subjektam izdarīt brīvu izvēli (ar nosacījumu, ka cenas samazinājums ir pietiekami mazs, lai neietekmētu viņu brīvo izvēli).

Tomēr, ja preces vai pakalpojumus var iegūt tikai tad, ja pārzinim vai tālāk trešām personām tiek atklāti noteikti personas dati, datu subjekta piekrišanu izpaust savus datus, kas nav nepieciešami līguma izpildei, nevar uzskatīt par brīvi izdarītu lēmumu un tāpēc saskaņā ar datu aizsardzības tiesību aktiem šāda piekrišana nav spēkā[351]. VDAR ir noteikts diezgan stingrs aizliegums sasaistīt piekrišanu ar preču un pakalpojumu sniegšanu[352].

Piemērs. Pasažieru piekrišanu aviokompānijai, kas pārsūta tā sauktos pasažieru datu reģistrus (t. i., datus par viņu identitāti, ēšanas paradumiem vai veselības problēmām) konkrētas ārvalsts imigrācijas iestādēm, nevar uzskatīt par derīgu piekrišanu saskaņā ar datu aizsardzības tiesību aktiem, jo ceļojošajiem pasažieriem nav izvēles, ja viņi vēlas apmeklēt šo valsti. Lai šādus datus pārsūtītu likumīgi, ir nepieciešams cits juridiskais pamats, nevis piekrišana, visticamāk īpašs likums.

Apzināta piekrišana

Pirms izvēles izdarīšanas datu subjekta rīcībā ir jābūt pietiekamai informācijai. Apzināta piekrišana parasti satur precīzu un viegli saprotamu priekšmeta, kam nepieciešama piekrišana, aprakstu. Kā skaidro 29. panta darba grupa, piekrišanai jābūt balstītai uz faktu un datu subjekta rīcības, kas saistīta ar piekrišanu apstrādei, seku novērtējumu un izpratni. Tāpēc "attiecīgajai personai skaidri un saprotami jāsniedz precīza un pilnīga informācija par visiem būtiskajiem jautājumiem (..), piemēram, apstrādāto datu raksturu, apstrādes nolūkiem, iespējamajiem saņēmējiem un datu subjekta tiesībām"[353]. Lai piekrišana būtu apzināta, indivīdiem ir jāapzinās arī sekas, ko rada nepiekrišana apstrādei.

Ņemot vērā apzinātas piekrišanas nozīmi, VDAR un modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā mēģināja precizēt šo jēdzienu. VDAR apsvērumos noteikts, ka apzināta piekrišana nozīmē, ka "datu subjektam vajadzētu būt

351 Vispārīgā datu aizsardzības regula, 7. panta 4. punkts.

352 Turpat.

353 29. panta darba grupa (2007), Darba dokuments par personas ar veselību saistīto datu apstrādi elektroniskajās pacienta veselības kartēs (EVK), WP 131, Brisele, 2007. gada 15. februāris.

informētam vismaz par pārziņa identitāti un paredzētās personas datu apstrādes nolūkiem"[354].

Izņēmuma gadījumā, ja piekrišana tiek izmantota kā atkāpe, lai nodrošinātu likumīgu pamatu starptautiskai datu nosūtīšanai, pārzinim ir jāinformē datu subjekts par iespējamiem šādas nosūtīšanas riskiem, ja nav pieņemts lēmums par aizsardzības līmeņa pietiekamību un nav atbilstošu garantiju, lai šī piekrišana tiktu uzskatīta par derīgu[355].

Modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā norādīts, ka jāsniedz informācija par datu subjekta lēmuma sekām, proti, "ko ietver sevī piekrišanas fakts un ciktāl šī piekrišana tiek sniegta"[356].

Informācijas kvalitāte ir svarīga. Informācijas kvalitāte nozīmē, ka informācijas valoda ir jāpielāgo tās paredzamajiem saņēmējiem. Informācijā nedrīkst izmantot žargonu, tā jāsniedz skaidrā un saprotamā valodā, ko parastais lietotājs varētu saprast[357]. Informācijai jābūt datu subjektam viegli pieejamai, to var sniegt mutiski vai rakstiski. Informācijas pieejamība un atpazīstamība ir svarīgi elementi: informācijai jābūt skaidri redzamai un pamanāmai. Tiešsaistes vidē daudzslāņu informācijas paziņojumi var būt labs risinājums, jo tie ļauj datu subjektiem izvēlēties lasīt īsāku vai plašāku informācijas versiju.

Konkrēta piekrišana

Lai piekrišana būtu derīga, tai jāattiecas tieši uz apstrādes nolūku, kas skaidri un nepārprotami jāapraksta. Tas ir cieši saistīts ar informācijas, kas sniegta par piekrišanas nolūku, kvalitāti. Šajā sakarībā būtiskas būs vidusmēra datu subjekta pamatotās cerības. Datu subjektam atkārtoti jālūdz sniegt piekrišanu, ja apstrādes darbības ir jāpievieno vai jāmaina veidā, ko nevarēja pamatoti paredzēt brīdī, kad tika sniegta sākotnējā piekrišana, un tādējādi mainīts nolūks. Ja apstrādei ir vairāki nolūki, piekrišana ir jādod visiem nolūkiem[358].

354 Vispārīgā datu aizsardzības regula, 42. apsvērums.

355 Turpat, 49. panta 1. punkta a) apakšpunkts.

356 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 42. punkts.

357 29. panta darba grupa (2011), *Atzinums 15/2011 par jēdziena "piekrišana" definīciju*, WP187, Brisele, 2011. gada 13. jūlijs, 19. lpp.

358 Vispārīgā datu aizsardzības regula, 32. apsvērums.

Piemēri. Lietā *Deutsche Telekom AG*[359] EST apsvēra, vai telekomunikāciju pakalpojumu sniedzējam, kuram bija jānodod abonentu personas dati publicēšanai katalogos, ir nepieciešama atkārtota datu subjektu piekrišana[360], jo datu saņēmēji sākotnēji netika nosaukti, kad piekrišana tika sniegta.

EST uzskatīja, ka saskaņā ar Direktīvas par privātumu un elektronisko komunikāciju 12. pantu pirms datu nodošanas atjaunota piekrišana nav nepieciešama. Tā kā datu subjektiem bija tikai iespēja piekrist apstrādes nolūkam, kas bija viņu datu publicēšana, viņiem nebija iespējas izvēlēties starp dažādiem katalogiem, kuros šos datus varētu publicēt.

Kā uzsvēra EST, "interpretējot Direktīvas par privāto dzīvi un elektronisko komunikāciju 12. pantu kontekstuāli un sistēmiski, ir jāsecina, ka piekrišana atbilstoši šī panta otrajam punktam attiecas uz personas datu publicēšanas publiskā sarakstā nolūku, nevis uz attiecīgā abonentu saraksta pakalpojumu sniedzēja personu"[361]. Turklāt "personas datu publicēšana abonentu sarakstā, kam ir īpašs nolūks, abonentam pati par sevi rada zaudējumus[362]", nevis izdevēja identitātes jautājums.

Lietā *Tele2 (Nīderlande) BV, Ziggo BV, Vodafone Libertel BV pret Autoriteit Consument en Markt (AMC)*[363] skāra Beļģijas uzņēmuma pieprasījumu telefona uzziņu pakalpojumiem un abonentu sarakstiem uzņēmumos, kuri piešķir tālruņu numurus Nīderlandē, nodrošināt tam piekļuvi datiem, kas saistīti ar viņu abonentiem. Beļģijas uzņēmums atsaucās uz pienākumu saskaņā ar universālo pakalpojumu direktīvu[364]. Tas uzliek pienākumu uzņēmumiem, kas piešķir tālruņu numurus, padarīt numurus pieejamus abonentu sarakstiem,

359 EST 2011. gada 5. maija spriedums lietā C-543/09 *Deutsche Telekom AG pret Vācijas Federatīvo Republiku*. Skatīt jo īpaši 53. un 54. punkts.

360 Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē, OV 2002 L 201 (Direktīva par privāto dzīvi un elektronisko komunikāciju).

361 EST 2011. gada 5. maija spriedums lietā C-543/09 *Deutsche Telekom AG pret Vācijas Federatīvo Republiku*, 61. punkts.

362 Turpat, 62. punkts.

363 EST 2017. gada 15. marta spriedums lietā C-536/15 *Tele2 (Netherlands) BV un citi pret Autoriteit Consument en Markt (AMC)*.

364 Eiropas Parlamenta un Padomes 2002. gada 7. marta Direktīva 2002/22/EK par universālo pakalpojumu un lietotāju tiesībām attiecībā uz elektronisko sakaru tīkliem un pakalpojumiem (universālā pakalpojuma direktīva), OV 2002 L 108, 51. lpp., kura grozīta ar Eiropas Parlamenta un Padomes Direktīvu 2009/136/EK (2009. gada 25. novembris) (universālā pakalpojuma direktīva), OV 2009 L 337, 11. lpp.

kuri tos pieprasa, ja abonenti piekrīt savu numuru publicēšanai. Nīderlandes uzņēmumi atteicās to darīt, norādot, ka tiem nav jāsniedz attiecīgie dati uzņēmumam, kas reģistrēts citā dalībvalstī. Uzņēmumi apgalvoja, ka lietotāji ir devuši piekrišanu numuru publicēšanai, saprotot, ka tie tiks publicēti Nīderlandes abonentu sarakstā. EST nosprieda, ka universālā pakalpojumu direktīva attiecas uz visiem uzziņu pakalpojumu sniedzēju uzņēmumu pieprasījumiem neatkarīgi no to reģistrācijas dalībvalsts. EST arī nosprieda, ka to pašu datu nodošana citam uzņēmumam, kas plāno publicēt publisku abonentu sarakstu, nesaņemot atjaunotu abonentu piekrišanu, nevar nodarīt būtisku kaitējumu tiesībām uz personas datu aizsardzību[365]. Līdz ar to uzņēmumam, kas abonentiem piešķir tālruņa numurus, nav jānošķir abonentam adresētais piekrišanas pieprasījums atbilstoši tai dalībvalstij, kurai varētu tikt nosūtīti viņa dati[366].

Nepārprotama piekrišana

Jebkurai piekrišanai jābūt sniegtai nepārprotami[367]. Tas nozīmē, ka nevajadzētu būt pamatotām šaubām par to, ka datu subjekts ir vēlējies sniegt piekrišanu viņa/viņas datu apstrādei. Piemēram, datu subjekta bezdarbība nenorāda uz nepārprotamu piekrišanu.

Tas attiecas uz gadījumiem, kad pārzinis iegūst piekrišanu ar paziņojumiem savā privātuma politikā, piemēram, "izmantojot mūsu pakalpojumu, jūs piekrītat savu personas datu apstrādei". Tādā gadījumā pārzinim, iespējams, jānodrošina, ka lietotāji manuāli un individuāli piekrīt šādai politikai.

Ja piekrišana tiek sniegta rakstiski līguma ietvaros, piekrišana personas datu apstrādei ir jāindividualizē, un katrā ziņā "aizsardzības pasākumiem būtu jānodrošina, ka datu subjekts apzinās to, ka viņš sniedz piekrišanu un kādā apmērā viņš to dara"[368].

365 EST 2017. gada 15. marta spriedums lietā C-536/15 *Tele2 (Netherlands) BV un citi pret Autoriteit Consument en Markt (AMC)*, 36. punkts

366 Turpat, 40.–41. punkts.

367 Vispārīgā datu aizsardzības regula, 4. panta 11. punkts.

368 Turpat, 42. apsvērums.

Prasības piekrišanai attiecībā uz bērniem

VDAR ir paredzēts, ka bērniem pienākas īpaša aizsardzība informācijas sabiedrības pakalpojumu kontekstā, jo "viņi var pietiekami neapzināties attiecīgos riskus, sekas un aizsardzības pasākumus, un savas tiesības saistībā ar personas datu apstrādi"[369]. Tādēļ saskaņā ar **ES tiesību aktiem**, ja informācijas sabiedrības pakalpojumu sniedzēji, pamatojoties uz piekrišanu, apstrādā datus par bērniem, kuri jaunāki par 16 gadiem, šāda apstrāde būs likumīga "tikai tad un tādā apmērā, ja piekrišanu ir devusi vai apstiprinājusi persona, kurai ir vecāku atbildība par bērnu"[370]. Dalībvalstis savos tiesību aktos var noteikt jaunāku vecumu, kaut arī ne jaunāku par 13 gadiem[371]. Tādas personas piekrišana, kurai ir vecāku atbildība par bērnu, nav nepieciešama "saistībā ar preventīviem vai konsultāciju pakalpojumiem, ko tiešā veidā piedāvā bērnam"[372]. Informācijai un komunikācijai, ja apstrāde attiecas uz bērnu, vajadzētu būt skaidrā un vienkāršā valodā, kas bērnam ir viegli saprotama[373].

Tiesības atsaukt piekrišanu jebkurā laikā

VDAR ietvertas vispārējas tiesības jebkurā laikā atsaukt piekrišanu[374]. Datu subjekts jāinformē par šādām tiesībām pirms piekrišanas sniegšanas, un viņš vai viņa šīs tiesības var īstenot pēc saviem ieskatiem. Nevajadzētu būt prasībai norādīt atteikuma iemeslus, kā arī negatīvu seku riskam, noņemot jebkādas priekšrocības, kas varētu būt saistītas ar iepriekš saskaņotu datu izmantošanu. Piekrišanas atsaukšanai vajadzētu būt tikpat vienkāršai kā tās sniegšanai[375]. Tā nav uzskatāma par labprātīgu piekrišanu, ja datu subjekts nevar atsaukt savu piekrišanu, neciešot zaudējumus, vai ja atsaukšana nav tikpat vienkārša kā tās sniegšana[376].

369 Turpat, 38. apsvērums.

370 Turpat. 8. panta 1. punkta pirmais ievilkums. Informācijas sabiedrības pakalpojumu jēdziens ir definēts Vispārīgās datu aizsardzības regulas 4. panta 25. punktā.

371 Vispārīgā datu aizsardzības regula, 8. panta 1. punkta otrais ievilkums.

372 Turpat, 38. apsvērums.

373 Turpat, 58. apsvērums. Skatīt arī modernizēto Konvenciju Nr. 108, 15. panta 2. punkta e) apakšpunkts. Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 68. un 125. pants.

374 Vispārīgā datu aizsardzības regula, 7. panta 3. punkts. Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 45. punkts

375 Vispārīgā datu aizsardzības regula, 7. panta 3. punkts.

376 Vispārīgā datu aizsardzības regula, 42. apsvērums; modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 42. punkts.

Piemērs. Klients piekrīt reklāmas pasta saņemšanai uz adresi, kuru norādījis datu pārzinim. Ja klients atsauc piekrišanu, pārzinim nekavējoties jāpārtrauc reklāmas pasta sūtīšana. Nedrīkstētu piemērot tādas soda sankcijas kā maksa. Tomēr piekrišanas atsaukšana ir piemērojama nākotnē, un tai nav atpakaļejoša spēka. Periods, kurā klienta personas dati tika likumīgi apstrādāti, pamatojoties uz klienta piekrišanu, ir bijis likumīgs. Atsaukšana novērš turpmāku šo datu apstrādi, izņemot gadījumus, kad šāda apstrāde ir saskaņā ar tiesībām uz dzēšanu[377].

Nepieciešamība līguma izpildei

ES tiesību aktos VDAR 6. panta 1. punkta b) apakšpunktā sniegts vēl viens likumīgas apstrādes pamats, proti, ja apstrāde ir "vajadzīga līguma, kura līgumslēdzēja puse ir datu subjekts, izpildei". Šis noteikums attiecas arī uz pirmslīguma attiecībām. Piemēram, gadījumos, kad puse plāno noslēgt līgumu, bet vēl to nav izdarījusi, iespējams, tāpēc, ka vēl veicamas dažas pārbaudes. Ja kādai no pusēm šim nolūkam ir jāapstrādā dati, šāda apstrāde ir likumīga, ja vien tā ir "nepieciešama, lai pirms līguma noslēgšanas īstenotu pasākumus pēc datu subjekta pieprasījuma"[378].

Jēdziens par datu apstrādi kā "likumā noteikto likumīgo pamatu" modernizētās Konvencijas Nr. 108 5. panta 2. punktā ietver arī "datu apstrādi līguma, kurā ir iesaistīts datu subjekts (vai pirmslīguma pasākumu pēc datu subjekta pieprasījuma), izpildei"[379].

Pārziņa juridiskie pienākumi

ES tiesību aktos noteikts vēl viens pamats datu apstrādes likumīgumam, proti, ja "apstrāde ir vajadzīga, lai izpildītu uz pārzini attiecināmu juridisku pienākumu" (VDAR 6. panta 1. punkta c) apakšpunkts). Šis noteikums attiecas uz pārziņiem, kas darbojas gan privātajā, gan publiskajā sektorā. Uz publiskā sektora datu pārziņu juridiskiem pienākumiem var attiekties arī VDAR 6. panta 1. punkta e) apakšpunkts. Ir daudz piemēru situācijām, kad likums privātā sektora pārziņiem uzliek pienākumu apstrādāt datus par konkrētiem datu subjektiem. Piemēram, darba devējiem ir

377 Vispārīgā datu aizsardzības regula, 17. panta 1. punkta b) apakšpunkts.

378 Turpat, 6. panta 1. punkta b) apakšpunkts.

379 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 46. punkts, Eiropas Padome, Ministru komiteja (2010), Ministru komitejas Ieteikums CM/Rec(2010)13 dalībvalstīm par fizisko personu aizsardzību attiecībā uz personas datu automātisku apstrādi datu profilu veidošanas kontekstā (Ieteikums par profilēšanu), 2010. gada 23. novembris, 3.4. punkta b) apakšpunkts.

jāapstrādā dati par saviem darbiniekiem sociālā nodrošinājuma un nodokļu vajadzībām, un uzņēmumiem jāapstrādā dati par saviem klientiem nodokļu vajadzībām.

Juridiskais pienākums var izrietēt no Savienības vai dalībvalsts tiesību aktiem, kas varētu būt vienas vai vairāku apstrādes darbību pamatā. Likumā ir jānosaka apstrādes nolūks, norādes, kā noteikt pārzini, apstrādājamo personas datu veidu, attiecīgos datu subjektus, struktūras, kurām dati var tikt izpausti, apstrādes nolūka ierobežojumus, glabāšanas termiņu un citus pasākumus, lai nodrošinātu likumīgu un godprātīgu apstrādi[380]. Jebkuram šādam likumam, kas ir personas datu apstrādes pamatā, ir jāatbilst gan Hartas 7. un 8. pantam, gan ECTK 8. pantam.

Pārziņa juridiskais pienākums ir arī likumīgs datu apstrādes pamats **saskaņā ar EP tiesību aktiem**[381]. Kā jau tika norādīts iepriekš, privātā sektora pārziņa juridiskais pienākums ir tikai viens konkrēts citu leģitīmo interešu gadījums, kā minēts ECTK 8. panta 2. punktā. Tāpēc piemērs par darba devējiem, kuri apstrādā datus par saviem darbiniekiem, ir būtisks arī EP tiesībās.

Datu subjekta vai citas fiziskas personas vitālās intereses

Saskaņā ar ES tiesību aktiem VDAR 6. panta 1. punkta d) apakšpunktā paredzēts, ka personas datu apstrāde ir likumīga, ja tā ir "vajadzīga, lai aizsargātu datu subjekta vai citas fiziskas personas vitālas intereses". Uz šo likumīgo pamatu var atsaukties tikai tad, ja personas datus apstrādā, pamatojoties uz citas fiziskas personas vitālām interesēm, ja šādu apstrādi "nevar acīmredzami balstīt uz citu juridisko pamatu"[382]. Dažreiz apstrādes veidu var pamatot gan ar sabiedrības interesēm, gan ar datu subjekta vai citas personas vitālajām interesēm. Tas attiecas, piemēram, uz epidēmiju pārraudzību un to attīstību vai gadījumiem, kad pastāv ārkārtas humanitārā situācija.

Saskaņā ar EP tiesību aktiem ECTK 8. pantā datu subjekta vitālās intereses nav minētas. Tomēr tiek uzskatīts, ka datu subjekta vitālās intereses ir ietvertas modernizētās Konvencijas Nr. 108 5. panta 2. punkta "likumīgā pamata" jēdzienā, kas attiecas uz personas datu apstrādes likumību[383].

380 Vispārīgā datu aizsardzības regula, 45. apsvērums.

381 Eiropas Padomes Ministru komiteja (2010), Ministru komitejas Ieteikums CM/Rec(2010)13 dalībvalstīm par fizisko personu aizsardzību attiecībā uz personas datu automātisku apstrādi datu profilu veidošanas kontekstā (Ieteikums par profilēšanu), 2010. gada 23. novembris, 3.4. punkta a) apakšpunkts.

382 Vispārīgā datu aizsardzības regula, 46. apsvērums.

383 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 46. punkts.

Sabiedrības intereses un oficiālo pilnvaru īstenošana

Ņemot vērā daudzos iespējamos sabiedrisko jautājumu organizēšanas veidus, VDAR 6. panta 1. punkta e) apakšpunktā paredzēts, ka personas datus var likumīgi apstrādāt, ja apstrāde "ir vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras (..)"[384].

Piemērs. Lietā *Huber pret Vācijas Federatīvo Republiku*[385] *Huber* kungs, Austrijas valstspiederīgais, kurš dzīvo Vācijā, lūdza Federālo migrācijas un bēgļu pārvaldi dzēst Ārvalstnieku centrālajā reģistrā (*AZR*) par viņu iekļautos datus. Šo reģistru, kurā ir personas dati par ES pilsoņiem, kuri nav Vācijas pilsoņi un kuri Vācijā uzturas ilgāk nekā trīs mēnešus, izmanto statistikas nolūkos, kā arī tiesībaizsardzības un tiesu iestādes, izmeklējot noziedzīgas darbības vai darbības, kas apdraud sabiedrības drošību, un saucot pie atbildības par tām. Iesniedzējtiesa jautāja, vai personas datu apstrāde, kas tiek veikta tādā reģistrā kā Ārvalstnieku centrālais reģistrs, kuram var piekļūt arī citas publiskas iestādes, ir savietojama ar ES tiesībām, ņemot vērā, ka attiecībā uz Vācijas valstspiederīgajiem šāda reģistra nav.

EST nosprieda, ka atbilstoši Direktīvas 95/46/EK 7. panta e) punktam[386] personas datus var likumīgi apstrādāt, ja tas ir nepieciešams, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot oficiālās pilnvaras.

EST uzskatīja, ka "ņemot vērā mērķi visās dalībvalstīs nodrošināt vienādu aizsardzības līmeni, vajadzības jēdzienam, kas izriet no Direktīvas 95/46/EK 7. panta e) punkta[387] (..), nevar būt atšķirīgs saturs atkarībā no dalībvalsts. Tādējādi tas ir autonoms Kopienas tiesību jēdziens, kas ir jāinterpretē tā, lai tas pilnībā atbilstu šīs direktīvas mērķim, kas ir noteikts tās 1. panta 1. punktā"[388].

384 Skatīt Vispārīgo datu aizsardzības regulas 45. apsvērumu.

385 EST 2008. gada 16. decembra spriedums lietā C-524/06 *Heinz Huber pret Vācijas Federatīvo Republiku* [GC].

386 Iepriekšējā Datu aizsardzības direktīva, 7. panta e) punkts, tagad Vispārīgā datu aizsardzības regula, 6. panta 1. punkta e) apakšpunkts.

387 Turpat.

388 EST 2008. gada 16. decembra spriedums lietā C-524/06 *Heinz Huber pret Vācijas Federatīvo Republiku* [GC], 52. punkts.

EST atzīmēja, ka Savienības pilsoņa brīvas pārvietošanās tiesības dalībvalsts teritorijā, kuras pilsonis viņš nav, nav beznosacījumu un uz tām var attiekties ierobežojumi un nosacījumi, kas noteikti Eiropas Kopienas dibināšanas līgumā un pasākumos, kas pieņemti, lai tos īstenotu. Tādējādi, ja principā dalībvalstij ir likumīgas tiesības izmantot tādu reģistru kā *AZR*, atbalstot iestādes, kuras ir atbildīgas par tiesību aktu piemērošanu attiecībā uz uzturēšanās tiesībām, šādā reģistrā nedrīkst būt nekāda cita informācija kā tā, kas ir nepieciešama šim konkrētajam mērķim. EST secināja, ka šāda personas datu apstrādes sistēma atbilst ES tiesību aktiem, ja tajā ir tikai dati, kas nepieciešami šo tiesību aktu piemērošanai, un ja apstrādes centralizētais raksturs padara šo tiesību aktu piemērošanu efektīvāku. Valsts tiesai jāpārliecinās, vai konkrētajā gadījumā šie nosacījumi ir izpildīti. Pretējā gadījumā personas datu glabāšanu un apstrādi tādā reģistrā kā *AZR* statistikas nolūkos nekādā gadījumā nevar uzskatīt par nepieciešamu Direktīvas 95/46/EK 7. panta e) punkta[389] izpratnē[390].

Visbeidzot, attiecībā uz jautājumu par reģistrā esošo datu izmantošanu noziedzības apkarošanai, EST nosprieda, ka šis mērķis "obligāti nozīmē, ka ir jāizmeklē izdarītie noziegumi un kriminālpārkāpumi neatkarīgi no to izdarītāju pilsonības". Lietā aplūkotajā reģistrā nav personas datu, kas attiecas uz attiecīgās dalībvalsts pilsoņiem, un šī atšķirīgā attieksme ir diskriminācija, ko aizliedz LESD 18. pants. Rezultātā EST secināja, ka šis noteikums "liedz dalībvalstij, lai cīnītos pret noziedzību, izveidot personas datu apstrādes sistēmu, kas attiecas tikai uz tiem Savienības pilsoņiem, kas nav šīs dalībvalsts valstspiederīgie"[391].

Uz personas datu izmantošanu iestādēs, kas darbojas sabiedriskajā jomā, attiecas arī **ECTK** 8. pants, attiecīgos gadījumos tai ir paredzēts piemērot modernizētās Konvencijas Nr. 108 5. panta 2. punktu[392].

389 Iepriekšējā Datu aizsardzības direktīva, 7. panta e) punkts, tagad Vispārīgā datu aizsardzības regula, 6. panta 1. punkta e) apakšpunkts.

390 EST 2008. gada 16. decembra spriedums lietā C-524/06 *Heinz Huber pret Vācijas Federatīvo Republiku* [GC], 54., 58.–59. un 66.–68. punkts.

391 Turpat, 78. un 81. punkts.

392 Modernizētās konvencijas Nr. 108 skaidrojošais ziņojums, 46. un 47. pants.

Pārziņa vai trešās personas leģitīmas intereses

ES tiesībās datu subjekts nav vienīgā persona, kurai ir leģitīmas intereses. VDAR 6. panta 1. punkta f) apakšpunktā paredzēts, ka personas datus var likumīgi apstrādāt, ja tas ir nepieciešams "pārziņa vai trešās personas [izņemot publiskas iestādes, pildot savus uzdevumus] leģitīmo interešu ievērošanai, izņemot, ja datu subjekta intereses vai pamattiesības un pamatbrīvības, kurām nepieciešama personas datu aizsardzība, ir svarīgākas par šādām interesēm (..)"[393].

Leģitīmo interešu esamība katrā konkrētajā gadījumā ir rūpīgi jāizvērtē[394]. Ja tiek identificētas pārziņa leģitīmās intereses, ir jāveic līdzsvarošanas uzdevums starp šīm interesēm un datu subjekta interesēm vai pamattiesībām un brīvībām[395]. Veicot šādu novērtējumu, jāņem vērā datu subjekta pamatotās cerības, nosakot, vai pārziņa intereses ir svarīgākas par datu subjekta interesēm vai pamattiesībām[396]. Ja datu subjekta tiesības ir svarīgākas par pārziņa leģitīmām interesēm, pārzinis var spert soļus un ieviest aizsardzības pasākumus, lai nodrošinātu ietekmes uz datu subjekta tiesībām minimizēšanu (piemēram, pseidonimizēt datus), un apvērst "līdzsvaru", pirms pilntiesīgi atsaukties uz šo apstrādes likumīgo pamatu. Atzinumā par datu pārziņa leģitīmo interešu jēdzienu 29. panta darba grupa uzsvēra pārskatatbildības un pārredzamības, kā arī datu subjekta tiesību celt iebildumus pret viņa datu apstrādi un tiesību piekļūt, mainīt, dzēst vai nosūtīt būtisko nozīmi, līdzsvarojot pārziņa likumīgās intereses un datu subjekta pamattiesības[397].

VDAR apsvērumos ir sniegti daži piemēri, kas ir attiecīgā datu pārziņa leģitīmās intereses. Piemēram, personas datu apstrāde ir atļauta bez datu subjekta piekrišanas, ja tā tiek veikta tiešās tirgvedības nolūkos vai "tādā apjomā, kas vajadzīgs, lai novērstu krāpšanu"[398].

Savā judikatūrā EST ir padziļināti aplūkojusi pārbaudi, ar ko nosaka, kas ir leģitīmas intereses.

393 Salīdzinājumā ar Direktīvu 95/46/EK Vispārīgā datu aizsardzības regula sniedz vairāk to gadījumu piemērus, kurus uzskata par leģitīmām interesēm.

394 Vispārīgā datu aizsardzības regula, preambula, 47. apsvērums.

395 29. panta darba grupa (2014), *Atzinums 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu*, 2014. gada 4. aprīlis.

396 Turpat.

397 Turpat.

398 Vispārīgā datu aizsardzības regula, preambula, 47. apsvērums.

Piemērs. Lieta *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*[399] attiecās uz kaitējumu, ko pasažieris, pēkšņi atverot durvis, nodarīja Rīgas satiksmes trolejbusam. Rīgas satiksme vēlējās zaudējumus no pasažiera piedzīt tiesas ceļā. Tomēr policija sniedza tikai pasažiera vārdu un atteicās norādīt pasažiera personas kodu un adresi, apgalvojot, ka šādas informācijas izpaušana būtu prettiesiska saskaņā ar valsts tiesību aktiem datu aizsardzības jomā.

Latvijas iesniedzējtiesa lūdza EST sniegt prejudiciālu nolēmumu par to, vai ES datu aizsardzības tiesību akti uzliek pienākumu izpaust visus personas datus, kas nepieciešami, lai sāktu civilprocesu pret personu, kura, iespējams, saucama pie atbildības par administratīvo pārkāpumu[400].

EST skaidroja, ka ES tiesību aktos datu aizsardzības jomā ir paredzēta iespēja, nevis pienākums, izpaust datus trešai personai šīs puses leģitīmo interešu īstenošanai[401]. EST noteica trīs kumulatīvus nosacījumus, kas jāizpilda, lai personas datu apstrāde būtu likumīga, pamatojoties uz "leģitīmajām interesēm"[402]. Pirmkārt, trešai personai, kurai dati tiek izpausti, ir jāīsteno tās leģitīmās intereses. Šajā konkrētajā gadījumā tas nozīmē, ka personiskas informācijas pieprasīšana, lai iesūdzētu personu par mantas bojāšanu, ir trešās personas leģitīmās intereses. Otrkārt, personas datu apstrādei jābūt nepieciešamai leģitīmo interešu mērķiem. Šajā gadījumā personas identificēšanai ir obligāti nepieciešama personiskā informācija, piemēram, adrese un/vai personas kods. Treškārt, datu subjekta pamattiesības un brīvības nedrīkst būt svarīgākas par pārziņa vai trešo personu leģitīmajām interesēm. Interešu līdzsvarošana jāveic katrā atsevišķā gadījumā, ņemot vērā tādus elementus kā datu subjekta tiesību pārkāpuma smagums vai pat datu subjekta vecums noteiktos apstākļos. Tomēr šajā konkrētajā lietā EST neuzskatīja, ka informācijas neizpaušana ir pamatota tikai tāpēc, ka datu subjekts ir nepilngadīgs.

399 EST 2017. gada 4. maija spriedums lietā C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde pret Rīgas pašvaldības SIA "Rīgas satiksme"*.

400 Turpat, 23. punkts.

401 Turpat, 26. punkts.

402 Turpat, 28.–34. punkts.

Spriedumā lietā *ASNEF un FECEMD* EST nepārprotami lēma par datu apstrādi, pamatojoties uz "leģitīmo interešu" likumīgo pamatu, kas tobrīd bija nostiprināts Datu aizsardzības direktīvas 7. panta f) punktā[403].

Piemērs. Spriedumā lietā *ASNEF un FECEMD*[404] EST paskaidroja, ka valsts tiesību aktos nav atļauts pievienot papildu likumīgas datu apstrādes nosacījumus tiem, kas minēti direktīvas 7. panta f) apakšpunktā[405]. Tiesa atsaucās uz situāciju, kad Spānijas datu aizsardzības tiesību aktos bija noteikums, saskaņā ar kuru citas privātas personas varēja, atsaucoties uz leģitīmajām interesēm, apstrādāt personas datus tikai tad, ja informācija jau bija parādījusies publiski pieejamos avotos.

EST vispirms atzīmēja, ka Direktīvas 95/46/EK[406] mērķis ir nodrošināt, ka indivīdu tiesību un brīvību aizsardzības līmenis attiecībā uz personas datu apstrādi ir vienāds visās dalībvalstīs. Šajā jomā piemērojamo valsts tiesību aktu tuvināšana nedrīkst arī samazināt to sniegto aizsardzību. Tā vietā ir jācenšas nodrošināt augstu aizsardzības līmeni ES teritorijā[407]. Tā rezultātā EST nosprieda, ka "no mērķa nodrošināt vienādu aizsardzības līmeni visās dalībvalstīs izriet, ka Direktīvas 95/46/EK 7. pants[408] paredz plašu un pilnīgu tādu situāciju sarakstu, kurās var uzskatīt, ka ir notikusi likumīga personas datu apstrāde". Turklāt "dalībvalstis nedrīkst ne pievienot Direktīvas 95/46/EK[409] 7. pantam jaunus kritērijus, kas attiektos uz likumīgu personas datu apstrādi, ne arī paredzēt papildu prasības, kas mainītu kāda no šajā pantā ietverto sešu kritēriju piemērošanu"[410]. EST atzina, ka attiecībā uz līdzsvarošanu, kas

403 Iepriekšējā Datu aizsardzības direktīva, 7. panta f) punkts, tagad Vispārīgā datu aizsardzības regula, 6. panta 1. punkta f) apakšpunkts.

404 EST 2011. gada 24. novembra spriedums apvienotajās lietas C-468/10 un C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) un Federación de Comercio Electrónico y Marketing Directo (FECEMD) pret Administración del Estado*.

405 Iepriekšējā Datu aizsardzības direktīva, 7. panta f) punkts, tagad Vispārīgā datu aizsardzības regula, 6. panta 1. punkta f) apakšpunkts.

406 Iepriekšējā Datu aizsardzības direktīva, tagad Vispārīgā datu aizsardzības regula.

407 EST 2011. gada 24. novembra spriedums apvienotajās lietās C-468/10 un C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) un Federación de Comercio Electrónico y Marketing Directo (FECEMD) pret Administración del Estado*, 28. punkts. Skatīt Datu aizsardzības direktīvas 8. un 10. apsvērumu.

408 Iepriekšējā Datu aizsardzības direktīva, 7. pants, tagad Vispārīgā datu aizsardzības regula, 6. panta 1. punkta f) apakšpunkts.

409 Iepriekšējā Datu aizsardzības direktīva, 7. pants, tagad Vispārīgā datu aizsardzības regula, 6. pants.

410 Turpat.

veicama saskaņā ar Direktīvas 95/46/EK 7. panta f) punktu, ir iespējams ņemt vērā, ka datu apstrādes subjekta pamattiesību pārkāpuma smagums, kas izriet no apstrādes, var mainīties atkarībā no tā, vai attiecīgie dati jau parādās publiski pieejamos avotos.

Tomēr direktīvas 7. panta f) punktam "ir pretrunā tas, ka dalībvalsts kategoriski un vispārīgi izslēdz iespēju, ka atsevišķu kategoriju personas dati var tikt apstrādāti, neļaujot konkrētajā gadījumā izvērtēt attiecīgās pretstatītās tiesības un intereses".

Ņemot vērā šos apsvērumus, EST secināja, ka Direktīvas 95/46/EK[411] 7. panta f) punkts ir jāinterpretē "tādējādi, ka tam ir pretrunā tāds valsts tiesiskais regulējums, ar kuru gadījumā, ja nav attiecīgās personas piekrišanas, un lai atļautu šo personas datu apstrādi, kura ir vajadzīga personas datu apstrādātāja vai trešo personu, kurām dati tiek atklāti, likumīgo interešu ievērošanai, papildus attiecīgās personas pamattiesību un pamatbrīvību ievērošanai tiek pieprasīts, lai šie dati atrastos publiski pieejamos avotos, tādējādi kategoriski un vispārīgi izslēdzot tādu datu apstrādes iespējamību, kuri neatrodas publiski pieejamos avotos"[412].

Kad personas dati tiek apstrādāti, pamatojoties uz "leģitīmajām interesēm", indivīdam ir tiesības jebkurā laikā iebilst pret apstrādi, pamatojoties uz viņa/viņas īpašo situāciju, atbilstoši VDAR 21. panta 1. punktam. Pārzinim ir jāpārtrauc apstrāde, izņemot gadījumus, kad tas uzrāda pārliecinošu likumīgu pamatu apstrādi turpināt.

Attiecībā uz **EP tiesībām** līdzīgi formulējumi ir atrodami modernizētajā Konvencijā Nr. 108[413] un EP ieteikumos. Ieteikumā par profilēšanu ir atzīts, ka personas datu apstrāde profilēšanas nolūkos ir likumīga, ja tā nepieciešama citu personu leģitīmo interešu īstenošanai, "izņemot gadījumus, kad datu subjektu pamattiesības un brīvības ir svarīgākas par tām"[414]. Turklāt "citu personu tiesību un brīvību aizsardzība"

411 Iepriekšējā Datu aizsardzības direktīva, 7. panta f) punkts, tagad Vispārīgā datu aizsardzības regula, 6. panta 1. punkta f) apakšpunkts.

412 EST 2011. gada 24. novembra spriedums apvienotajās lietās C-468/10 un C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) un Federación de Comercio Electrónico y Marketing Directo (FECEMD) pret Administración del Estado*, 40., 44. un 48.–49. punkts.

413 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 46. punkts

414 Eiropas Padomes Ministru komiteja (2010), Ieteikums CM/Rec(2010)13 dalībvalstīm par fizisko personu aizsardzību attiecībā uz personas datu automātisku apstrādi datu profilu veidošanas kontekstā, 2010. gada 23. novembris, 3.4. punkta b) apakšpunkts (Ieteikums par profilēšanu).

ir minēta ECTK 8. panta 2. punktā kā viens no likumīgajiem pamatiem, ierobežojot tiesības uz datu aizsardzību.

Piemērs. Lietā *Y pret Turciju*[415] prasītājs bija *HIV* pozitīvs. Ierodoties slimnīcā, prasītājs bija bezsamaņā, tāpēc ātrās palīdzības brigāde informēja slimnīcas personālu, ka viņš ir *HIV* pozitīvs. Prasītājs ECT apgalvoja, ka šīs informācijas izpaušana ir pārkāpusi viņa tiesības uz privātās dzīves neaizskaramību. Tomēr, ņemot vērā nepieciešamību aizsargāt slimnīcas personāla drošību, informācijas apmaiņa netika uzskatīta par viņa tiesību pārkāpumu.

4.1.2. Īpašu kategoriju datu (sensitīvu datu) apstrāde

Saskaņā ar **EP tiesību aktiem** valsts tiesību aktos ir jānosaka attiecīga aizsardzība sensitīvu datu izmantošanai, ja tiek izpildīti modernizētās Konvencijas Nr. 108 6. panta nosacījumi, proti, ja likumā ir ietverti piemēroti aizsardzības pasākumi, kas papildina pārējos konvencijas noteikumus. **ES tiesību aktos** VDAR 9. pantā paredzēts detalizēts režīms īpašu kategoriju datu (arī sauktu par "sensitīviem datiem") apstrādei. Šie dati atklāj rasu vai etnisko izcelsmi, politiskos uzskatus, reliģisko vai filozofisko pārliecību un dalību arodbiedrībās, kā arī ģenētiskos un biometriskos datus apstrādei, lai unikāli identificētu fizisku personu un iegūtu datus par veselību, personas dzimumdzīvi vai seksuālo orientāciju. Sensitīvu datu apstrāde principā ir aizliegta[416].

Taču pastāv izsmeļošs šā aizlieguma atbrīvojumu saraksts, kas atrodams regulas 9. panta 2. punktā un kas ir likumīgs pamats sensitīvu datu apstrādei. Šie atbrīvojumi ietver situācijas, kad:

- datu subjekts nepārprotami piekrīt datu apstrādei;
- apstrādi veic bezpeļņas organizācija politiskiem, filozofiskiem, reliģiskiem vai arodbiedrību nolūkiem tās likumīgās darbības ietvaros, un apstrāde attiecas tikai uz tās (bijušajiem) biedriem vai personām, ar kurām šādiem nolūkiem tiek uzturēti regulāri kontakti;

415 ECT 2015. gada 17. februāra spriedums lietā *Y pret Turciju*, Nr. 648/10.

416 Iepriekšējā Datu aizsardzības direktīva, 7. panta f) punkts, tagad Vispārīgā datu aizsardzības regula, 9. panta 1. punkts.

- apstrāde attiecas uz datiem, ko datu subjekts ir nepārprotami publiskojis;
- apstrāde ir nepieciešama, lai:
  - izpildītu pārziņa vai datu subjekta pienākumus un īstenotu konkrētas tiesības nodarbinātības, sociālā nodrošinājuma un sociālās aizsardzības kontekstā;
  - aizsargātu datu subjekta vai citas fiziskas personas vitālās intereses (ja datu subjekts nevar sniegt piekrišanu);
  - izveidotu, realizētu vai aizstāvētu likumīgas prasības, kā arī gadījumos, kad tiesas īsteno tiesu varu;
  - profilaktiskos vai arodmedicīnas nolūkos: "darbinieka darbspējas novērtēšanai, medicīniskas diagnozes, veselības vai sociālās aprūpes, ārstēšanas vai veselības, vai sociālās aprūpes sistēmu un pakalpojumu pārvaldības nodrošināšanas nolūkos, pamatojoties uz Savienības vai dalībvalsts tiesību aktiem vai saskaņā ar līgumu ar veselības darba profesionāli";
  - arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, kā arī statistikas nolūkos.
  - sabiedrības interesēs sabiedrības veselības jomā; vai
  - būtisku sabiedrības interešu dēļ.

Lai apstrādātu īpašu kategoriju datus, līgumattiecības ar datu subjektu līdz ar to netiek uzskatītas par sensitīvu datu likumīgas apstrādes juridisko pamatu, izņemot līgumu ar veselības aprūpes speciālistu, uz kuru attiecas dienesta noslēpuma glabāšanas pienākums[417].

Datu subjekta nepārprotama piekrišana

Saskaņā ar **ES tiesību aktiem** pirmais iespējamais pamats jebkādu datu likumīgai apstrādei neatkarīgi no tā, vai tie ir sensitīvi dati, ir datu subjekta piekrišana. Sensitīvu datu gadījumā šādai piekrišanai jābūt nepārprotamai. Savienības vai dalībvalsts tiesību aktos tomēr var paredzēt, ka indivīds nedrīkst atcelt īpašo kategoriju datu

417 Vispārīgā datu aizsardzības regula, 9. panta 2. punkta h) un i) apakšpunkts.

apstrādes aizliegumu[418]. Tas varētu būt, piemēram, ja apstrādes rezultātā datu subjektam rodas neparasti riski.

Nodarbinātības tiesības vai sociālā nodrošinājuma un sociālās aizsardzības tiesības

Saskaņā ar **ES tiesību aktiem** 9. panta 1. punkta aizliegumu var atcelt, ja apstrāde ir nepieciešama pārziņa vai datu subjekta pienākumu vai tiesību izpildei nodarbinātības vai sociālā nodrošinājuma jomā. Tomēr apstrādei jābūt atļautai saskaņā ar ES tiesību aktiem, valsts tiesību aktiem vai koplīgumu atbilstoši valsts tiesību aktiem, kas nodrošina attiecīgas garantijas datu subjekta pamattiesībām un interesēm[419]. Organizācijas nodarbinātības reģistros var iekļaut sensitīvus personas datus, ievērojot dažus nosacījumus, kas norādīti VDAR un attiecīgajos valsts tiesību aktos. Sensitīvu datu piemēri var būt dalība arodbiedrībās vai informācija par veselības stāvokli.

Datu subjekta vai citas personas vitālās intereses

Saskaņā ar **ES tiesību aktiem**, tāpat kā nesensitīvu datu gadījumā, sensitīvus datus var apstrādāt datu subjekta vai citas fiziskas personas vitālu interešu dēļ[420]. Ja apstrādes pamatā ir citas personas vitālās intereses, uz šo likumīgo pamatu var atsaukties tikai tad, ja šādu apstrādi "nevar acīmredzami balstīt uz citu juridisko pamatu"[421]. Dažos gadījumos personas datu apstrāde var aizsargāt gan individuālās, gan sabiedrības intereses, piemēram, ja apstrāde ir vajadzīga humanitāros nolūkos[422].

Lai sensitīvu datu apstrāde uz šāda pamata būtu likumīga, jābūt situācijai, kad nav iespējams lūgt datu subjekta piekrišanu, jo, piemēram, datu subjekts ir bezsamaņā vai nav klātesošs un ar viņu nav iespējams sazināties. Citiem vārdiem sakot, persona fiziski vai juridiski nav spējīga sniegt piekrišanu.

418 Turpat, 9. panta 2. punkta a) apakšpunkts.

419 Vispārīgā datu aizsardzības regula, 9. panta 2. punkta b) apakšpunkts.

420 Turpat, 9. panta 2. punkta c) apakšpunkts.

421 Turpat, 46. apsvērums.

422 Turpat.

Labdarības un bezpeļņas organizācijas

Personas datu apstrāde ir atļauta arī nodibinājumu, apvienību vai citu bezpeļņas organizāciju likumīgas darbības gaitā, ja tām ir politisks, filozofisks, reliģisks vai arodbiedrību mērķis. Tomēr apstrādei jāattiecas tikai uz organizācijas locekļiem vai bijušajiem locekļiem, vai personām, kas uztur regulāru kontaktu ar organizāciju[423]. Sensitīvus datus nedrīkst izpaust ārpus šīm organizācijām bez datu subjekta piekrišanas.

Dati, ko datu subjekts ir apzināti publiskojis

VDAR 9. panta 2. punkta e) apakšpunktā paredzēts, ka apstrāde nav aizliegta, ja tā attiecas uz datiem, kurus datu subjekts ir apzināti publiskojis. Pat ja jēdziens "datu subjekts apzināti publiskojis" nav definēts regulā, jo tas ir izņēmums sensitīvu datu apstrādes aizliegumam, tas ir jāinterpretē šauri un kā tāds, kas datu subjektam pieprasa apzināti publiskot savus personas datus. Tādējādi, ja televīzijā tiek pārraidīts ar videonovērošanas kameru uzņemts video, kurā cita starpā redzams, kā ugunsdzēsējs tiek ievainots, mēģinot evakuēt cilvēkus no ēkas, nevar uzskatīt, ka ugunsdzēsējs ir apzināti publiskojis datus. Bet ja ugunsdzēsējs nolemj aprakstīt notikušo un publicēt video un fotoattēlus publiskā interneta vietnē, viņš vai viņa ir veicis apzinātu, apstiprinošu rīcību, publiskojot personas datus. Ir svarīgi atzīmēt, ka datu publiskošana nenozīmē piekrišanu, bet gan vēl vienu atļauju veikt īpašu kategoriju datu apstrādi.

Fakts, ka datu subjekts bija publiskojis apstrādātos personas datus, neatbrīvo pārziņus no viņu pienākumiem saskaņā ar datu aizsardzības tiesību aktiem. Piemēram, nolūka ierobežojuma principu turpina piemērot personas datiem pat tad, ja šādi dati ir publiski pieejami[424].

Likumīgas prasības

Saskaņā ar VDAR[425] ir atļauta arī īpašu kategoriju datu apstrāde, kas "vajadzīgi, lai celtu, īstenotu vai aizstāvētu likumīgas prasības" vai nu tiesas procesā, vai administratīvā vai ārpustiesas procedūrā[426]. Šajā gadījumā apstrādei jābūt attiecināmai uz

423 Turpat, 9. panta 2. punkta d) apakšpunkts.

424 29. panta darba grupa (2013), *Atzinums 3/13 par nolūka ierobežojumu*, WP 203, Brisele, 2013. gada 2. aprīlis, 14. lpp.

425 Turpat, 9. panta 2. punkta f) apakšpunkts.

426 Vispārīgā datu aizsardzības regula, preambula, 52. apsvērums

konkrētu likumīgu prasību un attiecīgi tās īstenošanai vai aizstāvībai, un to var pieprasīt jebkura no strīdā iesaistītajām pusēm.

Pildot savus uzdevumus, tiesas var apstrādāt īpašas datu kategorijas juridiska strīda risināšanas kontekstā[427]. Šajā saistībā apstrādāto datu īpašo kategoriju piemēri varētu būt, piemēram, ģenētiski dati, nosakot paternitāti, vai veselības stāvoklis, ja daļa no pierādījumiem attiecas uz detalizētu informāciju par noziegumā cietušajam nodarīto kaitējumu.

Būtisku sabiedrības interešu dēļ

Atbilstoši VDAR 9. panta 2. punkta g) apakšpunktam dalībvalstis var noteikt papildu apstākļus, kādos var apstrādāt sensitīvus datus, ja:

- datu apstrāde tiek veikta būtisku sabiedrības interešu dēļ;
- to paredz ar Eiropas vai valstu tiesību aktiem;
- Eiropas vai valstu tiesību akti ir samērīgi, tajos ievērotas tiesības uz datu aizsardzību un nodrošināti atbilstoši un konkrēti pasākumi, lai aizsargātu datu subjekta tiesības un intereses[428].

Izcils piemērs ir elektroniskās veselības datņu sistēmas. Šādas sistēmas ļauj veselības datus, ko veselības aprūpes sniedzēji apkopo pacienta ārstēšanas gaitā, darīt pieejamus citiem šā pacienta veselības aprūpes sniedzējiem plašā, parasti valsts mērogā.

29. panta darba grupa secināja, ka šādu sistēmu izveidošana nevar notikt saskaņā ar spēkā esošajiem tiesību aktiem, kas reglamentē pacientu datu apstrādi[429]. Tomēr elektroniskās veselības datņu sistēmas var pastāvēt, ja to pamatā ir "būtiskas sabiedrības intereses"[430]. To izveidošanai būtu nepieciešams skaidrs juridiskais

427 Turpat.

428 Turpat, 9. panta 2. punkta g) apakšpunkts.

429 29. panta darba grupa (2007), *Darba dokuments par personas ar veselību saistīto datu apstrādi elektroniskajās pacienta veselības kartēs* (EVK), WP 131, Brisele, 2007. gada 15. februāris. Skatīt arī Vispārīgo datu aizsardzības regulu, 9. panta 3. punkts.

430 Vispārīgā datu aizsardzības regula, 9. panta 2. punkta g) apakšpunkts.

pamats, kurā būtu ietverti arī sistēmas drošas darbības nodrošināšanai nepieciešamie drošības pasākumi[431].

Citi sensitīvu datu likumīgas apstrādes pamati

VDAR paredzēts, ka sensitīvus datus var apstrādāt, ja tas nepieciešams šādos nolūkos[432]:

- profilaktiskās vai arodmedicīnas nolūkos, darbspējas novērtēšanai, medicīniskas diagnozes, veselības vai sociālās aprūpes vai ārstēšanas vai veselības vai sociālās aprūpes sistēmu un pakalpojumu pārvaldības nodrošināšanas nolūkos, pamatojoties uz ES vai dalībvalsts tiesību aktiem vai saskaņā ar līgumu ar veselības darba profesionāli;

- sabiedrības interešu dēļ sabiedrības veselības jomā, piemēram, aizsardzībai pret nopietniem pārrobežu draudiem veselībai vai augstu kvalitātes un drošības standartu nodrošināšanai veselības aprūpē, kā arī zālēm vai medicīniskām ierīcēm, pamatojoties uz ES vai dalībvalsts tiesību aktiem. Likumā jāparedz atbilstoši un konkrēti pasākumi datu subjekta tiesību aizsardzībai;

- arhivēšanas, zinātniskās vai vēstures pētniecības, kā arī statistikas nolūkos, pamatojoties uz Savienības vai dalībvalsts tiesību aktiem. Likumam jābūt samērīgam attiecībā uz sasniedzamo mērķi, tajā jāievēro tiesību uz datu aizsardzību būtība un jānodrošina attiecīgi un konkrēti pasākumi, lai aizsargātu datu subjekta tiesības un intereses.

Papildu nosacījumi valstu tiesību aktos

VDAR arī ļauj dalībvalstīm ieviest vai uzturēt papildu nosacījumus, tostarp ierobežojumus ģenētisko, biometrisko un ar veselību saistīto datu apstrādei[433].

431 29. panta darba grupa (2007), *Darba dokuments par personas ar veselību saistīto datu apstrādi elektroniskajās pacienta veselības kartēs* (EVK), WP 131, Brisele, 2007. gada 15. februāris.

432 Vispārīgā datu aizsardzības regula, 9. panta 2. punkta h) un j) apakšpunkts.

433 Turpat, 9. panta 2. punkta h) apakšpunkts un 9. panta 4. punkts.

4.2. Apstrādes drošības noteikumi

Svarīgākie aspekti

- Apstrādes drošības noteikumi uzliek pārzinim un apstrādātājam pienākumu ieviest attiecīgus tehniskos un organizatoriskos pasākumus, lai novērstu jebkādu neatļautu iejaukšanos datu apstrādes darbībās.
- Nepieciešamo datu drošības līmeni nosaka:
  - tirgū pieejamās drošības funkcijas attiecīgajam apstrādes veidam;
  - izmaksas;
  - datu apstrādes riski attiecībā uz datu subjektu pamattiesībām un brīvībām.
- Personas datu konfidencialitātes nodrošināšana ir daļa no vispārējā principa, kas atzīts Vispārīgajā datu aizsardzības regulā.

Saskaņā gan ar **ES, gan EP tiesību aktiem** pārziņiem noteikts vispārējs pienākums personas datu apstrādi veikt pārredzami un atbildīgi, un jo īpaši attiecībā uz datu aizsardzības pārkāpumiem, ja šādi pārkāpumi notiek. Personas datu aizsardzības pārkāpumu gadījumā pārzinim ir pienākums informēt uzraudzības iestādes, izņemot gadījumus, kad ir maz ticams, ka personas datu aizsardzības pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām. Arī datu subjekti ir jāinformē par personas datu aizsardzības pārkāpumu, ja tā rezultātā varētu tikt radīts liels risks fizisku personu tiesībām un brīvībām.

4.2.1. Datu drošības elementi

Atbilstoši attiecīgajām **ES tiesību aktu** normām:

> *"Ņemot vērā tehnikas līmeni, īstenošanas izmaksas un apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un smaguma pakāpes riskus attiecībā uz fizisku personu tiesībām un brīvībām, pārzinis un apstrādātājs īsteno atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam (..)"*[434].

Šie pasākumi cita starpā ir šādi:

434 Turpat, 32. panta 1. punkts.

- personas datu pseidonimizācija un šifrēšana[435];
- spēja nodrošināt apstrādes sistēmu un pakalpojumu nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību[436];
- spēja laicīgi atjaunot personas datu pieejamību un piekļuvi tiem gadījumā, ja ir noticis fizisks vai tehnisks negadījums[437];
- process regulārai tehnisko un organizatorisko pasākumu efektivitātes testēšanai, izvērtēšanai un novērtēšanai, lai nodrošinātu apstrādes drošību[438].

EP tiesību aktos ir līdzīga norma:

> *"Katra Puse nodrošina, ka pārzinis un attiecīgā gadījumā apstrādātājs īsteno atbilstošus drošības pasākumus attiecībā uz tādiem riskiem kā nejauša vai neatļauta piekļuve personas datiem, to iznīcināšana, pazaudēšana, izmantošana, modificēšana vai izpaušana"*[439].

Saskaņā ar **ES un EP tiesību aktiem** datu aizsardzības pārkāpums, kas var ietekmēt fizisku personu tiesības un brīvības, pārzinim uzliek pienākumu informēt uzraudzības iestādi par pārkāpumu (skatīt 4.2.3. iedaļu).

Bieži vien pastāv arī nozares, valsts un starptautiskie standarti, kas izstrādāti drošai datu apstrādei. Piemēram, Eiropas privātuma zīmogs (*EuroPriSe*) ir ES *eTEN* (Eiropas telekomunikāciju tīkli) projekts, kas pēta produktu, īpaši programmatūru, sertifikācijas iespējas, lai veicinātu atbilstību Eiropas tiesību aktiem datu aizsardzības jomā. Eiropas Savienības Tīklu un informācijas drošības aģentūra (*ENISA*) tika izveidota, lai uzlabotu ES, ES dalībvalstu un uzņēmēju spēju novērst tīkla un informācijas drošības problēmas, risināt tās un reaģēt uz šīm problēmām[440]. *ENISA* regulāri publicē pašreizējo drošības apdraudējumu analīzi un ieteikumus, kā tos novērst[441].

435 Turpat, 32. panta 1. punkta a) apakšpunkts.

436 Turpat, 32. panta 1. punkta b) apakšpunkts.

437 Turpat, 32. panta 1. punkta c) apakšpunkts.

438 Turpat, 32. panta 1. punkta d) apakšpunkts.

439 Modernizētā Konvencija Nr. 108, 7. panta 1. punkts.

440 Eiropas Parlamenta un Padomes 2013. gada 21. maija Regula (ES) Nr. 526/2013 par Eiropas Savienības Tīklu un informācijas drošības aģentūru (*ENISA*) un ar ko atceļ Regulu (EK) Nr. 460/2004, OV 2013 L 165.

441 Piemēram, *ENISA* (2016), Kiberdrošība un viedo automašīnu noturība. Laba prakse un ieteikumi; *ENISA* (2016), Mobilo maksājumu un digitālo maciņu drošums.

Datu drošību panāk ne tikai ar pareizā aprīkojuma, aparatūras un programmatūru uzstādīšanu. Tā prasa arī attiecīgus iekšējos organizatoriskos noteikumus. Iekšējie noteikumi ideālā gadījumā attiektos uz šādiem jautājumiem:

- regulāru informācijas sniegšanu visiem darbiniekiem par datu drošības noteikumiem un viņu pienākumiem saskaņā ar datu aizsardzības tiesību aktiem, jo īpaši attiecībā uz viņu konfidencialitātes ievērošanas pienākumiem;

- skaidru pienākumu sadalījumu un skaidru kompetenču izklāstu datu apstrādes jautājumos, jo īpaši attiecībā uz lēmumiem apstrādāt personas datus un pārsūtīt datus trešām personām vai datu subjektiem;

- personas datu izmantošanu tikai atbilstoši kompetentās personas norādījumiem vai atbilstoši vispārīgajiem noteikumiem;

- piekļuves pārziņa vai apstrādātāja atrašanās vietai, kā arī aparatūrai un programmatūrām aizsardzību, tostarp piekļuves atļaujas pārbaudes;

- atļaujas piešķiršanas nodrošināšanu kompetentajai personai piekļūt personas datiem un tai nepieciešamo pareizo dokumentāciju;

- automatizētiem protokoliem par elektronisku piekļuvi personas datiem un regulāru šādu protokolu pārbaudi, ko veic iekšējais uzraudzības birojs (tāpēc ir jāreģistrē visas datu apstrādes darbības);

- rūpīgu dokumentāciju citiem izpaušanas veidiem, izņemot automātisku piekļuvi datiem, lai pierādītu, ka nav notikusi nelikumīga datu pārsūtīšana.

Efektīvu drošības pasākumu svarīgs elements ir arī personāla apmācība un izglītošana par datu drošību. Jāievieš arī verifikācijas procedūras, lai nodrošinātu, ka attiecīgie pasākumi ne tikai pastāv uz papīra, bet arī tiek ieviesti un darbojas praksē (piemēram, iekšējas vai ārējas revīzijas).

Pārziņa vai apstrādātāja drošības līmeņa uzlabošanas pasākumos ietver tādus instrumentus kā personas datu aizsardzības speciālisti, darbinieku izglītošana drošības jomā, regulāras revīzijas, ielaušanās testi un kvalitātes zīmogi.

Piemērs. Lietā *I pret Somiju*[442] prasītāja nespēja pierādīt, ka slimnīcas, kurā viņa strādāja, darbinieki bija nelikumīgi piekļuvuši viņas medicīniskajai kartei. Tādēļ valsts tiesas noraidīja viņas prasību par tiesību uz datu aizsardzību pārkāpumu. ECT secināja, ka ir pārkāpts ECTK 8. pants, jo slimnīcas veselības dokumentu reģistra sistēma "bija tāda, ka nebija iespējams ar atpakaļejošu datumu precizēt pacienta medicīnisko karšu izmantošanu, jo tajā bija redzamas tikai piecas pēdējās ieskatīšanās, turklāt šī informācija tika dzēsta, tiklīdz dokuments bija atgriezts arhīvos". Tiesa par izšķirošu uzskatīja apstākli, ka slimnīcā esošā uzskaites sistēma acīmredzami neatbilda valsts tiesību aktos noteiktajām juridiskajām prasībām – fakts, kuru valsts tiesas pienācīgi neizvērtēja.

ES ir ieviesusi Direktīvu par tīklu un informācijas sistēmu drošību (*NIS* direktīva)[443], kas ir pirmais ES mēroga tiesību instruments kiberdrošības jomā. Direktīvas mērķis ir uzlabot kiberdrošību valstu līmenī, no vienas puses, un palielināt sadarbības līmeni ES iekšienē, no otras puses. Tas uzliek arī pienākumus būtisko pakalpojumu sniedzējiem (tostarp enerģētikas, veselības, banku, transporta, digitālās infrastruktūras u. tml. nozares dalībniekiem) un digitālo pakalpojumu sniedzējiem pārvaldīt riskus, nodrošināt sava tīkla un informācijas sistēmu drošību un ziņot par drošības incidentiem.

Perspektīva

Eiropas Komisija 2017. gada septembrī iesniedza priekšlikumu regulai ar mērķi reformēt *ENISA* pilnvaras, ņemot vērā aģentūras jaunās kompetences un pienākumus saskaņā ar *NIS* direktīvu. Ierosinātās regulas mērķis ir izstrādāt *ENISA* uzdevumus un stiprināt tās funkciju būt par "uzziņas punktu ES kiberdrošības ekosistēmā"[444]. Ierosinātajai regulai nevajadzētu ierobežot VDAR principus, un, precizējot nepieciešamos elementus, kas veido Eiropas kiberdrošības sertifikācijas shēmas, tai būtu arī jāstiprina personas datu drošība. Paralēli 2017. gada septembrī Eiropas Komisija ierosināja īstenošanas regulas priekšlikumu, precizējot elementus, kas digitālo pakalpojumu sniedzējiem jāņem vērā, lai nodrošinātu viņu tīklu un informācijas sistēmu drošību,

442 ECT 2008. gada 17. jūlija spriedums lietā *I. pret Somiju*, Nr. 20511/03.

443 Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā, OV 2016 L 194.

444 Priekšlikums Eiropas Parlamenta un Padomes regulai par *ENISA* – ES Kiberdrošības aģentūru – un Regulas (ES) 526/2013 atcelšanu un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju (Kiberdrošības akts), COM(2017)477, 2017. gada 13. septembris, 6. lpp.

kā prasīts *NIS* direktīvas 16. panta 8. punktā. Rokasgrāmatas izstrādes laikā joprojām norisinājās diskusijas par šiem diviem priekšlikumiem.

4.2.2. Konfidencialitāte

Saskaņā ar ES tiesību aktiem VDAR atzīst personas datu konfidencialitāti vispārīga principa ietvaros[445]. Publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzējiem ir jānodrošina konfidencialitāte. Viņiem ir pienākums arī nodrošināt savu pakalpojumu drošību[446].

Piemērs. Apdrošināšanas sabiedrības darbinieks saņem telefona zvanu savā darba vietā no personas, kura saka, ka ir klients, pieprasot informāciju par viņa apdrošināšanas līgumu.

Saskaņā ar pienākumu ievērot klientu datu konfidencialitāti darbiniekam pirms personas datu izpaušanas jāveic vismaz minimālie drošības pasākumi. To var izdarīt, piemēram, piedāvājot atzvanīt uz tālruņa numuru, kas reģistrēts klienta lietā.

Saskaņā ar 5. panta 1. punkta f) apakšpunktu dati jāapstrādā tādā veidā, lai tiktu nodrošināta atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot attiecīgus tehniskos vai organizatoriskos pasākumus ("integritāte un konfidencialitāte").

Saskaņā ar 32. pantu pārzinim un apstrādātājam jāievieš tehniski un organizatoriski pasākumi, lai nodrošinātu augstu drošības līmeni. Šādi pasākumi cita starpā ietver personas datu pseidonimizāciju un šifrēšanu, spēju nodrošināt pastāvīgu apstrādes konfidencialitāti, integritāti, pieejamību un noturību, pasākumu efektivitātes novērtēšanu un pārbaudi, kā arī spēju atjaunot apstrādi fiziska vai tehniska incidenta gadījumā. Turklāt apstiprināts rīcības kodekss vai apstiprināts sertifikācijas mehānisms var tikt izmantots kā elements, lai pierādītu atbilstību integritātes un konfidencialitātes principiem. Papildus atbilstoši VDAR 28. pantam līgumā, ar ko pārzinim rodas saistības pret apstrādātāju, ir jāietver, ka apstrādātājam jānodrošina, ka personas,

445 Vispārīgā datu aizsardzības regula, 5. panta 1. punkta f) apakšpunkts.

446 Direktīva par privāto dzīvi un elektronisko komunikāciju, 5. panta 1. punkts.

kuras ir pilnvarotas apstrādāt datus, ir apņēmušās ievērot konfidencialitāti vai tām ir noteikts attiecīgs likumisks pienākums ievērot konfidencialitāti.

Konfidencialitātes pienākums neattiecas uz situācijām, kad dati kļūst zināmi personai kā privātpersonai, nevis kā pārziņa vai apstrādātāja darbiniekam. Šajā gadījumā nepiemēro VDAR 32. un 28. pantu, jo regulas tvērums nekādā mērā neattiecas uz privātpersonu personas datu izmantošanu, ja šāda izmantošana ir tā dēvētā mājsaimniecības atbrīvojuma robežās[447]. Uz mājsaimniecībām attiecināmais atbrīvojums ir personas datu izmantošana, ko veic "fiziska persona tikai personiska vai mājsaimnieciska pasākuma gaitā"[448]. Kopš EST lēmuma lietā *Bodil Lindqvist*[449] šis atbrīvojums tomēr ir jāinterpretē šauri, īpaši attiecībā uz datu izpaušanu. Īpaši mājsaimniecības atbrīvojums nav attiecināms uz personas datu publicēšanu internetā neierobežotam saņēmēju skaitam vai uz datu apstrādi, kurai ir profesionāli vai komerciāli aspekti (plašāku informāciju par to skatīt 2.1.2., 2.2.2. un 2.3.1. iedaļā).

"Komunikācijas konfidencialitāte" ir vēl viens konfidencialitātes aspekts, uz kuru attiecas *lex specialis*. Īpašie noteikumi elektroniskās komunikācijas konfidencialitātes nodrošināšanai saskaņā ar E-privātuma direktīvu prasa dalībvalstīm aizliegt citām personām, izņemot lietotājus, vai bez lietotāju piekrišanas klausīties, noklausīties, glabāt vai citā veidā pārtvert vai uzraudzīt komunikāciju un saistītos metadatus[450]. Valsts likumos var atļaut izņēmumus no šā principa tikai valsts drošības, aizsardzības, noziegumu novēršanas vai atklāšanas vajadzībām un tikai tad, ja šādi pasākumi ir nepieciešami un samērīgi ar izvirzītajiem mērķiem[451]. Tie paši noteikumi attieksies arī uz nākotnes e-privātuma regulu, tomēr tiesību akta par E-privātumu darbības joma tiks paplašināta, attiecinot to uz publiski pieejamiem elektronisko komunikāciju pakalpojumiem, lai aptvertu arī komunikāciju, kas tiek veikta, izmantojot *over-the-top* pakalpojumus (piemēram, mobilās lietotnes).

EP tiesību aktos konfidencialitātes pienākums ir ietverts datu drošības jēdzienā modernizētās Konvencijas Nr. 108 7. panta 1. punktā, kas skar datu drošību.

Apstrādātājiem konfidencialitātes pienākums nozīmē to, ka viņi bez atļaujas nedrīkst izpaust datus trešām personām vai citiem saņēmējiem. Pārziņa vai apstrādātāja

447 Vispārīgā datu aizsardzības regula, 2. panta 2. punkta c) apakšpunkts.

448 Turpat.

449 EST 2003. gada 6. novembra spriedums lietā C-101/01 *Kriminālprocess pret Bodil Lindqvist*.

450 Direktīva par privāto dzīvi un elektronisko komunikāciju, 5. panta 1. punkts.

451 Turpat, 15. panta 1. punkts.

darbiniekiem konfidencialitātes pienākums pieprasa, lai viņi personas datus izmantotu tikai atbilstoši kompetento vadītāju norādījumiem.

Konfidencialitātes pienākums jāiekļauj visos līgumos starp pārziņiem un viņu apstrādātājiem. Turklāt pārziņiem un apstrādātājiem jāievieš īpaši pasākumi, lai darbiniekiem noteiktu juridisku konfidencialitātes pienākumu, ko parasti panāk, iekļaujot konfidencialitātes klauzulas darba līgumos.

Par profesionālā konfidencialitātes pienākuma pārkāpumu daudzās ES dalībvalstīs un Konvencijas Nr. 108. līgumslēdzējās valstīs ir paredzēta krimināltiesiskā atbildība.

4.2.3. Paziņojumi par personas datu aizsardzības pārkāpumiem

Personas datu aizsardzības pārkāpums attiecas uz drošības pārkāpumu, kura rezultātā iestājusies apstrādāto personas datu nejauša vai nelikumīga iznīcināšana, nozaudēšana, izmaiņas vai neatļauta izpaušana, vai piekļuve tiem[452]. Kaut arī jaunās tehnoloģijas, piemēram, šifrēšana, tagad sniedz vairāk iespēju nodrošināt apstrādes drošību, datu aizsardzības pārkāpumi joprojām ir plaši sastopama parādība. Datu aizsardzības pārkāpumu cēloņi var būt dažādi – no nejaušām kļūdām, ko izdara organizācijā strādājošās personas, līdz ārējiem draudiem, piemēram, hakeriem un kibernoziedzības organizācijām.

Datu aizsardzības pārkāpumi var nodarīt lielu kaitējumu to personu privātumam un datu aizsardzības tiesībām, kuras pārkāpuma rezultātā zaudē kontroli pār saviem personas datiem. Pārkāpumi var izraisīt identitātes zādzību vai krāpšanu, finansiālus zaudējumus vai materiālus zaudējumus, ar dienesta noslēpumu aizsargātu personas datu konfidencialitātes zaudēšanu un kaitējumu datu subjekta reputācijai. Pamatnostādnēs par personas datu aizsardzības pārkāpumu paziņošanu saskaņā ar Regulu (ES) 2016/679 29. panta darba grupa skaidro, ka pārkāpumiem var būt trīs veidu ietekme uz personas datiem: izpaušana, nozaudēšana un/vai izmaiņas[453]. Papildus pienākumam veikt pasākumus apstrādes drošības nodrošināšanai, kā

452 Vispārīgā datu aizsardzības regula, 4. panta 12. punkts; skatīt arī 29. panta darba grupas (2017) *Pamatnostādnes par personas datu aizsardzības pārkāpumu paziņošanu saskaņā ar Regulu 2016/679*, WP 250, 2017. gada 3. oktobris, 8. lpp.

453 29. panta darba grupa (2017), *Pamatnostādnes par personas datu aizsardzības pārkāpumu paziņošanu saskaņā ar Regulu 2016/679*, WP 250, 2017. gada 3. oktobris, 6. lpp.

paskaidrots 4.2. iedaļā, vienlīdz svarīgi arī nodrošināt, ka gadījumā, kad notiek pārkāpumi, pārziņi tos risina pienācīgi un savlaicīgi.

Uzraudzības iestādes un personas bieži neuzzina par datu aizsardzības pārkāpumu, un tas indivīdiem liedz veikt pasākumus, lai pasargātu sevi no tā negatīvajām sekām. Lai apstiprinātu privātpersonu tiesības un ierobežotu datu aizsardzības pārkāpumu ietekmi, **ES un EP** noteiktos apstākļos pārzinim uzliek pienākumu paziņot.

Saskaņā ar **EP** modernizēto Konvenciju Nr. 108 līgumslēdzējām pusēm obligāti jāuzliek pārziņiem pienākums ziņot kompetentajai uzraudzības iestādei par datu aizsardzības pārkāpumiem, kas var nopietni ietekmēt datu subjektu tiesības. Šāds paziņojums ir jāsniedz "nekavējoties"[454].

ES tiesību aktos ir noteikts sīki izstrādāts režīms attiecībā uz paziņojumu sniegšanas laiku un saturu[455]. Attiecīgi pārziņiem jāpaziņo uzraudzības iestādēm par noteiktiem datu aizsardzības pārkāpumiem bez nepamatotas kavēšanās un, ja iespējams, 72 stundu laikā pēc brīža, kad viņi uzzina par šādu pārkāpumu. Ja 72 stundu termiņš nav ievērots, paziņojumam jāpievieno paskaidrojums par kavēšanos. Pārziņus atbrīvo no paziņošanas pienākuma tikai tad, ja viņi spēj pierādīt, ka datu aizsardzības pārkāpums, visticamāk, nerada risku attiecīgo personu tiesībām un brīvībām.

Regulā ir noteikts minimālais informācijas apjoms, kas jāiekļauj paziņojumā, lai uzraudzības iestāde varētu veikt nepieciešamās darbības[456]. Paziņojumā jāiekļauj vismaz datu aizsardzības pārkāpuma rakstura apraksts un skarto datu subjektu kategorijas un aptuvenais skaits, pārkāpuma iespējamo seku un pārziņa īstenoto pasākumu, lai novērstu un mazinātu šīs sekas, apraksts. Turklāt ir jānorāda datu aizsardzības speciālista vai citas kontaktpersonas vārds un kontaktinformācija, lai kompetentā uzraudzības iestāde vajadzības gadījumā var iegūt papildu informāciju.

Ja datu aizsardzības pārkāpums var radīt lielu risku personu tiesībām un brīvībām, pārziņiem bez nepamatotas kavēšanās šīs personas (datu subjekti) jāinformē par pārkāpumu[457]. Informācija datu subjektiem, tostarp datu aizsardzības pārkāpuma apraksts, ir jāsagatavo skaidrā un saprotamā valodā, un tajā jāiekļauj līdzīga informācija kā paziņojumā uzraudzības iestādēm. Noteiktos gadījumos pārziņus var

454 Modernizētā Konvencija Nr. 108, 7. panta 2. punkts; modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 64.–66. punkts.

455 Vispārīgā datu aizsardzības regula, 33. un 34. pants.

456 Turpat, 33. panta 3. punkts.

457 Turpat, 34. pants.

atbrīvot no pienākuma informēt datu subjektus par šādiem pārkāpumiem. Atbrīvojumi attiecas uz gadījumiem, kad pārzinis ir īstenojis attiecīgus tehniskus un organizatoriskus aizsardzības pasākumus un minētie pasākumi ir piemēroti personas datiem, ko skāris personas datu aizsardzības pārkāpums, jo īpaši tādi pasākumi, kas personas datus padara nesaprotamus personām, kurām nav pilnvaru piekļūt datiem, piemēram, šifrēšana. Pēc pārkāpuma pārziņa veiktās darbības, lai nodrošinātu, ka vairs netiks nodarīts kaitējums datu subjektu tiesībām, var arī atbrīvot pārzini no pienākuma informēt datu subjektus. Visbeidzot, ja paziņojuma sniegšana rada nesamērīgas pūles pārzinim, datu subjektus var informēt par pārkāpumu, izmantojot citus līdzekļus, piemēram, izmantojot publisku komunikāciju vai līdzīgus pasākumus[458].

Pienākums paziņot par datu aizsardzības pārkāpumiem uzraudzības iestādēm un datu subjektiem attiecas uz pārziņiem. Tomēr datu aizsardzības pārkāpumi var notikt neatkarīgi no tā, vai apstrādi veic pārzinis vai apstrādātājs. Šā iemesla dēļ ir svarīgi nodrošināt, ka apstrādātājiem ir pienākums ziņot arī par datu aizsardzības pārkāpumiem. Šajā gadījumā apstrādātājiem bez nepamatotas kavēšanās jāinformē pārzinis par datu aizsardzības pārkāpumiem[459]. Pārziņa pienākums ir informēt uzraudzības iestādes un skartos datu subjektus, ievērojot iepriekš minētos noteikumus un termiņus.

4.3. Pārskatatbildības un atbilstības veicināšanas noteikumi

Svarīgākie aspekti

- Lai nodrošinātu pārskatatbildību par personas datu apstrādi, pārziņiem un apstrādātājiem jāuztur viņu atbildības jomā veikto apstrādes darbību uzskaite un pēc pieprasījuma tā jāsniedz uzraudzības iestādēm.
- Vispārīgajā datu aizsardzības regulā izklāstīti vairāki instrumenti atbilstības veicināšanai:
  - datu aizsardzības speciālistu iecelšana noteiktās situācijās;
  - ietekmes novērtējuma veikšana pirms to apstrādes darbību uzsākšanas, kuras, iespējams, rada lielu risku personu tiesībām un brīvībām;

458 Turpat, 34. panta 3. punkta c) apakšpunkts.

459 Turpat, 33. panta 2. punkts.

  - iepriekšēja apspriešanās ar attiecīgo uzraudzības iestādi, ja ietekmes novērtējums liecina, ka apstrāde rada riskus, kurus nevar mazināt;
  - pārziņu un apstrādātāju rīcības kodeksi, kuros precizē regulas piemērošanu dažādās apstrādes nozarēs;
  - sertifikācijas mehānismi, zīmogi un marķējumi;
- EP tiesībās modernizētajā Konvencijā Nr. 108 ierosināti līdzīgi instrumenti atbilstības veicināšanai.

Pārskatatbildības princips ir īpaši svarīgs, lai Eiropā garantētu datu aizsardzības noteikumu izpildi. Pārzinis ir atbildīgs par datu aizsardzības noteikumu ievērošanu, un viņam jāspēj šo atbilstību pierādīt. Pārskatatbildība nedrīkst iestāties tikai pēc pārkāpuma izdarīšanas. Pārziņiem ir drīzāk proaktīvs pienākums visos datu apstrādes posmos ievērot atbilstošu datu pārvaldības politiku. Eiropas tiesību aktos datu aizsardzības jomā pārziņiem paredzēts pienākums ieviest tehniskos un organizatoriskos pasākumus, lai nodrošinātu un spētu pierādīt, ka apstrāde tiek veikta saskaņā ar likumu. Starp šiem pasākumiem var minēt datu aizsardzības speciālistu iecelšanu, ar apstrādi saistītās uzskaites un dokumentācijas kārtošanu, kā arī privātuma ietekmes novērtējumu veikšanu.

4.3.1. Datu aizsardzības speciālisti

Datu aizsardzības speciālisti (DAS) ir personas, kuras organizācijās, kas veic datu apstrādi, konsultē par datu aizsardzības noteikumu ievērošanu. Viņi ir "pārskatatbildības stūrakmens", jo veicina noteikumu ievērošanu, vienlaikus darbojoties kā starpnieki starp uzraudzības iestādēm, datu subjektiem un organizāciju, kas viņus ir iecēlusi.

Saskaņā ar **EP tiesību aktiem** modernizētās Konvencijas Nr. 108 10. panta 1. punkts uzliek pārziņiem un apstrādātājiem vispārēju pārskatatbildību. Saskaņā ar to pārziņiem un apstrādātājiem ir jāievieš visi attiecīgie pasākumi, lai izpildītu konvencijā paredzētos datu aizsardzības noteikumus un spētu pierādīt, ka viņu kontrolē esošā datu apstrāde atbilst konvencijas noteikumiem. Kaut arī konvencijā nav noteikti konkrēti pasākumi, kas pārziņiem un apstrādātājiem ir jāievieš, modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā norādīts, ka DAS iecelšana būtu viens no iespējamiem pasākumiem, kas palīdzētu pierādīt atbilstību. DAS ir jānodrošina ar visiem līdzekļiem, kas nepieciešami viņu pilnvaru izpildei[460].

460 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 87. punkts.

Pretstatā EP tiesību aktiem **ES** tiesību aktos par DAS iecelšanu ne vienmēr lemj pārziņi un apstrādātāji, bet noteiktos apstākļos tas ir obligāti. VDAR atzīst DAS būtisko funkciju jaunajā pārvaldības sistēmā un ietver sīki izstrādātus noteikumus par speciālista iecelšanu, amatu, pienākumiem un uzdevumiem[461].

Saskaņā ar VDAR DAS iecelšana ir obligāta trīs īpašos gadījumos: ja apstrādi veic publiska iestāde vai struktūra, ja pārziņa vai apstrādātāja pamatdarbības veido apstrādes darbības, kurām nepieciešama regulāra un sistemātiska datu subjektu uzraudzība plašā mērogā, vai ja pamatdarbību veido īpašo kategoriju datu vai personas datu, kas saistīti ar sodāmību un nodarījumiem, apstrāde lielā apmērā[462]. Kaut arī tādi jēdzieni kā "sistemātiska uzraudzība lielā apmērā" un "pamatdarbība" nav definēti regulā, 29. panta darba grupa ir sniegusi pamatnostādnes par to interpretāciju[463].

Piemērs. Sociālo mediju uzņēmumus un meklētājprogrammas, iespējams, uzskatīs par pārziņiem, kuru apstrādes darbībām nepieciešama regulāra un sistemātiska datu subjektu uzraudzība lielā apjomā. Šādu uzņēmumu uzņēmējdarbības modelis ir balstīts uz personas datu apstrādi lielā apjomā, un tā nes ievērojamus ienākumus, piedāvājot mērķtiecīgus reklāmas pakalpojumus un ļaujot uzņēmumiem reklamēties vietnēs. Mērķtiecīga reklāma ir veids, kā izvietot reklāmas, pamatojoties uz demogrāfiskajiem datiem un patērētāju iepriekšējo pirkumu vēsturi vai uzvedību. Tāpēc tai nepieciešama sistemātiska datu subjektu tiešsaistes paradumu un uzvedības uzraudzība.

Piemērs. Slimnīca un veselības apdrošināšanas sabiedrība ir tipiski pārziņu piemēri, kuru darbība sastāv no īpašu kategoriju personas datu apstrādes lielā apjomā. Dati, kas atklāj informāciju par indivīda veselību, ir īpašu kategoriju personas dati gan EP, gan ES tiesību aktos, tāpēc tiem ir vajadzīga pastiprināta aizsardzība. ES tiesību aktos arī ģenētiskie un biometriskie dati ir atzīti kā īpašas kategorijas. Ciktāl medicīnas iestādes un apdrošināšanas sabiedrības apstrādā šādus datus lielā apjomā, saskaņā ar VDAR viņiem ir pienākums iecelt datu aizsardzības speciālistu.

461 Vispārīgā datu aizsardzības regula, 37.–39. pants.

462 Turpat, 37. panta 1. punkts.

463 29. panta darba grupa (2017), *Pamatnostādnes par datu aizsardzības speciālistiem* ("DAS"), WP 243 rev.01, pēdējoreiz pārskatītas un pieņemtas 2017. gada 5. aprīlī.

Turklāt VDAR 37. panta 4. punktā paredzēts, ka gadījumos, kas nav starp trim 37. panta 1. punktā noteiktajiem obligātajiem gadījumiem, pārzinis, apstrādātājs vai apvienības un citas struktūras, kas pārstāv pārziņu vai apstrādātāju kategorijas, var iecelt vai, ja to pieprasa Savienības vai dalībvalsts tiesību akti, ieceļ datu aizsardzības speciālistu.

Visām pārējām organizācijām nav juridiska pienākuma iecelt DAS. Tomēr VDAR paredzēts, ka pārziņi un apstrādātāji var izvēlēties brīvprātīgi iecelt DAS, vienlaikus dodot arī iespēju dalībvalstīm šādu iecelšanu noteikt par obligātu vairāk organizāciju veidiem, nekā tiem, kas paredzēti regulā[464].

Tiklīdz pārzinis ieceļ DAS, viņiem jāpārliecinās, ka viņš/viņa ir "pienācīgi un laikus iesaistīts visos jautājumos saistībā ar personas datu aizsardzību" organizācijā[465]. Piemēram, DAS ir jāiesaista konsultāciju sniegšanā par datu aizsardzības ietekmes novērtējumu veikšanu, kā arī datu apstrādes darbību izveidē un uzskaites uzturēšanā organizācijā. Lai DAS varētu efektīvi izpildīt savus uzdevumus, pārziņiem un apstrādātājiem jānodrošina viņiem nepieciešamie resursi, tostarp finanšu resursi, infrastruktūra un aprīkojums. Papildu prasības ietver pietiekama laika nodrošināšanu DAS viņu funkciju veikšanai un pastāvīgu apmācību, lai viņi varētu attīstīt savu kompetenci un būt informēti par visām datu aizsardzības tiesību aktu izmaiņām[466].

VDAR ir noteiktas dažas pamata garantijas, lai nodrošinātu DAS darbības neatkarību. Pārziņiem un apstrādātājiem jānodrošina, ka, pildot savus uzdevumus, kas saistīti ar datu aizsardzību, DAS nesaņem nekādus norādījumus no uzņēmuma, tostarp personām augstākajā vadības līmenī. Turklāt viņus nekādā veidā nedrīkst atcelt no pienākumiem vai sodīt par viņu uzdevumu izpildi[467]. Piemēram, ja DAS iesaka pārzinim vai apstrādātājam veikt datu aizsardzības ietekmes novērtējumu, jo viņš/viņa uzskata, ka apstrāde varētu radīt lielu risku datu subjektiem. Uzņēmums nepiekrīt DAS ieteikumam, neuzskata to par pamatotu un tāpēc nolemj neveikt ietekmes novērtējumu. Uzņēmums var ignorēt ieteikumus, taču nevar DAS atcelt no pienākumiem vai sodīt DAS par ieteikumu sniegšanu.

464 Vispārīgā datu aizsardzības regula, 37. panta 3. un 4. punkts.

465 Turpat, 38. panta 1. punkts.

466 29. panta darba grupa (2017), Pamatnostādnes par datu aizsardzības speciālistiem ("DAS"), WP 243 rev.01, pēdējoreiz pārskatītas un pieņemtas 2017. gada 5. aprīlī, 3.1. punkts.

467 Vispārīgā datu aizsardzības regula, 38. panta 2. un 3. punkts.

Visbeidzot DAS uzdevumi un pienākumi ir detalizēti aprakstīti VDAR 39. pantā. Šeit ietilpst prasības informēt un konsultēt uzņēmumus un darbiniekus, kas veic savu pienākumu apstrādi saskaņā ar tiesību aktiem, un uzraudzīt atbilstību ES un valstu datu aizsardzības noteikumiem, veicot revīzijas un apmācot apstrādes operācijās iesaistītos darbiniekus. DAS arī jāsadarbojas ar uzraudzības iestādi un jākļūst par tās kontaktpersonu jautājumos, kas saistīti ar datu apstrādi, piemēram, attiecībā uz datu aizsardzības pārkāpumiem.

Attiecībā uz personas datiem, kurus apstrādā ES iestādes un struktūras, Regulā (EK) Nr. 45/2001 paredzēts, ka katrai Savienības iestādei un struktūrai ir jāieceļ DAS. DAS ir uzticēts nodrošināt, ka regulas noteikumi ES iestādēs un struktūrās tiek pareizi piemēroti un ka datu subjekti un datu apstrādātāji tiek informēti par viņu tiesībām un pienākumiem[468]. Viņš vai viņa ir atbildīgs(-a) arī par atbildi uz EDAU pieprasījumiem un nepieciešamības gadījumā ar viņu sadarbojas. Tāpat kā VDAR, arī Regulā (EK) Nr. 45/2001 ir ietverti noteikumi par DAS neatkarību viņu uzdevumu veikšanā un nepieciešamību nodrošināt viņus ar nepieciešamo personālu un resursiem[469]. DAS jāinformē pirms ES iestāde vai struktūra (vai šo organizāciju departamenti) veic jebkādas apstrādes darbības, un viņiem jāuztur visu paziņoto apstrādes darbību uzskaite[470].

4.3.2. Apstrādes darbību reģistrēšana

Lai uzņēmumi spētu pierādīt atbilstību un tiktu saukti pie atbildības, uzņēmumiem nereti ir likumīgi noteikts pienākums dokumentēt un reģistrēt savu darbību. Svarīgs piemērs ir nodokļu tiesības un revīzijas, kas visiem uzņēmumiem prasa uzturēt plašu dokumentāciju un lietvedību. Ir svarīgi noteikt arī līdzīgas prasības citās tiesību jomās, jo īpaši datu aizsardzības tiesībās, jo lietvedība ir būtisks veids, kā atvieglot datu aizsardzības noteikumu ievērošanu. Tādējādi **ES tiesību aktos** paredzēts, ka pārziņiem vai viņu pārstāvjiem jāreģistrē to pakļautībā veiktās apstrādes darbības[471]. Šā pienākuma mērķis ir nodrošināt, ka vajadzības gadījumā uzraudzības iestādēm ir nepieciešamā dokumentācija, lai varētu apstiprināt apstrādes likumību.

468 Pilnīgu DAS uzdevumu sarakstu skatīt Regulas (EK) Nr. 45/2001 24. panta 1. punktā.

469 Regula (EK) Nr. 45/2001, 24. panta 6. un 7. punkts.

470 Turpat, 25. un 26. pants.

471 Vispārīgā datu aizsardzības regula, 30. pants.

Dokumentējamā informācija ietver turpmāk norādīto:

- pārziņa un attiecīgajā gadījumā kopīgo pārziņu, pārziņa pārstāvja un DAS nosaukums/vārds, uzvārds un kontaktinformācija;
- apstrādes nolūki;
- ar datu apstrādi saistīto datu subjektu kategoriju un personas datu kategoriju apraksts;
- informācija par saņēmēju kategorijām, kurām tiek vai tiks izpausti personas dati;
- informācija par to, vai tiek vai tiks veikta personas datu nosūtīšana trešām valstīm vai starptautiskām organizācijām;
- ja iespējams, termiņi, kas paredzēti dažādu kategoriju personas datu dzēšanai, kā arī pārskats par tehniskajiem pasākumiem, kas ieviesti, lai nodrošinātu apstrādes drošību[472].

Pienākums veikt apstrādes darbību uzskaiti saskaņā ar VDAR attiecas ne tikai uz pārziņiem, bet arī apstrādātājiem. Šis ir svarīgs pagrieziens, jo pirms regulas pieņemšanas līgums, kas noslēgts starp pārzini un apstrādātāju, galvenokārt attiecās uz apstrādātāja pienākumiem. Viņu uzskaites veikšanas pienākums tagad ir tieši paredzēts likumā.

VDAR paredzēts izņēmums šim pienākumam. Prasība veikt uzskaiti neattiecas uz uzņēmumu vai organizāciju (pārzini vai apstrādātāju), kas nodarbina mazāk nekā 250 personas. Izņēmumam tomēr piemēro prasības, ka attiecīgā organizācija neveic apstrādi, kas varētu radīt risku datu subjektu tiesībām un brīvībām, ka apstrāde ir tikai neregulāra un ka tajā nav iekļautas īpašas datu kategorijas, kas minētas 9. panta 1. punktā, vai personas dati, kas saistīti ar sodāmību un 10. pantā minētajiem nodarījumiem.

Apstrādes darbību uzskaitei ir jāļauj pārziņiem un apstrādātājiem pierādīt atbilstību regulai. Tai ir arī jāļauj uzraudzības iestādēm uzraudzīt apstrādes likumību. Ja uzraudzības iestāde pieprasa piekļuvi šai uzskaitei, pārziņiem un apstrādātājiem ir pienākums sadarboties un nodrošināt pieeju.

472 Turpat, 30. panta 1. punkts.

4.3.3. Novērtējums par ietekmi uz datu aizsardzību un iepriekšēja apspriešanās

Apstrādes darbībām ir raksturīgi daži riski personu tiesībām. Personas dati var tikt nozaudēti, izpausti nepiederošām personām vai apstrādāti nelikumīgā veidā. Protams, riski atšķiras atkarībā no apstrādes veida un apjoma. Piemēram, liela mēroga darbības, kas saistītas ar sensitīvu datu apstrādi, rada datu subjektiem daudz augstāku riska līmeni salīdzinājumā ar iespējamiem riskiem, kad mazs uzņēmums apstrādā savu darbinieku adreses un personiskos tālruņu numurus.

Tā kā parādās jaunas tehnoloģijas un apstrāde kļūst arvien sarežģītāka, pārziņiem ir jāpievēršas šādiem riskiem un pirms apstrādes sākšanas jāpārbauda paredzētās apstrādes iespējamā ietekme. Tas ļauj organizācijām iepriekš pareizi identificēt, novērst un mazināt riskus, ievērojami samazinot apstrādes negatīvās ietekmes uz indivīdiem iespējamību.

Datu aizsardzības ietekmes novērtējumi ir paredzēti **gan EP, gan ES tiesību aktos**. EP tiesiskajā regulējumā modernizētās Konvencijas Nr. 108 10. panta 2. punkts uzliek līgumslēdzējām pusēm pienākumu nodrošināt, lai pārziņi un apstrādātāji "pirms šādas apstrādes sākšanas pārbaudītu paredzētās datu apstrādes iespējamo ietekmi uz datu subjektu tiesībām un pamatbrīvībām" un pēc novērtējuma plānotu apstrādi tā, lai novērstu vai samazinātu ar apstrādi saistītos riskus.

ES tiesību aktos paredzēts līdzīgs, detalizētāk izstrādāts pienākums pārziņiem, uz kuriem attiecas VDAR. Kā 35. pantā paredzēts, ietekmes novērtējums jāveic gadījumos, kad apstrāde, iespējams, rada lielu risku indivīdu tiesībām un brīvībām. Regulā nav noteikts, kā vērtēt riska iespējamību, bet gan norādīts, kādi varētu būt šie riski[473]. Tajā ietverts to apstrādes darbību saraksts, kuras uzskata par paaugstināta riska darbībām un kurām īpaši nepieciešams iepriekšējs ietekmes novērtējums, proti, gadījumos, kad:

- personas dati tiek apstrādāti, lai pieņemtu lēmumus par fiziskām personām pēc sistemātiska un plaša personisko aspektu, kas attiecas uz šiem indivīdiem, izvērtējuma (profilēšana);

- sensitīvi dati vai personas dati, kas attiecas uz sodāmību un pārkāpumiem, tiek apstrādāti lielā apjomā;

473 Vispārīgā datu aizsardzības regula, preambula, 75. apsvērums.

- apstrāde ietver plašu un sistemātisku publiski pieejamu teritoriju uzraudzību.

Uzraudzības iestādēm jāpieņem un jāpublicē to apstrādes darbību saraksts, attiecībā uz kurām jāveic ietekmes novērtējumi. Tās var arī izveidot to apstrādes darbību sarakstu, kas ir atbrīvotas no šā pienākuma[474].

Ja ietekmes novērtējums ir obligāts, pārziņiem jānovērtē apstrādes nepieciešamība un samērīgums, kā arī iespējamie riski personu tiesībām. Ietekmes novērtējumā jāietver arī plānotie drošības pasākumi identificēto risku novēršanai. Lai izveidotu sarakstus, dalībvalstu uzraudzības iestādēm ir jāsadarbojas savā starpā un ar Eiropas Datu aizsardzības kolēģiju. Tas visā ES nodrošinās konsekventu pieeju tām darbībām, kurām obligāti jāveic ietekmes novērtējums, un uz pārziņiem neatkarīgi no atrašanās vietas attieksies līdzīgas prasības.

Ja pēc ietekmes novērtējuma izrādās, ka apstrāde radīs lielu risku personu tiesībām, turklāt nav ieviesti nekādi riska samazināšanas pasākumi, pārzinim pirms apstrādes darbības sākšanas ir jākonsultējas ar attiecīgo uzraudzības iestādi[475].

29. panta darba grupa ir izdevusi pamatnostādnes par datu aizsardzības ietekmes novērtējumiem un par to, kā noteikt, vai apstrāde var radīt lielu risku[476]. Tā izstrādāja deviņus kritērijus, lai palīdzētu noteikt, vai datu aizsardzības ietekmes novērtējums konkrētā gadījumā ir nepieciešams[477]: 1) novērtēšana vai punktu piešķiršana; 2) automatizēta lēmumu pieņemšana ar juridiskām vai līdzīgi būtiskām sekām; 3) sistemātiska uzraudzība; 4) sensitīvi dati; 5) dati, kas tiek apstrādāti lielā apjomā; 6) saskaņotās vai apvienotās datu kopas; 7) dati par neaizsargātiem datu subjektiem; 8) inovatīvs lietojums vai tehnoloģisku vai organizatorisku risinājumu pielietošana; 9) ja apstrāde pati par sevi "liedz datu subjektiem īstenot tiesības vai izmantot pakalpojumu vai līgumu". 29. panta darba grupa ieviesa vērtēšanas principu, ka apstrādes darbības, kas atbilst mazāk nekā diviem kritērijiem, rada zemāku riska līmeni un nav nepieciešams datu aizsardzības novērtējums, savukārt tām, kas atbilst diviem vai vairākiem kritērijiem, šāds novērtējums ir nepieciešams. Gadījumos, kad

474 Turpat, 35. panta 4. un 5. punkts.

475 Turpat, 36. panta 1. punkts; 29. panta darba grupa (2017), *Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA) veikšanai un noskaidrošanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē*, WP 248 rev. 01, Brisele, 2017. gada 4. oktobris.

476 29. panta darba grupa (2017), *Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA) veikšanai un noskaidrošanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē*, WP 248 rev. 01, Brisele, 2017. gada 4. oktobris.

477 Turpat, 9.–11. lpp.

nav skaidrs, vai ir nepieciešams datu aizsardzības ietekmes novērtējums, 29. panta darba grupa iesaka veikt šādu novērtējumu, jo tas ir "noderīgs rīks, kas palīdz datu apstrādātājiem ievērot datu aizsardzības tiesības"[478]. Ja tiek ieviesta jauna datu apstrādes tehnoloģija, ir būtiski veikt datu aizsardzības ietekmes novērtējumu[479].

4.3.4. Rīcības kodeksi

Rīcības kodeksi ir paredzēti izmantošanai vairākās nozarēs, lai ieskicētu un precizētu VDAR piemērošanu konkrētajās nozarēs. Personas datu pārziņiem un apstrādātājiem šādu kodeksu izveidošana var ievērojami uzlabot atbilstību un ES datu aizsardzības noteikumu ieviešanu. Nozares dalībnieku zināšanas palīdzēs rast risinājumus, kas ir praktiski un līdz ar to ticamāk, ka tiks ievēroti. Atzīstot šādu kodeksu nozīmi datu aizsardzības tiesību efektīvā piemērošanā, VDAR aicina dalībvalstis, uzraudzības iestādes, Komisiju un Eiropas Datu aizsardzības kolēģiju mudināt izstrādāt rīcības kodeksus, kuru mērķis ir dot ieguldījumu pareizā regulas piemērošanā visā ES[480]. Kodeksos varētu precizēt regulas piemērošanu konkrētās nozarēs, ieskaitot tādus jautājumus kā personas datu vākšana, informācija, kas jāsniedz datu subjektiem un sabiedrībai, un datu subjektu tiesību īstenošana.

Lai nodrošinātu rīcības kodeksu atbilstību saskaņā ar VDAR ieviestajiem noteikumiem, kodeksi pirms to pieņemšanas jāiesniedz kompetentajai uzraudzības iestādei. Pēc tam uzraudzības iestāde sniedz atzinumu par to, vai iesniegtais kodeksa priekšlikums sekmē atbilstību regulai, un, ja tā konstatē, ka kodekss nodrošina attiecīgus aizsardzības pasākumus, iestāde apstiprina kodeksu[481]. Uzraudzības iestādēm jāpublicē apstiprinātie rīcības kodeksi, kā arī kritēriji, uz kuriem balstīta to apstiprināšana. Ja rīcības kodeksa priekšlikums attiecas uz apstrādes darbībām vairākās dalībvalstīs, kompetentā uzraudzības iestāde pirms kodeksa, grozījumu vai papildinājumu priekšlikuma apstiprināšanas iesniedz kodeksu Eiropas Datu aizsardzības kolēģijai, kas sniedz atzinumu par kodeksa atbilstību VDAR. Komisija ar īstenošanas aktiem var nolemt, ka tai iesniegtajam apstiprinātajam rīcības kodeksam ir vispārējs spēks Savienībā.

Rīcības kodeksa ievērošana sniedz nozīmīgas priekšrocības gan datu subjektiem, gan pārziņiem un apstrādātājiem. Šādi kodeksi sniedz sīki izstrādātas vadlīnijas,

478 Turpat, 9. lpp.

479 Turpat.

480 Vispārīgā datu aizsardzības regula, 40. panta 1. punkts.

481 Turpat, 40. panta 5. punkts.

ar ko juridiskās prasības pielāgo konkrētām nozarēm un veicina apstrādes darbību pārredzamību. Pārziņi un apstrādātāji var izmantot šo kodeksu ievērošanu arī kā pierādījumus savai atbilstībai ES tiesību aktiem un kā līdzekli sava sabiedriskā tēla kā organizāciju, kuras savās darbībās piešķir prioritāru statusu datu aizsardzībai un apņemas to ievērot, uzlabošanai. Apstiprinātus rīcības kodeksus kopā ar saistošām un izpildāmām saistībām var izmantot kā attiecīgus aizsardzības pasākumus datu nosūtīšanai trešām valstīm. Lai nodrošinātu, ka organizācijas, kam ir rīcības kodeksi, tos patiešām ievēro, to uzraudzībai un atbilstības nodrošināšanai var tikt izveidota īpaša struktūra (ko akreditējusi attiecīgā uzraudzības iestāde). Lai efektīvi pildītu savus uzdevumus, struktūrai jābūt neatkarīgai, ar apliecinātu kompetenci jautājumos, ko regulē rīcības kodekss, un tai jābūt pārredzamām procedūrām un struktūrām, lai varētu izskatīt sūdzības par kodeksa pārkāpumiem[482].

Saskaņā ar **EP tiesību aktiem** modernizētajā Konvencijā Nr. 108 paredzēts, ka valstu tiesību aktos garantēto datu aizsardzības līmeni var lietderīgi uzlabot ar brīvprātīgiem reglamentējošiem pasākumiem, piemēram, labas prakses kodeksiem vai profesionālās ētikas kodeksiem. Tomēr tie ir tikai brīvprātīgi pasākumi saskaņā ar modernizēto Konvenciju Nr. 108: šeit neizriet nekāds juridisks pienākums ieviest šādus pasākumus, kaut arī tas ir ieteicams, un ar šādiem pasākumiem vien nepietiek, lai nodrošinātu pilnīgu atbilstību konvencijai[483].

4.3.5. Sertifikācija

Papildu rīcības kodeksiem sertifikācijas mehānismi un datu aizsardzības zīmogi un marķējumi ir vēl viens līdzeklis, ar ko pārziņi un apstrādātāji var pierādīt atbilstību VDAR. Šajā nolūkā ar regulu paredz brīvprātīgu sertifikācijas sistēmu, saskaņā ar kuru noteiktas organizācijas vai uzraudzības iestādes var izsniegt sertifikātus. Pārziņi un apstrādātāji, kuri izvēlas ievērot sertifikācijas mehānismu, var iegūt lielāku atpazīstamību un uzticamību, jo sertifikāti, zīmogi un marķējumi ļauj datu subjektiem ātri novērtēt organizācijas datu apstrādes aizsardzības līmeni. Svarīgi, ka šādas sertifikācijas esamība pārzinim vai apstrādātājam nemazina tā pienākumus un atbildību ievērot visas regulas prasības.

482 Turpat, 41. panta 1. un 2. punkts.

483 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 33. punkts

4.4. Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma

Integrēta datu aizsardzība

ES tiesību aktos ir pārziņiem noteikts pienākums ieviest pasākumus, lai efektīvi īstenotu datu aizsardzības principus un integrētu nepieciešamos aizsardzības pasākumus nolūkā izpildīt regulas prasības un aizsargāt datu subjektu tiesības[484]. Šie pasākumi ir jāīsteno gan apstrādes laikā, gan nosakot apstrādes līdzekļus. Īstenojot šādus pasākumus, pārzinim jāņem vērā tehniskais līmenis, ieviešanas izmaksas, personas datu apstrādes raksturs, tvērums un mērķi, kā arī riski un to nopietnība attiecībā uz datu subjekta tiesībām un brīvībām[485].

EP tiesību aktos paredzēts, ka pārziņiem un apstrādātājiem pirms apstrādes uzsākšanas jānovērtē personas datu apstrādes iespējamā ietekme uz datu subjektu tiesībām un brīvībām. Turklāt pārziņiem un apstrādātājiem ir pienākums datu apstrādi plānot tā, lai novērstu vai mazinātu šo tiesību un brīvību pārkāpuma risku, un ieviest tehniskus un organizatoriskus pasākumus, kuros ņemta vērā ietekme uz tiesībām uz aizsardzību visos personas datu apstrādes posmos[486].

Datu aizsardzība pēc noklusējuma

ES tiesību aktos noteikts, ka pārzinim ir jāveic attiecīgi pasākumi, lai nodrošinātu, ka pēc noklusējuma tiek apstrādāti tikai tie personas dati, kas nepieciešami mērķiem. Šis pienākums attiecas uz vākto personas datu daudzumu, apstrādes apmēru, glabāšanas periodu un pieejamību[487]. Ar šādu pasākumu ir jānodrošina, piemēram, tas, ka ne visiem pārziņu darbiniekiem ir piekļuve subjektu personas datiem. EDAU ir izstrādājis papildu norādījumus metodiskajā līdzeklī *Necessity Toolkit*[488].

EP tiesību aktos paredzēts, ka pārziņiem un apstrādātājiem jāīsteno tehniski un organizatoriski pasākumi, apsverot tiesību uz datu aizsardzību sekas, un jāievieš

484 Vispārīgā datu aizsardzības regula, 25. panta 1. punkts.

485 29. panta darba grupa (2017), Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA) veikšanai un noskaidrošanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē, WP 248 rev. 01, 2017. gada 4. oktobris. Skatīt arī *ENISA* (2015), Integrēta privātuma un datu aizsardzība – no politikas līdz inženierijai, 2015. gada 12. janvāris.

486 Modernizētā Konvencija Nr. 108, 10. panta 2. un 3. punkts, modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 89. punkts.

487 Vispārīgā datu aizsardzības regula, 25. panta 2. punkts.

488 Eiropas Datu aizsardzības uzraudzītājs (EDAU), (2017), *Necessity Toolkit*, Brisele, 2017. gada 11. aprīlis.

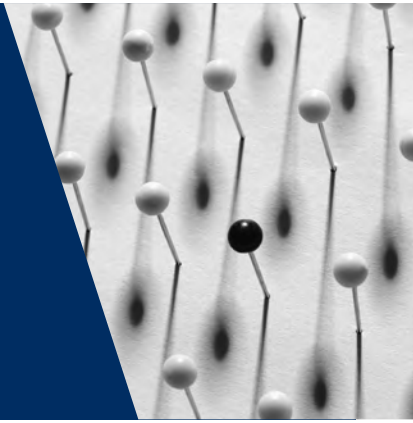
tehniski un organizatoriski pasākumi, kuros visos datu apstrādes posmos ņemtas vērā tiesību uz personas datu aizsardzības sekas[489].

ENISA 2016. gadā publicēja ziņojumu par pieejamajiem privātuma rīkiem un pakalpojumiem[490]. Cita starpā šajā novērtējumā sniegti kritēriji un parametri, kas ir labas vai sliktas privātuma prakses rādītāji. Kamēr daži kritēriji tieši attiecas uz VDAR noteikumiem, piemēram, pseidonimizāciju un apstiprinātiem sertifikācijas mehānismiem, citi piedāvā inovatīvas iniciatīvas, lai nodrošinātu integrētu privātuma aizsardzību un datu aizsardzību pēc noklusējuma. Piemēram, kaut arī lietojamības kritērijs nav tieši saistīts ar privātumu, tas var uzlabot privātumu, jo var ļaut plašāk piemērot privātuma rīku vai pakalpojumu. Patiesi, privātuma rīkus, kurus ir grūti ieviest praksē, plašākā sabiedrība var izmantot ļoti mazā apmērā, pat ja tie piedāvā ļoti stingras privātuma garantijas. Turklāt kritiski svarīgs ir privātuma rīka gatavības un stabilitātes kritērijs — tas nozīmē, kā rīks laika gaitā attīstās un reaģē uz esošām vai jaunām problēmām privātuma jomā. Citas ar privātumu saistītas tehnoloģijas, piemēram, drošas komunikācijas kontekstā, ietver šifrēšanu no viena gala līdz otram (komunikāciju, kur ziņojumus var izlasīt tikai tie cilvēki, kuri sazinās); klienta-servera šifrēšanu (starp klientu un serveri izveidotā komunikācijas kanāla šifrēšanu); autentifikāciju (komunikācijā iesaistīto pušu identitātes pārbaudi); un anonīmu komunikāciju (neviena trešā persona nevar identificēt komunikācijā iesaistītās puses).

489 Modernizētā Konvencija Nr. 108, 10. panta 3. punkts, modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 89. punkts.

490 *ENISA*, Privātuma aizsardzības tehnoloģiju kontroles matrica: sistemātiska pieeja tiešsaistes un mobilo konfidencialitātes rīku novērtēšanai, 2016. gada 20. decembris.

5 Neatkarīga uzraudzība



ES	Aptvertie jautājumi	EP
Harta, 8. panta 3. punkts Līgums par ES darbību, 16. panta 2. punkts Vispārīgā datu aizsardzības regula, 51.–59. pants EST lieta C-518/07 *Eiropas Komisija pret Vācijas Federatīvo Republiku* [GC], 2010 EST lieta C-614/10 *Eiropas Komisija pret Austrijas Republiku* [GC], 2012 EST lieta C-288/12 *Eiropas Komisija pret Ungāriju* [GC], 2014 EST lieta C-362/14 *Maximillian Schrems pret Datu aizsardzības komisāru* [GC], 2015.	**Uzraudzības iestādes**	Modernizētā Konvencija Nr. 108, 15. pants
Vispārīgā datu aizsardzības regula, 60.–67. pants	**Uzraudzības iestāžu sadarbība**	Modernizētā Konvencija Nr. 108, 16.–21. pants
Vispārīgā datu aizsardzības regula, 68.–76. pants	**Eiropas Datu aizsardzības kolēģija**	

Svarīgākie aspekti

- Neatkarīga uzraudzība ir būtiska Eiropas datu aizsardzības tiesību sastāvdaļa, un tā ir nostiprināta Hartas 8. panta 3 punktā.
- Lai nodrošinātu efektīvu datu aizsardzību, saskaņā ar valstu tiesību aktiem ir jāizveido neatkarīgas uzraudzības iestādes.
- Uzraudzības iestādēm jārīkojas pilnīgi neatkarīgi, tam jābūt garantētam dibināšanas likumā un tas jāatspoguļo uzraudzības iestādes īpašajā organizatoriskajā struktūrā.
- Uzraudzības iestādēm ir īpašas pilnvaras un uzdevumi. Tie cita starpā ir šādi:
  - uzraudzīt un veicināt datu aizsardzību valsts mērogā;
  - konsultēt datu subjektus un pārziņus, kā arī valdību un sabiedrību kopumā;
  - izskatīt sūdzības un palīdzēt datu subjektiem saistībā ar iespējamiem datu aizsardzības tiesību pārkāpumiem;
  - pārraudzīt pārziņus un apstrādātājus.
- Uzraudzības iestādēm ir arī pilnvaras nepieciešamības gadījumā iejaukties šādos veidos:
  - brīdināt pārziņus un apstrādātājus, izteikt rājienu vai pat piemērot naudas sodu;
  - uzdot labot, bloķēt vai dzēst datus;
  - piemērot apstrādes aizliegumu vai administratīvo naudas sodu;
  - nodot lietu izskatīšanai tiesā.
- Tā kā personas datu apstrādē bieži ir iesaistīti pārziņi, apstrādātāji un datu subjekti, kas atrodas dažādās valstīs, uzraudzības iestādēm ir savstarpēji jāsadarbojas pārrobežu jautājumos, lai nodrošinātu efektīvu personu aizsardzību Eiropā.
- ES ar Vispārīgo datu aizsardzības regulu izveidots vienas pieturas aģentūras mehānisms pārrobežu apstrādes lietām. Daži uzņēmumi veic pārrobežu apstrādes darbības sakarā ar personas datu apstrādi saistībā ar uzņēmumu darbībām vairāk nekā vienā dalībvalstī vai saistībā ar atsevišķu uzņēmumu Savienībā, bet kas būtiski ietekmē datu subjektus vairāk nekā vienā dalībvalstī. Saskaņā ar mehānismu šādiem uzņēmumiem jāsadarbojas tikai ar vienu valsts datu aizsardzības uzraudzības iestādi.
- Sadarbības un konsekvences mehānisms ļaus izmantot saskaņotu pieeju starp visām lietā iesaistītajām uzraudzības iestādēm. Galvenās vai vienīgās uzņēmējdarbības vietas vadošā uzraudzības iestāde sniegs konsultācijas un iesniegs lēmuma projektu citām iesaistītajām uzraudzības iestādēm.

- Līdzīgi kā pašreizējā 29. panta darba grupā, katras dalībvalsts uzraudzības iestāde un Eiropas Datu aizsardzības uzraudzītājs (EDAU) ietilps Eiropas Datu aizsardzības kolēģijā.
- Eiropas Datu aizsardzības kolēģijas uzdevumos ietilpst, piemēram, regulas pareizas piemērošanas uzraudzība, konsultāciju sniegšana Komisijai par attiecīgajiem jautājumiem, atzinumu, vadlīniju vai paraugprakses izdošana par dažādām tēmām.
- Galvenā atšķirība ir tā, ka Eiropas Datu aizsardzības kolēģija sniedz ne tikai atzinumus, kā paredzēts Direktīvā 95/46/EK. Tā izdod arī saistošus lēmumus gadījumos, kad uzraudzības iestāde vienas pieturas aģentūras gadījumos ir izvirzījusi būtisku un motivētu iebildumu, ja ir pretrunīgi viedokļi attiecībā uz to, kura no uzraudzības iestādēm ir vadošā, un, visbeidzot, ja kompetentā uzraudzības iestāde nelūdz vai neievēro EDAK atzinumu. Mērķis ir nodrošināt konsekventu regulas piemērošanu visās dalībvalstīs.

Neatkarīga uzraudzība ir būtiska Eiropas datu aizsardzības tiesību aktu sastāvdaļa. Gan ES, gan EP tiesību aktos neatkarīgu uzraudzības iestāžu pastāvēšana tiek uzskatīta par obligātu personu tiesību un brīvību efektīvai aizsardzībai attiecībā uz viņu personas datu apstrādi. Tā kā datu apstrāde kļūst arvien aktuālāka un indivīdiem arvien sarežģītāka, šīs iestādes ir digitālā laikmeta sargsuņi. ES neatkarīgu uzraudzības iestāžu pastāvēšana tiek uzskatīta par vienu no būtiskākajiem elementiem tiesībām uz personas datu aizsardzību, kas nostiprinātas ES primārajos tiesību aktos. ES Pamattiesību hartas 8. panta 3. punktā un LESD 16. panta 2. punktā personas datu aizsardzība ir atzīta par pamattiesībām un apstiprināts, ka datu aizsardzības noteikumu ievērošana ir jāpārbauda neatkarīgai iestādei.

Neatkarīgas uzraudzības nozīme datu aizsardzības tiesībās ir atzīta arī judikatūrā.

Piemērs. Lieta *Schrems*[491] EST skāra jautājumu, vai personas datu nosūtīšana Amerikas Savienotajām Valstīm (ASV) saskaņā ar pirmo ES un ASV Nolīgumu par drošības zonu (*Safe Harbour Agreement*) notika atbilstoši ES datu aizsardzības tiesību aktiem, ņemot vērā Edvarda Snoudena atklāto, ka ASV Nacionālās drošības aģentūra veic masveida novērošanu. Personas datu nosūtīšana uz ASV pamatojās uz 2000. gadā pieņemto Eiropas Komisijas lēmumu, kas ļāva personas datus no ES pārsūtīt ASV organizācijām, kuras veikušas pašsertifikāciju saskaņā ar drošības zonas shēmu, pamatojoties uz to, ka šī shēma nodrošina atbilstošu personas datu aizsardzības līmeni. Pēc lūguma izmeklēt prasītāja sūdzību par datu nosūtīšanas likumību, pamatojoties uz Snoudena atklājumiem, Īrijas uzraudzības iestāde sūdzību noraidīja,

491 EST 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems pret Datu aizsardzības komisāru* [GC].

pamatojoties uz to, ka Komisijas lēmums par ASV datu aizsardzības režīma atbilstību ir atspoguļots drošības zonas principos ("Lēmums par drošības zonu") neļauj tai sīkāk izmeklēt sūdzību.

EST savukārt uzskatīja, ka fakts, ka pastāv Komisijas lēmums, ar kuru tiek atļauta datu nosūtīšana trešām valstīm un kurš nodrošina atbilstošu aizsardzības līmeni, neatceļ un nemazina valstu uzraudzības iestāžu pilnvaras. EST atzīmēja, ka šo iestāžu pilnvaras uzraudzīt un nodrošināt atbilstību ES datu aizsardzības noteikumiem izriet no ES primārajiem tiesību aktiem, jo īpaši Hartas 8. panta 3. punkta un LESD 16. panta 2. punkta. "Neatkarīgas uzraudzības iestādes izveide (..) ir būtisks apstāklis personu aizsardzības nodrošināšanā attiecībā uz personas datu apstrādi"[492].

Tādēļ EST lēma, ka pat tad, ja uz personas datu nosūtīšanu attiecināms Komisijas lēmums par aizsardzības līmeņa pietiekamību un sūdzība ir iesniegta valsts uzraudzības iestādei, iestādei sūdzība rūpīgi jāizskata. Uzraudzības iestāde var noraidīt sūdzību, ja uzskata, ka tā nav pamatota. Šādā gadījumā EST uzsvēra, ka saskaņā ar tiesībām uz efektīvu tiesisko aizsardzību indivīdiem jābūt iespējai apstrīdēt šādu lēmumu valstu tiesās, kuras var vērsties EST, lai saņemtu prejudiciālu nolēmumu par Komisijas lēmuma spēkā esamību. Ja uzraudzības iestāde uzskata, ka sūdzība ir pamatota, tai jābūt iespējai uzsākt tiesvedību un iesniegt lietu izskatīšanai valstu tiesās. Valstu tiesas var nodot lietu EST, jo tā ir vienīgā institūcija, kas ir pilnvarota lemt, vai Komisijas lēmums par aizsardzības līmeņa pietiekamību ir spēkā[493].

Tālāk EST pārbaudīja lēmuma par drošības zonu pamatotību, lai noteiktu, vai nosūtīšanas sistēma atbilst ES datu aizsardzības noteikumiem. Tiesa secināja, ka lēmuma par drošības zonu 3. punkts ierobežo valstu uzraudzības iestāžu pilnvaras (kas piešķirtas saskaņā ar Datu aizsardzības direktīvu) rīkoties, lai novērstu datu nosūtīšanu, ja personas datu aizsardzības līmenis ASV ir nepietiekams. Ņemot vērā neatkarīgo uzraudzības iestāžu nozīmi datu aizsardzības tiesību aktu ievērošanas nodrošināšanā, EST uzskatīja, ka saskaņā ar Datu aizsardzības direktīvu un lasot to kopā ar Hartu, Komisijai nebija pilnvaru

492 EST 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems pret Datu aizsardzības komisāru* [GC], 41. punkts.

493 Turpat, 53.–66. punkts.

šādi ierobežot neatkarīgu uzraudzības iestāžu pilnvaras. Uzraudzības iestāžu pilnvaru ierobežošana bija viens no iemesliem, kādēļ EST pasludināja lēmumu par drošības zonu par spēkā neesošu.

Tādējādi Eiropas tiesībās ir ietverta prasība par neatkarīgu uzraudzību kā svarīgu mehānismu efektīvas datu aizsardzības nodrošināšanai. Neatkarīgas uzraudzības iestādes ir pirmais datu subjektu kontaktpunkts privātuma pārkāpumu gadījumos[494]. Saskaņā ar ES un EP tiesību aktiem uzraudzības iestāžu izveidošana ir obligāta. Abi tiesiskie regulējumi šo iestāžu uzdevumus un pilnvaras apraksta līdzīgi tiem, kas ietverti VDAR. Tāpēc uzraudzības iestādēm principā ir jādarbojas vienādi gan saskaņā ar ES tiesību aktiem, gan EP tiesību aktiem[495].

5.1. Neatkarība

ES un **EP tiesību aktos** prasīts, lai katra uzraudzības iestāde, veicot savus uzdevumus un īstenojot pilnvaras, rīkotos pilnīgi neatkarīgi[496]. Uzraudzības iestādes un tās locekļu, kā arī personāla neatkarība no tiešas vai netiešas ārējas ietekmes ir būtiska, lai garantētu pilnīgu objektivitāti, lemjot par datu aizsardzības jautājumiem. Tiesību aktos, kas ir uzraudzības iestādes izveidošanas pamatā, jāiekļauj ne tikai noteikumi, kas īpaši garantē neatkarību, bet arī iestādes organizatoriskajai struktūrai ir jāapliecina tās neatkarība. EST 2010. gadā pirmo reizi aplūkoja jautājumu, cik lielā mērā datu aizsardzības uzraudzības iestādēm jābūt neatkarīgām[497]. Izceltie piemēri ilustrē EST "pilnīgas neatkarības" nozīmes definīciju.

Piemērs. Lietā *Eiropas Komisija pret Vācijas Federatīvo Republiku*[498] Eiropas Komisija lūdza EST atzīt, ka Vācija ir nepareizi transponējusi prasību attiecībā uz par datu aizsardzības nodrošināšanu atbildīgo uzraudzības iestāžu "pilnīgu neatkarību" un tādējādi nav izpildījusi Datu aizsardzības direktīvas 28. pantā 1. punktā noteiktos pienākumus. Komisija uzskatīja, ka apstāklis,

494 Vispārīgā datu aizsardzības regula, 13. panta 2. punkta d) apakšpunkts.

495 Turpat, 51. pants, modernizētā Konvencija Nr. 108, 12. pants.

496 Vispārīgā datu aizsardzības regula, 52. panta 1. punkts; modernizētā Konvencija Nr. 108, 15. panta 5. punkts.

497 *FRA* (2010), *Pamattiesības: problēmas un sasniegumi 2010. gadā*, 2010. gada ziņojums, 59. lpp.; *FRA* (2010), *Datu aizsardzība Eiropas Savienībā: valsts datu aizsardzības iestāžu loma*, 2010. gada maijs.

498 EST 2010. gada 9. marta spriedums lietā C-518/07 *Eiropas Komisija pret Vācijas Federatīvo Republiku* [GC], 27. punkts.

ka Vācijā uzraudzības iestādes, kas atbildīgas par personas datu apstrādi dažādās federālajās zemēs (*Länder*), ir valsts uzraudzībā, lai nodrošinātu datu aizsardzības likuma ievērošanu, pārkāpj neatkarības prasību.

EST uzsvēra, ka vārdi "pilnīga neatkarība" ir jāinterpretē, pamatojoties uz šā noteikuma faktisko formulējumu un uz ES datu aizsardzības tiesību aktu mērķiem un sistēmu.[499] EST uzsvēra, ka uzraudzības iestādes ir ar personas datu apstrādi saistīto tiesību "garanti". Tādējādi to izveide dalībvalstīs ir "būtiska sastāvdaļa personu aizsardzībā attiecībā uz personas datu apstrādi".[500] EST secināja, ka "uzraudzības iestādēm savu pienākumu izpildē ir jārīkojas objektīvi un neatkarīgi. Šajā nolūkā tām ir jābūt pasargātām no jebkādas ārējās ietekmes, tostarp tiešas vai netiešas publisko iestāžu ietekmes"[501].

EST arī uzskatīja, ka "pilnīgas neatkarības" nozīme ir jāinterpretē, ņemot vērā EDAU neatkarību, kā tā definēta ES iestāžu datu aizsardzības regulā. Šajā regulā neatkarības jēdziens paredz, ka EDAU nedrīkst nevienam nedz lūgt norādījumus, nedz arī tos pieņemt.

Attiecīgi EST uzskatīja, ka uzraudzības iestādes Vācijā sakarā ar publisko iestāžu pārraudzību nebija pilnīgi neatkarīgas ES datu aizsardzības tiesību izpratnē.

Piemērs. Lietā *Eiropas Komisija pret Austrijas Republiku*[502] EST uzsvēra līdzīgas problēmas saistībā ar noteiktu Austrijas datu aizsardzības iestādes (Datu aizsardzības komisija, DAK) locekļu un darbinieku neatkarību. EST secināja, ka fakts, ka Federālā kanceleja nodrošināja uzraudzības iestādei darbaspēku, apdraud ES datu aizsardzības tiesību aktos noteikto neatkarības prasību. EST arī uzskatīja, ka prasība jebkurā brīdī informēt kanceleju par savu darbu negatīvi ietekmē uzraudzības iestādes neatkarību.

Piemērs. Lietā *Eiropas Komisija pret Ungāriju*[503] tika aizliegta līdzīga valsts prakse, kas ietekmē darbaspēka neatkarību. EST norādīja, ka "prasība (..) ir jānodrošina, lai katra uzraudzības iestāde tām uzticēto pienākumu izpildē

499 Turpat, 17. un 29. punkts.

500 Turpat, 23. punkts.

501 Turpat, 25. punkts.

502 EST 2012. gada 16. oktobra spriedums lietā C-614/10 *Eiropas Komisija pret Austrijas Republiku* [GC], 59. un 63. punkts.

503 EST 2014. gada 8. aprīļa spriedums lietā C-288/12 *Eiropas Komisija pret Ungāriju* [GC], 50. un 67. punkts.

darbotos pilnīgi neatkarīgi, nozīmē attiecīgajai dalībvalstij pienākumu ievērot šādas iestādes pilnvaru termiņa ilgumu līdz tās sākotnēji paredzētā pilnvaru termiņa beigām". EST arī nosprieda, ka, "priekšlaicīgi izbeidzot personas datu aizsardzības uzraudzības iestādes pilnvaru termiņu, Ungārija nav izpildījusi pienākumus, kas tai noteikti Direktīvā 95/46/EK (..)".

"Pilnīgas neatkarības" jēdziens un kritēriji tagad ir skaidri noteikti VDAR, kurā ietverti aprakstītajos EST spriedumos iedibinātie principi. Saskaņā ar regulu pilnīga neatkarība, pildot savus uzdevumus un īstenojot pilnvaras, nozīmē, ka[504]:

- ikvienas uzraudzības iestādes locekļiem jābūt brīviem no ārējas tiešas vai netiešas ietekmes, un viņi nedrīkst pieņemt neviena norādījumus;
- ikvienas uzraudzības iestādes locekļiem ir jāatturas no jebkādas darbības, kas nav savienojama ar viņu pienākumiem, lai novērstu interešu konfliktus;
- dalībvalstīm ir jānodrošina ikvienai uzraudzības iestādei nepieciešamie cilvēkresursi, tehniskie un finanšu resursi, kā arī infrastruktūra, lai efektīvi pildītu savus uzdevumus;
- dalībvalstīm ir jānodrošina, ka ikviena uzraudzības iestāde izvēlas savus darbiniekus;
- finanšu kontrole, kas saskaņā ar valsts tiesību aktiem piemērojama ikvienai uzraudzības iestādei, nedrīkst ietekmēt tās neatkarību. Uzraudzības iestādēm jābūt atsevišķiem un publiski pieejamiem gada budžetiem, kas ļauj tām pienācīgi darboties.

Uzraudzības iestāžu neatkarība tiek uzskatīta arī par būtisku prasību saskaņā ar EP tiesību aktiem. Modernizētajā Konvencijā Nr. 108 uzraudzības iestādēm ir noteikts pienākums "rīkoties pilnīgi neatkarīgi un objektīvi, pildot savus uzdevumus un īstenojot pilnvaras", neprasot un nepieņemot neviena norādījumus[505]. Šādā veidā konvencijā atzīts, ka šīs iestādes nevar efektīvi aizsargāt personu tiesības un brīvības, kas saistītas ar datu apstrādi, ja tās savas funkcijas nevar pildīt pilnīgi neatkarīgi. Modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā ir izklāstīti vairāki elementi, kas veicina šādas neatkarības saglabāšanu. Pie šādiem elementiem pieder

504 Vispārīgā datu aizsardzības regula, 52. pants.

505 Modernizētā Konvencija Nr. 108, 15. panta 5. punkts.

uzraudzības iestāžu iespēja pašām pieņemt darbā savus darbiniekus un pieņemt lēmumus bez ārējas iejaukšanās, kā arī faktori, kas saistīti ar to funkciju izpildes ilgumu un apstākļiem, kādos tās var pārtraukt pildīt savas funkcijas[506].

5.2. Kompetence un pilnvaras

Saskaņā ar ES tiesību aktiem VDAR izklāstīta uzraudzības iestāžu kompetence un organizatoriskā struktūra un izvirzīta prasība, ka tām jābūt kompetentām un pilnvarotām pildīt regulā noteiktos uzdevumus.

Uzraudzības iestāde ir galvenā struktūra valsts tiesību aktos, kas nodrošina atbilstību ES tiesību aktiem datu aizsardzības jomā. Uzraudzības iestādēm ir visaptverošs pārraudzības uzdevumu un pilnvaru katalogs, kurā ietilpst proaktīvas un preventīvas uzraudzības darbības. Lai pildītu šos uzdevumus, uzraudzības iestādēm jābūt attiecīgām izmeklēšanas, koriģēšanas un konsultēšanas pilnvarām, kā uzskaitīts VDAR 58. pantā, piemēram[507]:

- konsultēt pārziņus un datu subjektus par visiem datu aizsardzības jautājumiem;
- apstiprināt līguma standartklauzulas, saistošos uzņēmuma noteikumus vai administratīvās vienošanās;
- izmeklēt apstrādes darbības un attiecīgi iejaukties;
- pieprasīt iesniegt visu informāciju, kas attiecas uz pārziņa darbību uzraudzību;
- brīdināt vai izteikt rājienu pārziņiem un izdot rīkojumu sniegt paziņojumus par personas datu aizsardzības pārkāpumiem, kas jānosūta datu subjektiem;
- uzdot labot, bloķēt, dzēst vai iznīcināt datus;
- piemērot pagaidu vai galīgu apstrādes aizliegumu vai administratīvo naudas sodu;
- nodot lietu izskatīšanai tiesā.

506 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums.

507 Vispārīgā datu aizsardzības regula, 57. un 58. pants. Skatīt arī Konvencijas Nr. 108 Papildu protokolu, 1. pants.

Lai pildītu savas funkcijas, uzraudzības iestādei jābūt piekļuvei visiem personas datiem un informācijai, kas nepieciešama izmeklēšanai, kā arī piekļuvei visām telpām, kurās pārzinis glabā būtisko informāciju. EST uzskatīja, ka uzraudzības iestādes pilnvaras ir jāinterpretē plaši, lai nodrošinātu datu subjektiem pilnīgu datu aizsardzības efektivitāti ES.

Piemērs. Lieta *Schrems* EST aplūkoja jautājumu, vai personas datu nosūtīšana uz ASV saskaņā ar pirmo ES un ASV Nolīgumu par drošības zonu notika atbilstoši ES datu aizsardzības tiesību aktiem, ņemot vērā Edvarda Snoudena atklāto. EST argumentācijā tika atzīts, ka valstu uzraudzības iestādes, rīkojoties kā neatkarīgi pārziņu veiktās datu apstrādes uzraudzītāji, var neļaut personas datus nosūtīt trešai valstij, kaut pastāv lēmums par aizsardzības līmeņa pietiekamību, ja ir pamatoti pierādījumi, ka trešā valstī vairs netiek garantēta atbilstoša aizsardzība[508].

Ikviena uzraudzības iestāde ir kompetenta īstenot izmeklēšanas un iejaukšanās pilnvaras savā teritorijā. Tomēr, tā kā pārziņu un apstrādātāju darbības bieži ir pārrobežu un datu apstrāde ietekmē datu subjektus, kuri atrodas vairākās dalībvalstīs, rodas jautājums par kompetences sadalījumu starp dažādām uzraudzības iestādēm. EST bija iespēja aplūkot šo jautājumu *Weltimmo* lietā.

Piemērs. Lietā *Weltimmo*[509] EST aplūkoja valstu uzraudzības iestāžu kompetenci izskatīt jautājumus, kas saistīti ar organizācijām, kuras nav reģistrētas to jurisdikcijā. *Weltimmo* bija Slovākijā reģistrēts uzņēmums, kas pārvaldīja Ungārijas nekustamo īpašumu tirdzniecības tīmekļa vietni. Reklāmdevēji iesniedza sūdzību Ungārijas datu aizsardzības uzraudzības iestādē par Ungārijas datu aizsardzības likuma pārkāpumiem, un iestāde piemēroja naudas sodu uzņēmumam *Weltimmo*. Uzņēmums apstrīdēja naudas sodu valstu tiesās, un lieta tika nodota EST, lai noskaidrotu, vai ES Datu aizsardzības direktīva ļauj dalībvalsts uzraudzības iestādēm piemērot tās valsts datu aizsardzības tiesību aktus uzņēmumam, kas reģistrēts citā dalībvalstī.

508 EST 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems pret Datu aizsardzības komisāru* [GC], 26.–36. un 40.–41. punkts.

509 EST 2015. gada 1. oktobra spriedums lietā C-230/14 *Weltimmo s.r. o. pret Nemzeti Adatvédelmi és Információszabadság Hatóság*.

EST interpretēja Datu aizsardzības direktīvas 4. panta 1. punkta a) apakšpunktu tādējādi, ka tas ļauj piemērot datu aizsardzības tiesību aktus dalībvalstī, kas nav pārziņa reģistrācijas dalībvalsts, "ciktāl tas, izmantojot stabilu veidojumu šīs dalībvalsts teritorijā, veic reālu un efektīvu darbību – pat ja tā ir minimāla –, kuras ietvaros notiek šī apstrāde". EST norādīja, ka, pamatojoties uz tai iesniegto informāciju, *Weltimmo* veica reālu un efektīvu darbību Ungārijā, jo uzņēmumam bija pārstāvis Ungārijā, kurš Slovākijas uzņēmumu reģistrā bija iekļauts ar adresi Ungārijā, kā arī bankas konts un pastkastīte Ungārijā, kā arī tas veica darbības Ungārijā, ungāru valodā. Šī informācija liecināja par nodibinājuma esamību, un tādā gadījumā uz *Weltimmo* darbību attiecas Ungārijas datu aizsardzības tiesību akti un Ungārijas uzraudzības iestādes jurisdikcija. Tomēr EST atstāja valsts tiesas ziņā pārbaudīt informāciju un lemt, vai faktiski *Weltimmo* bija nodibinājums Ungārijā.

Ja iesniedzējtiesa konstatētu, ka *Weltimmo* ir nodibinājums Ungārijā, Ungārijas uzraudzības iestādei būtu tiesības piemērot naudas sodu. Tomēr, ja valsts tiesa nolemtu pretēji, t. i., ka *Weltimmo* nebija nodibinājuma Ungārijā, piemērojami attiecīgi būtu tās dalībvalsts(-u) likumi, kurā uzņēmums reģistrēts. Šajā gadījumā, tā kā uzraudzības iestāžu pilnvaras ir jāīsteno saskaņā ar citu dalībvalstu teritoriālo suverenitāti, Ungārijas iestāde nevarētu piemērot sodus. Tā kā Datu aizsardzības direktīvā paredzēts uzraudzības iestāžu sadarbības pienākums, Ungārijas iestāde tomēr varētu lūgt savu Slovākijas kolēģi izskatīt lietu, konstatēt Slovākijas tiesību aktu pārkāpumu un piemērot sankcijas, kas paredzētas Slovākijas tiesību aktos.

Pieņemot VDAR, tagad ir sīki izstrādāti noteikumi par uzraudzības iestāžu kompetenci pārrobežu gadījumos. Ar šo regulu izveidots "vienas pieturas aģentūras" mehānisms, un tajā iekļauti noteikumi, kas nosaka sadarbību starp dažādām uzraudzības iestādēm. Lai efektīvi sadarbotos pārrobežu gadījumos, VDAR pieprasa noteikt vadošo uzraudzības iestādi kā pārziņa vai apstrādātāja galvenās vai vienīgās uzņēmējdarbības vietas uzraudzības iestādi[510]. Vadošā uzraudzības iestāde ir atbildīga par pārrobežu lietām, ir pārziņa vai apstrādātāja vienīgais partneris un koordinē sadarbību ar citām uzraudzības iestādēm, lai panāktu vienprātību. Sadarbība ietver informācijas apmaiņu, savstarpēju palīdzību uzraudzībā, izmeklēšanā un saistošu lēmumu pieņemšanā[511].

510 Vispārīgā datu aizsardzības regula, 56. panta 1. punkts.

511 Turpat, 60. pants.

EP tiesību aktos uzraudzības iestāžu kompetence un pilnvaras ir paredzētas modernizētās Konvencijas Nr. 108 15. pantā. Šīs pilnvaras atbilst tām pilnvarām, kas uzraudzības iestādēm piešķirtas saskaņā ar ES tiesību aktiem, tostarp izmeklēšanas un korektīvās pilnvaras, pilnvaras izdot lēmumus un piemērot administratīvas sankcijas par konvencijas noteikumu pārkāpumiem un pilnvaras iesaistīties tiesvedībā. Neatkarīgo uzraudzības iestāžu kompetencē ir arī datu subjektu iesniegto pieprasījumu un sūdzību izskatīšana, sabiedrības informētības par datu aizsardzības tiesību aktiem veicināšana un valstu lēmumu pieņēmēju konsultēšana par visiem likumdošanas vai administratīvajiem pasākumiem, ar ko nodrošina personas datu apstrādi.

5.3. Sadarbība

Ar VDAR tiek izveidota vispārēja uzraudzības iestāžu sadarbības sistēma un tiek paredzēti konkrētāki noteikumi par uzraudzības iestāžu sadarbību pārrobežu datu apstrādes darbībās.

Saskaņā ar VDAR uzraudzības iestādes sniedz savstarpēju palīdzību un apmainās ar būtisko informāciju nolūkā konsekventi īstenot un piemērot regulu[512]. Šī sadarbība ietver sevī to, ka pieprasījuma saņēmēja uzraudzības iestāde konsultē, veic pārbaudes un izmeklēšanu. Uzraudzības iestādes var veikt kopīgas operācijas, tostarp kopīgu izmeklēšanu un kopīgus piespiedu izpildes pasākumus, iesaistot visu uzraudzības iestāžu darbiniekus[513].

ES iekšienē pārziņi un apstrādātāji arvien vairāk darbojas starpvalstu mērogā. Tam nepieciešama cieša sadarbība starp kompetentajām uzraudzības iestādēm dalībvalstīs, lai nodrošinātu personas datu apstrādes atbilstību VDAR prasībām. Saskaņā ar regulas "vienas pieturas aģentūras" mehānismu, ja pārzinim vai apstrādātājam ir uzņēmējdarbības vietas vairākās dalībvalstīs vai ja tam ir viena uzņēmējdarbības vieta, bet apstrādes darbības būtiski ietekmē datu subjektus vairāk nekā vienā dalībvalstī, galvenā (vai vienīgā) uzņēmējdarbības vietas uzraudzības iestāde ir vadošā iestāde attiecībā uz pārziņa vai apstrādātāja pārrobežu darbībām. Vadošajām iestādēm ir tiesības veikt izpildes pasākumus pret pārzini vai apstrādātāju. Vienas pieturas aģentūras mehānisma mērķis ir uzlabot ES datu aizsardzības tiesību aktu saskaņošanu un vienādu piemērošanu dažādās dalībvalstīs. Tas ir izdevīgi arī uzņēmumiem, jo tiem ir jāsadarbojas tikai ar vadošo iestādi, nevis ar vairākām uzraudzības iestādēm. Tas palielina juridisko noteiktību uzņēmumiem, un praksē

512 Turpat, 61. panta 1.–3. punkts un 62. panta 1. punkts.

513 Turpat, 62. panta 1. punkts.

tam vajadzētu arī nozīmēt, ka lēmumi tiek pieņemti ātrāk un ka uzņēmumiem nav jāsaskaras ar dažādām uzraudzības iestādēm, kuras tām uzliek pretrunīgas prasības.

Vadošās iestādes identificēšana nozīmē uzņēmuma galvenās uzņēmējdarbības vietas atrašanās vietas noteikšanu ES. Termins "galvenā uzņēmējdarbības vieta" ir definēts VDAR. Turklāt 29. panta darba grupa ir izdevusi pamatnostādnes pārziņa vai apstrādātāja vadošās uzraudzības iestādes noteikšanai, ietverot galvenās uzņēmējdarbības vietas noteikšanas kritērijus.[514]

Lai nodrošinātu augstu datu aizsardzības līmeni visā ES, vadošā uzraudzības iestāde nerīkojas viena pati. Tai ir jāsadarbojas ar citām iesaistītajām uzraudzības iestādēm, pieņemot lēmumus par personas datu apstrādi, ko veic pārziņi un apstrādātāji, lai panāktu vienprātību un nodrošinātu konsekvenci. Iesaistīto uzraudzības iestāžu sadarbība ietver informācijas apmaiņu, savstarpēju palīdzību, kopīgu izmeklēšanas veikšanu un uzraudzības pasākumus[515]. Sniedzot savstarpēju palīdzību, uzraudzības iestādēm precīzi jāizskata informācijas pieprasījumi, ko iesniegušas citas uzraudzības iestādes, un jāveic uzraudzības pasākumi, piemēram, iepriekšēju atļauju sniegšana un apspriešanās ar datu pārzini par tā apstrādes darbībām, pārbaudes vai izmeklēšana. Savstarpēja palīdzība citu dalībvalstu uzraudzības iestādēm jāsniedz pēc pieprasījuma bez nepamatotas kavēšanās un ne vēlāk kā mēnesi pēc pieprasījuma saņemšanas[516].

Ja pārzinim ir uzņēmējdarbības vietas vairākās dalībvalstīs, uzraudzības iestādes var veikt kopīgas operācijas, tostarp izmeklēšanu un piespiedu izpildes pasākumus, kuros ir iesaistīti citu dalībvalstu uzraudzības iestāžu darbinieki[517].

Sadarbība starp dažādām uzraudzības iestādēm ir svarīga prasība arī EP tiesību aktos. Modernizētajā Konvencijā Nr. 108 paredzēts, ka uzraudzības iestādēm jāsadarbojas savā starpā tiktāl, ciktāl tas nepieciešams to uzdevumu izpildei[518]. Tas ir jādara, piemēram, sniedzot savstarpēji visu būtisko un noderīgo informāciju, kā arī koordinējot izmeklēšanu un veicot kopīgas darbības[519].

514 29. panta darba grupa (2016), *Pamatnostādnes pārziņa vai apstrādātāja vadošās uzraudzības iestādes noteikšanai*, WP 244, Brisele, 2016. gada 13. decembris, pārskatītas 2017. gada 5. aprīlī.

515 Vispārīgā datu aizsardzības regula, 60. panta 1.–3. punkts.

516 Turpat, 61. panta 1. un 2. punkts.

517 Turpat, 62. panta 1. punkts.

518 Modernizētā Konvencija Nr. 108, 16. un 17. pants.

519 Turpat, 17. pants.

5.4. Eiropas Datu aizsardzības kolēģija

Neatkarīgu uzraudzības iestāžu nozīme un galvenās kompetences, kas tām piešķirtas saskaņā ar Eiropas tiesību aktiem datu aizsardzības jomā, ir iepriekš aprakstītas šajā nodaļā. Eiropas Datu aizsardzības kolēģija (EDAK) ir vēl viens svarīgs dalībnieks, kas nodrošina datu aizsardzības noteikumu efektīvu un konsekventu piemērošanu visā ES.

VDAR izveidoja EDAK kā ES struktūru ar juridiskas personas statusu[520]. Tā ir pēctece 29. panta darba grupai[521], ko izveidoja ar Datu aizsardzības direktīvu, lai konsultētu Komisiju par jebkādiem ES pasākumiem, kas ietekmē indivīdu tiesības attiecībā uz personas datu apstrādi un privātumu, lai veicinātu direktīvas vienādu piemērošanu un sniegtu ekspertu atzinumus Komisijai par jautājumiem, kas saistīti ar datu aizsardzību. 29. panta darba grupas sastāvā bija ES dalībvalstu uzraudzības iestāžu pārstāvji, kā arī pārstāvji no Komisijas un EDAU.

Līdzīgi kā darba grupā arī EDAK ir katras dalībvalsts uzraudzības iestāžu vadītāji un EDAU vai viņu pārstāvji[522]. EDAU ir vienādas balsstiesības, izņemot gadījumus, kas saistīti ar strīdu izšķiršanu, kad tas var balsot tikai par lēmumiem attiecībā uz principiem un noteikumiem, kuri piemērojami ES iestādēm un kuri pēc būtības atbilst VDAR. Eiropas Komisijai ir tiesības piedalīties EDAK darbībā un sanāksmēs bez balsošanas tiesībām[523]. Kolēģija no savu locekļu vidus uz piecu gadu termiņu ievēl priekšsēdētāju (kuram uzticēta tās pārstāvība) un divus priekšsēdētāja vietniekus. Turklāt EDAK ir arī sekretariāts, ko nodrošina EDAU, lai kolēģijai būtu analītiskais, administratīvais un loģistikas atbalsts[524].

EDAK uzdevumi ir detalizēti aprakstīti VDAR 64., 65. un 70. pantā, un tajos ietilpst visaptveroši pienākumi, ko var sadalīt trīs galvenajās darbībās:

- **Konsekvence:** EDAK var izdot juridiski saistošus lēmumus trīs gadījumos: kad uzraudzības iestāde vienas pieturas aģentūras lietās ir izteikusi būtisku un

520 Vispārīgā datu aizsardzības regula, 68. pants

521 Saskaņā ar Direktīvu 95/46/EK 29. panta darba grupai bija jākonsultē Komisija par jebkādiem ES pasākumiem, kas ietekmē indivīdu tiesības attiecībā uz personas datu apstrādi un privātumu, jāveicina direktīvas vienāda piemērošana un jāsniedz ekspertu atzinumi Komisijai par jautājumiem, kas saistīti ar datu aizsardzību. 29. panta darba grupas sastāvā bija ES dalībvalstu uzraudzības iestāžu pārstāvji, kā arī pārstāvji no Komisijas un EDAU.

522 Vispārīgā datu aizsardzības regula, 68. panta 3. punkts.

523 Turpat, 68. panta 4. un 5. punkts.

524 Turpat, 73. un 75. pants.

motivētu iebildumu; ja ir pretrunīgi viedokļi attiecībā uz to, kura no uzraudzības iestādēm ir vadošā; un, visbeidzot, ja kompetentā uzraudzības iestāde nelūdz vai neievēro EDAK atzinumu[525]. EDAK galvenā atbildība ir nodrošināt VDAR konsekventu piemērošanu visā ES, un tai ir būtiska nozīme konsekvences mehānismā, kā aprakstīts 5.5. iedaļā.

- **Konsultācijas:** EDAK uzdevumos ietilpst konsultēt Komisiju par jebkādiem jautājumiem, kas saistīti ar personas datu aizsardzību Savienībā, piemēram, par VDAR grozījumiem, to ES tiesību aktu pārskatīšanu, kas saistīti ar datu apstrādi un kas varētu būt pretrunā ES datu aizsardzības noteikumiem, vai Komisijas lēmumu par aizsardzības līmeņa pietiekamību izdošanu, kas atļauj personas datu nosūtīšanu trešai valstij vai starptautiskai organizācijai.

- **Norādījumu sniegšana:** Kolēģija arī izdod pamatnostādnes, ieteikumus un paraugpraksi, lai veicinātu regulas konsekventu piemērošanu, kā arī veicina sadarbību un zināšanu apmaiņu starp uzraudzības iestādēm. Turklāt tai ir jāmudina pārziņu vai apstrādātāju apvienības izstrādāt rīcības kodeksus, kā arī izveidot datu aizsardzības sertifikācijas mehānismus un zīmogus.

EDAK lēmumus var pārsūdzēt EST.

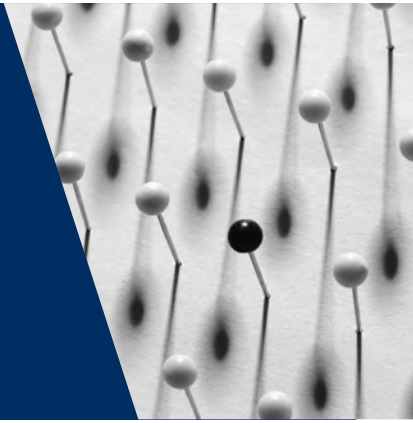
5.5. VDAR konsekvences mehānisms

Lai nodrošinātu regulas konsekventu piemērošanu visās dalībvalstīs, ar VDAR tiek izveidots konsekvences mehānisms, saskaņā ar kuru uzraudzības iestādes sadarbojas savā starpā un attiecīgā gadījumā ar Komisiju. Konsekvences mehānisms tiek izmantots divās situācijās. Pirmais attiecas uz EDAK atzinumiem gadījumos, kad kompetentā uzraudzības iestāde plāno īstenot pasākumus, piemēram, izveidot apstrādes darbību sarakstu, kam nepieciešams novērtējums par ietekmi uz datu aizsardzību (NIDA), vai noteikt līguma standartklauzulas. Otrais attiecas uz EDAK saistošajiem lēmumiem uzraudzības iestādēm vienas pieturas aģentūras gadījumos un gadījumos, kad uzraudzības iestāde neievēro vai neprasa EDAK atzinumu.

525 Turpat, 65. pants.

6

Datu subjektu tiesības un to īstenošana



ES	Aptvertie jautājumi	EP
Tiesības tikt informētam		
Vispārīgā datu aizsardzības regula, 12. pants EST lieta C-473/12 *Institut professionnel des agents immobiliers (IPI) pret Englebert*, 2013 EST lieta C-201/14 *Smaranda Bara un citi pret Casa Națională de Asigurări de Sănătate un citiem*, 2015	**Informācijas pārredzamība**	Modernizētā Konvencija Nr. 108, 8. pants
Vispārīgā datu aizsardzības regula, 13. panta 1. un 2. punkts un 14. panta 1. un 2. punkts	**Informācijas saturs**	Modernizētā Konvencija Nr. 108, 8. panta 1. punkts
Vispārīgā datu aizsardzības regula, 13. panta 1. punkts un 14. panta 3. punkts	**Informācijas sniegšanas laiks**	Modernizētā Konvencija Nr. 108, 9. panta 1. punkta b) apakšpunkts.
Vispārīgā datu aizsardzības regula, 12. panta 1., 5. un 7. punkts	**Informācijas sniegšanas līdzekļi**	Modernizētā Konvencija Nr. 108, 9. panta 1. punkta b) apakšpunkts.
Vispārīgā datu aizsardzības regula, 13. panta 2. punkta d) apakšpunkts un 14. panta 2. punkta e) apakšpunkts, 77., 78. un 79. pants	**Tiesības iesniegt sūdzību**	Modernizētā Konvencija Nr. 108, 9. panta 1. punkta f) apakšpunkts

ES	Aptvertie jautājumi	EP
Tiesības uz piekļuvi		
Vispārīgā datu aizsardzības regula, 15. panta 1. punkts EST lieta C-553/07 *College van burgemeester en wethouders van Rotterdam pret M. E. E. Rijkeboer*, 2009 EST apvienotās lietas C-141/12 un C-372/12 *YS pret Minister voor Immigratie, Integratie en Asiel* un *Minister voor Immigratie, Integratie en Asiel pret M un S*, 2014 EST lieta C-434/16 *Peter Nowak pret Datu aizsardzības komisāru*, 2017	**Tiesības piekļūt saviem datiem**	Modernizētā Konvencija Nr. 108, 9. panta 1. punkta b) apakšpunkts ECT lieta *Leander pret Zviedriju*, Nr. 9248/81, 1987
Tiesības labot datus		
Vispārīgā datu aizsardzības regula, 16. pants	**Neprecīzu personas datu labošana**	Modernizētā Konvencija Nr. 108, 9. panta 1. punkta e) apakšpunkts ECT lieta *Cemalettin Canli pret Turciju*, Nr. 22427/04, 2008 ECT lieta *Ciubotaru pret Moldovu*, Nr. 27138/04, 2010
Tiesības uz dzēšanu		
Vispārīgā datu aizsardzības regula, 17. panta 1. punkts	**Personas datu dzēšana**	Modernizētā Konvencija Nr. 108, 9. panta 1. punkta e) apakšpunkts ECT lieta *Segerstedt-Wiberg un citi pret Zviedriju*, Nr. 62332/00, 2006
EST lieta C-131/12 *Google Spain SL, Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 EST lieta C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce pret Salvatore Manni*, 2017	**Tiesības tikt aizmirstam**	
Tiesības uz apstrādes ierobežošanu		
Vispārīgā datu aizsardzības regula, 18. panta 1. punkts	**Tiesības ierobežot personas datu izmantošanu**	
Vispārīgā datu aizsardzības regula, 19. pants	**Paziņošanas pienākums**	

ES	Aptvertie jautājumi	EP
Tiesības uz datu pārnesamību		
Vispārīgā datu aizsardzības regula, 20. pants	**Tiesības uz datu pārnesamību**	
Tiesības iebilst		
Vispārīgā datu aizsardzības regula, 21. panta 1. punkts EST lieta C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce pret Salvatore Manni*, 2017	**Tiesības iebilst, pamatojoties uz datu subjekta īpašo situāciju**	Ieteikums par profilēšanu, 5.3. punkts Modernizētā Konvencija Nr. 108, 9. panta 1. punkta d) apakšpunkts
Vispārīgā datu aizsardzības regula, 21. panta 2. punkts	**Tiesības iebilst pret datu izmantošanu tirgvedības nolūkos**	Ieteikums par tiešo tirgvedību, 4.1. punkts
Vispārīgā datu aizsardzības regula, 21. panta 5. punkts	**Tiesības iebilst, izmantojot automatizētus līdzekļus**	
Ar automatizētu lēmumu pieņemšanu un profilēšanu saistītās tiesības		
Vispārīgā datu aizsardzības regula, 22. pants	**Ar automatizētu lēmumu pieņemšanu un profilēšanu saistītās tiesības**	Modernizētā Konvencija Nr. 108, 9. panta 1. punkta a) apakšpunkts
Vispārīgā datu aizsardzības regula, 21. pants	**Tiesības iebilst pret automatizētu lēmumu pieņemšanu**	
Vispārīgā datu aizsardzības regula, 13. panta 2. punkta f) apakšpunkts	**Tiesības saņemt jēgpilnu skaidrojumu**	Modernizētā Konvencija Nr. 108, 9. panta 1. punkta c) apakšpunkts
Tiesiskās aizsardzības līdzekļi, atbildība, sankcijas un kompensācija		
Harta, 47. pants EST lieta C-362/14 *Maximillian Schrems pret Datu aizsardzības komisāru* [GC], 2015. Vispārīgā datu aizsardzības regula, 77.–84. pants	**Par valsts datu aizsardzības tiesību aktu pārkāpumiem**	ECTK, 13. pants (tikai EP dalībvalstīm) Modernizētā Konvencija Nr. 108, 9. panta 1. punkta f) apakšpunkts, 12., 15., 16.–21. pants ECT lieta *K.U. pret Somiju*, Nr. 2872/02, 2008 ECT lieta *Biriuk pret Lietuvu*, Nr. 23373/03, 2008
ES iestāžu datu aizsardzības regula, 34. un 49. pants EST lieta C-28/08 P *Eiropas Komisija pret The Bavarian Lager Co. Ltd* [GC], 2010	**Par ES tiesību aktu pārkāpumiem, ko izdara ES iestādes un struktūras**	

Tiesisko normu efektivitāte kopumā un jo īpaši datu subjektu tiesības lielā mērā ir atkarīgi no tā, vai pastāv attiecīgi mehānismi to izpildei. Digitālajā laikmetā datu apstrāde ir kļuvusi visuresoša un indivīdiem arvien grūtāk saprotama. Lai mazinātu varas nelīdzsvarotību starp datu subjektiem un pārziņiem, indivīdiem ir dotas noteiktas tiesības kontrolēt personiskās informācijas apstrādi. Tiesības piekļūt saviem datiem un tiesības tos labot ir noteiktas ES Pamattiesību hartas 8. panta 2. punktā – dokumentā, kas ietilpst ES primārajos tiesību aktos un kam ir fundamentāla vērtība ES tiesību sistēmā. ES sekundārie tiesību akti, jo īpaši Vispārīgā datu aizsardzības regula, ir izveidojuši saskaņotu tiesisko regulējumu, kas sniedz datu subjektiem tiesības attiecībā uz datu pārziņiem. Papildus piekļuves un labošanas tiesībām VDAR atzīst virkni citu tiesību, piemēram, tiesības dzēst ("tiesības tikt aizmirstam"), tiesības iebilst vai ierobežot datu apstrādi un tiesības, kas saistītas ar automatizētu lēmumu pieņemšanu un profilēšanu. Līdzīgi aizsardzības pasākumi, kas paredzēti, lai datu subjekti varētu efektīvi kontrolēt savus datus, ir iekļauti arī modernizētajā Konvencijā Nr. 108. Tiesības, ko indivīdiem vajadzētu būt iespējai īstenot saistībā ar viņu personas datiem, ir norādītas 9. pantā. Līgumslēdzējām pusēm jānodrošina, ka šīs tiesības ir pieejamas ikvienam datu subjektam viņa jurisdikcijā, un tās papildina efektīvi juridiski un praktiski līdzekļi, kas ļauj datu subjektiem šīs tiesības īstenot.

Papildus indivīdu tiesību nodrošināšanai ir vienlīdz svarīgi izveidot mehānismus, kas datu subjektiem ļauj celt pretenzijas par viņu tiesību pārkāpumiem, saukt pie atbildības pārziņus un pieprasīt kompensāciju. Ar tiesībām uz efektīvu tiesību aizsardzību, kas garantētas ECTK un Hartā, paredz, ka ikvienam ir pieejami tiesiskās aizsardzības līdzekļi.

6.1. Datu subjektu tiesības

Svarīgākie aspekti

- Ikvienam datu subjektam ir tiesības saņemt informāciju par jebkuru personas datu apstrādātāja veiktu viņa personas datu apstrādi, ievērojot atsevišķus izņēmumus.
- Datu subjektiem ir tiesības:
  - piekļūt saviem datiem un iegūt noteiktu informāciju par apstrādi;
  - lūgt pārzinim, kurš veic viņu datu apstrādi, labot datus, ja tie ir neprecīzi;
  - lūgt pārzinim attiecīgi dzēst viņu datus, ja pārzinis apstrādā viņu datus nelikumīgi;
  - uz laiku ierobežot apstrādi;
  - noteiktos apstākļos panākt viņu datu pārsūtīšanu citam pārzinim.

- Turklāt datu subjektiem ir tiesības iebilst pret apstrādi šādos gadījumos:
  - tādu iemeslu dēļ, kas saistīti ar viņu īpašo situāciju;
  - viņu datu izmantošana tiešās tirgvedības nolūkos.
- Datu subjektiem ir tiesības netikt pakļautiem lēmumiem, kuru pamatā ir tikai automatizēta apstrāde, tostarp profilēšana, kam ir juridiskas sekas vai kas viņus būtiski ietekmē. Datu subjektiem ir arī tiesības:
  - panākt cilvēka līdzdalību no pārziņa puses;
  - izteikt savu viedokli un apstrīdēt lēmumu, kura pamatā ir automatizēta apstrāde.

6.1.1. Tiesības tikt informētam

Atbilstoši **EP tiesību aktiem** un **ES tiesību aktiem** apstrādes darbību pārziņiem ir pienākums informēt datu subjektu personas datu vākšanas laikā par paredzēto apstrādi. Šis pienākums nav atkarīgs no datu subjekta pieprasījuma, drīzāk pārzinim ir proaktīvi jāpilda pienākums neatkarīgi no tā, vai datu subjekts izrāda interesi par šo informāciju vai nē.

EP tiesiskajā regulējumā saskaņā ar modernizētās Konvencijas Nr. 108 8. pantu līgumslēdzējām pusēm jāparedz, ka pārziņi informē datu subjektus par savu identitāti un pastāvīgo dzīvesvietu, apstrādes juridisko pamatu un nolūku, apstrādāto personas datu kategorijām, personas datu saņēmējiem (ja tādi ir) un to, kā datu subjekti var īstenot savas tiesības saskaņā ar 9. pantu, kas ietver tiesības piekļūt, labot un saņemt tiesisko aizsardzību. Datu subjektiem ir jāsniedz arī jebkura cita papildu informācija, kas uzskatāma par nepieciešamu, lai nodrošinātu godīgu un pārredzamu personas datu apstrādi. Modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā ir precizēts, ka datu subjektiem sniegtajai informācijai "vajadzētu būt viegli pieejamai, salasāmai, saprotamai un pielāgotai attiecīgajiem datu subjektiem"[526].

ES tiesību aktos saskaņā ar pārredzamības principu jebkādai personas datu apstrādei kopumā jābūt personām pārredzamai. Indivīdiem ir tiesības zināt, kā un kādi personas dati tiek vākti, izmantoti vai kā citādi apstrādāti, kā arī būt informētiem par riskiem, aizsardzības pasākumiem un viņu tiesībām attiecībā uz apstrādi[527]. Tādējādi VDAR 12. pantā pārziņiem noteikts plašs un visaptverošs pienākums sniegt pārredzamu informāciju un/vai paziņot, kā datu subjekti var īstenot savas tiesības[528].

526 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 68. punkts.

527 Vispārīgā datu aizsardzības regula, 39. apsvērums.

528 Turpat, 13. un 14. pants, modernizētā Konvencija Nr. 108, 8. panta 1. punkta b) apakšpunkts.

Informācijai jābūt kodolīgai, pārredzamai, saprotamai un viegli pieejamai, izmantojot skaidru un vienkāršu valodu. Tā ir jāsniedz rakstiski, vajadzības gadījumā arī elektroniski, un to var sniegt pat mutiski pēc datu subjekta pieprasījuma un gadījumā, kad viņa vai viņas identitāte ir neapšaubāmi pierādīta. Informācija jāsniedz bez pārmērīgas kavēšanās un bez maksas[529].

VDAR 13. un 14. pants attiecas uz datu subjektu tiesībām būt informētiem attiecīgi gan situācijās, kad personas dati ir vākti tieši no viņiem, gan arī situācijās, kad dati nav iegūti no viņiem.

Tiesību uz informāciju tvērums un to ierobežojumi saskaņā ar ES tiesību aktiem ir precizēti EST judikatūrā.

Piemērs. Lietā *Institut professionnel des agents immobiliers (IPI) pret Englebert*[530] EST tika lūgta interpretēt Direktīvas 95/46/EK 13. panta 1. punktu. Šis pants dalībvalstīm ļāva izvēlēties, vai pieņemt likumdošanas pasākumus, ierobežojot datu subjekta tiesības tikt informētam, ja tas ir nepieciešams, lai cita starpā aizsargātu citu personu tiesības un brīvības, novērstu un izmeklētu noziegumus vai ētikas pārkāpumus reglamentētajās profesijās. IPI ir profesionāla nekustamo īpašumu aģentu organizācija Beļģijā, kas ir atbildīga par nekustamā īpašuma aģenta profesijas pareizu praksi. Tā lūdza valsts tiesu atzīt, ka atbildētāji ir pārkāpuši profesionālos noteikumus, un likt viņiem pārtraukt dažādas nekustamā īpašuma aģentūras darbības. Darbības pamatā bija IPI izmantotu privāto detektīvu sniegtie pierādījumi.

Valsts tiesai bija šaubas par detektīvu pierādījumu vērtību, ņemot vērā iespēju, ka tie bija iegūti, neievērojot Beļģijas tiesību aktu datu aizsardzības prasības, jo īpaši pienākumu informēt datu subjektus par viņu personas datu apstrādi pirms šādas informācijas vākšanas. EST atzīmēja, ka 13. panta 1. punktā noteikts, ka dalībvalstis "var", bet tām nav pienākuma, savos tiesību aktos paredzēt izņēmumus no pienākuma informēt datu subjektus par viņu datu apstrādi. Tā kā 13. panta 1. punkts ietver noziedzīgu nodarījumu vai ētikas pārkāpumu novēršanu, izmeklēšanu, atklāšanu un saukšanu pie atbildības par tiem, pamatojoties uz ko dalībvalstis var ierobežot indivīdu

529 Vispārīgā datu aizsardzības regula, 12. panta 5. punkts; modernizētā Konvencija Nr. 108, 9. panta 1. punkta b) apakšpunkts.

530 EST 2013. gada 7. novembra spriedums lietā C-473/12 *Institut professionnel des agents immobiliers (IPI) pret Englebert un citiem*.

tiesības, līdz ar to tādas organizācijas kā *IPI* un privātie detektīvi, kas darbojas tās vārdā, var atsaukties uz šo noteikumu. Tomēr, ja dalībvalsts nav paredzējusi šādu izņēmumu, datu subjekta informēšanas pienākums ir spēkā.

Piemērs. Lietā *Smaranda Bara un citi pret Casa Națională de Asigurări de Sănătate un citiem*[531] EST precizēja, vai ES tiesību akti liedz valsts pārvaldes iestādei nosūtīt personas datus citai valsts pārvaldes iestādei tālākai apstrādei, datu subjektus neinformējot par šo nosūtīšanu un apstrādi. Šajā lietā nacionālā Nodokļu administrācijas aģentūra nebija pirms nosūtīšanas informējusi prasītājus, ka ir nosūtījuši viņu datus Valsts veselības apdrošināšanas fondam.

EST uzskatīja, ka ES tiesību aktos noteiktā prasība informēt datu subjektu par viņu personas datu apstrādi ir "jo svarīgāka tāpēc, ka tā ir priekšnosacījums ieinteresēto personu tiesību uz piekļuvi apstrādātajiem datiem un tiesībām to labot, (..) un viņu tiesību iebilst pret datu apstrādi īstenošanai (..)". Godprātīgas apstrādes princips pieprasa informēt datu subjektu par viņa datu nosūtīšanu citai publiskai iestādei turpmākai apstrādei. Atbilstoši Direktīvas 95/46/EK 13. panta 1. punktam dalībvalstis var ierobežot tiesības saņemt informāciju, ja tas tiek uzskatīts par nepieciešamu, aizsargājot svarīgas valsts ekonomiskās intereses, tostarp nodokļu jautājumus. Tomēr šādi ierobežojumi ir jānosaka ar likumdošanas pasākumiem. Tā kā ne nosūtāmo datu definīcija, ne detalizēti nosūtīšanas noteikumi nebija noteikti likumdošanas pasākumā, bet gan tikai protokolā starp abām publiskām iestādēm, atkāpei piemērojamie nosacījumi saskaņā ar ES tiesību aktiem nebija izpildīti. Prasītājiem vajadzēja būt iepriekš informētiem par viņu datu nosūtīšanu Valsts veselības apdrošināšanas fondam un par to, kā iestāde vēlāk apstrādās šos datus.

Informācijas saturs

Saskaņā ar modernizētās Konvencijas Nr. 108 8. panta 1. punktu pārzinim ir pienākums sniegt datu subjektam visu informāciju, kas nodrošina godprātīgu un pārredzamu personas datu apstrādi, tostarp:

- pārziņa identitāte un pastāvīgā dzīvesvieta vai uzņēmējdarbības vieta;
- paredzētās apstrādes juridiskais pamats un mērķi;

531 EST 2015. gada 1. oktobra spriedums lietā C-201/14 *Smaranda Bara un citi pret Casa Națională de Asigurări de Sănătate un citiem*.

- apstrādāto personas datu kategorijas;
- personas datu saņēmēji vai saņēmēju kategorijas, ja tādi ir;
- veidi, kā datu subjekti var īstenot savas tiesības.

Saskaņā ar VDAR, ja personas dati tiek vākti no datu subjekta, pārziņa pienākums ir personas datu iegūšanas laikā sniegt datu subjektam šādu informāciju[532]:

- pārziņa identitāte un kontaktinformācija, tostarp informācija par DAS, ja tāds ir;
- apstrādes mērķis un juridiskais pamats, t. i., līgums vai juridisks pienākums;
- datu apstrādātāja leģitīmās intereses, ja tās ir apstrādes pamats;
- personas datu iespējamie saņēmēji vai saņēmēju kategorijas;
- vai dati tiks nosūtīti trešai valstij vai starptautiskai organizācijai un vai tas balstās lēmumā par aizsardzības līmeņa pietiekamību, vai arī atsaucas uz attiecīgiem aizsardzības pasākumiem;
- laikposms, cik ilgi personas dati tiks glabāti, kā arī – ja nav iespējams noteikt šādu laikposmu – kritēriji, kas izmantoti šā datu glabāšanas perioda noteikšanai;
- datu subjektu tiesības attiecībā uz apstrādi, piemēram, tiesības piekļūt, labot, dzēst un ierobežot apstrādi vai iebilst pret to;
- vai personas datu sniegšanu pieprasa likums vai līgums, vai datu subjektam ir pienākums sniegt savus personas datus, kā arī sekas personas datu nesniegšanas gadījumā;
- automatizētas lēmumu pieņemšanas, tostarp profilēšanas, esamība;
- tiesības iesniegt sūdzību uzraudzības iestādei;
- tiesības atsaukt piekrišanu.

532 Vispārīgā datu aizsardzības regula, 13. panta 1. punkts; modernizētā Konvencija Nr. 108, 7.bis panta 1. punkts.

Automatizētas lēmumu pieņemšanas, tostarp profilēšanas, gadījumos datu subjektiem jāsaņem jēgpilna informācija par profilēšanā izmantoto loģiku, tās nozīmīgumu un paredzamajām sekām, ar kurām viņi saskarsies apstrādes rezultātā.

Gadījumos, kad personas dati netiek iegūti tieši no datu subjekta, datu pārzinim ir pienākums informēt indivīdu par personas datu izcelsmi. Jebkurā gadījumā pārzinim cita starpā ir jāinformē datu subjekti par automatizētu lēmumu pieņemšanu, tostarp profilēšanu[533]. Visbeidzot, ja pārzinis plāno apstrādāt personas datus citam mērķim, nekā tas sākotnēji datu subjektam tika norādīts, saskaņā ar nolūka ierobežojuma un pārredzamības principiem pārzinim ir pienākums sniegt datu subjektam informāciju par šo jauno nolūku. Pārziņiem ir pienākums sniegt informāciju pirms jebkādas turpmākas apstrādes. Citiem vārdiem sakot, gadījumos, kad datu subjekts ir devis piekrišanu personas datu apstrādei, pārzinim jāsaņem atjaunota datu subjekta piekrišana, ja mainās datu apstrādes nolūks vai ja tiek pievienoti citi nolūki.

Informācijas sniegšanas laiks

VDAR nošķirti divi scenāriji un divi brīži laikā, kad datu pārzinim jāsniedz informācija datu subjektam:

- Ja personas dati tiek iegūti tieši no datu subjekta, pārzinim datu iegūšanas laikā jāinformē datu subjekts par visu ar viņu saistīto informāciju un tiesībām, kas izriet no VDAR[534].

- Ja pārzinis plāno turpmāk apstrādāt personas datus citam nolūkam, pārzinis pirms apstrādes veikšanas sniedz visu būtisko informāciju.

Ja personas dati nav iegūti tieši no datu subjekta, pārzinim ir pienākums sniegt datu subjektam informāciju par apstrādi "saprātīgā termiņā pēc personas datu iegūšanas, bet vēlākais mēneša laikā" vai pirms datu izpaušanas trešai personai[535].

533 Vispārīgā datu aizsardzības regula, 13. panta 2. punkts un 14. panta 2. punkta f) apakšpunkts.

534 Turpat, 13. panta 1. un 2. punkts, ievadvārdi, kuros Vispārīgā datu aizsardzības regulā ir atsauce uz informāciju par pienākumu piemērot "personas datu iegūšanas laikā".

535 Turpat, 13. panta 3. punkts un 14. panta 3. punkts; skatīt arī atsauci uz saprātīgiem intervāliem un bez pārmērīgas kavēšanās saskaņā ar modernizētās Konvencijas Nr. 108 8. panta 1. punkta b) apakšpunktu.

Modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā noteikts, ka, ja datu apstrādes subjektu informēšana nav iespējama, uzsākot apstrādi, to var izdarīt vēlāk, piemēram, kad pārzinis jebkāda iemesla dēļ sazinās ar datu subjektu[536].

Dažādi informācijas sniegšanas veidi

Gan saskaņā ar EP, gan ES tiesību aktiem informācijai, kas pārzinim jāsniedz datu subjektiem, jābūt kodolīgai, pārredzamai, saprotamai un viegli pieejamai. Tā jāsniedz rakstiski vai ar citiem līdzekļiem, ieskaitot elektroniskos saziņas līdzekļus, skaidrā, vienkāršā un viegli saprotamā valodā. Sniedzot informāciju, pārzinis var izmantot standartizētas ikonas, lai sniegtu informāciju viegli saskatāmā un saprotamā veidā[537]. Piemēram, ikonu, kas attēlo slēdzeni, var izmantot, lai signalizētu, ka dati ir droši vākti un/vai šifrēti. Datu subjekti var pieprasīt sniegt informāciju mutiski. Informācijai jābūt bez maksas, ja vien datu subjekta pieprasījumi nav acīmredzami nepamatoti vai pārmērīgi (t. i., atkārtoti pēc būtības)[538]. Ērta piekļuve sniegtajai informācijai ir ārkārtīgi svarīga datu subjekta spējai īstenot savas ES datu aizsardzības tiesību aktos noteiktās tiesības.

Godprātīgas apstrādes princips paredz, lai informācija būtu datu subjektiem viegli saprotama. Jāizmanto adresātiem piemērota valoda. Izmantotās valodas līmenim un veidam jāatšķiras atkarībā no tā, vai paredzētā auditorija ir, piemēram, pieaugušais vai bērns, plašāka sabiedrība vai akadēmiskais eksperts. Jautājums par to, kā līdzsvarot šo saprotamās informācijas aspektu, ir aplūkots 29. panta darba grupas atzinumā par saskaņotākiem noteikumiem attiecībā uz informāciju. Tajā ir veicināta ideja par tā sauktajiem daudzpakāpju paziņojumiem, ļaujot datu subjektam izlemt, kādai detalizācijas pakāpei viņš vai viņa dod priekšroku[539]. Tomēr šis informācijas sniegšanas veids neatbrīvo pārzini no VDAR 13. un 14. pantā noteiktā pienākuma. Pārzinim joprojām ir jāsniedz datu subjektam visa informācija.

Viens no visefektīvākajiem informācijas sniegšanas veidiem ir pārziņa mājaslapā ievietot attiecīgas informācijas klauzulas, piemēram, vietnes konfidencialitātes

536 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 70. punkts.

537 Eiropas Komisija turpinās pilnveidot ar ikonām apzīmējamo informāciju un procedūras standartizētu ikonu nodrošināšanai, izmantojot deleģētos aktus; skatīt Vispārīgās datu aizsardzības regulas 12. panta 8. punktu.

538 Vispārīgā datu aizsardzības regula, 12. panta 1., 5. un 7. punkts; modernizētā Konvencija Nr. 108, 9. panta 1. punkta b) apakšpunkts.

539 Skatīt arī 29. panta darba grupas (2004) *Atzinumu 10/2004 par saskaņotākiem noteikumiem attiecībā uz informāciju*, WP 100, Brisele, 2004. gada 25. novembris.

politiku. Tomēr ievērojama daļa iedzīvotāju neizmanto internetu, un uzņēmuma vai publiskas iestādes informācijas politikā tas ir jāņem vērā.

Paziņojums par privātumu attiecībā uz personas datu apstrādi tīmekļa vietnē varētu izskatīties šādi:

Kas mēs esam?

Datu apstrādes pārzinis ir "Viesu nams C&U", kurš atrodas [adrese: xxx], tālr.: xxx; fakss: xxx; e-pasts info@c&u.com; datu aizsardzības speciālista kontaktinformācija: [xxx].

Paziņojums par personas datiem ietilpst pakalpojumu sniegšanas noteikumos.

Kādus datus no jums vācam?

Mēs no jums vācam šādus personas datus: jūsu vārds, uzvārds, pasta adrese, tālruņa numurs, e-pasta adrese, uzturēšanās informācija, kredītkartes un debetkartes numurs un to datoru IP adreses vai domēnu nosaukumi, ko izmantojāt, lai izveidotu savienojumu ar mūsu tīmekļa vietni.

Kāpēc mēs vācam jūsu datus?

Mēs apstrādājam jūsu datus, pamatojoties uz jūsu piekrišanu, lai veiktu rezervācijas, noslēgtu un izpildītu līgumus, kas saistīti ar jums piedāvātajiem pakalpojumiem, kā arī izpildītu likumos noteiktās prasības, piemēram, Likumā par vietējām nodevām, saskaņā ar kuru mums ir pienākums vākt personas datus, lai mēs varētu samaksāt pilsētas nodokli par izmitināšanu.

Kā mēs apstrādājam jūsu datus?

Jūsu personas dati tiks glabāti trīs mēnešus. Uz jūsu datiem neattiecas automātiskas lēmumu pieņemšanas procedūras.

Mūsu "Viesu nams C&U" ievēro stingras drošības procedūras, lai nodrošinātu, ka jūsu personiskā informācija netiek bojāta, iznīcināta, bez jūsu atļaujas izpausta trešām personām, kā arī novērstu neatļautu piekļuvi. Datori, kuros tiek uzglabāta informācija, tiek turēti drošā vidē ar ierobežotu fizisko piekļuvi.

Mēs izmantojam drošus ugunsmūrus, kā arī citus pasākumus, lai ierobežotu elektronisko piekļuvi. Ja dati ir jāpārsūta trešai personai, mēs pieprasām, lai tā īstenotu līdzīgus pasākumus jūsu personas datu aizsardzībai.

Visa informācija, ko mēs apkopojam vai reģistrējam, atrodas tikai mūsu birojos. Piekļuve personas datiem tiek piešķirta tikai tām personām, kurām nepieciešama informācija, lai pildītu savus pienākumus saskaņā ar šo līgumu. Mēs skaidri pieprasīsim, ja būs nepieciešama informācija jūsu identificēšanai. Mēs, iespējams, lūgsim jūs iziet mūsu drošības pārbaudes, pirms mēs jums izpaudīsim informāciju. Jebkurā laikā varat atjaunināt jūsu sniegto personisko informāciju, tieši sazinoties ar mums.

Kādas ir jūsu tiesības?

Jums ir tiesības piekļūt jūsu datiem, iegūt šo datu kopijas, pieprasīt datu dzēšanu vai veikt labojumus vai lūgt jūsu datus nodot citam pārzinim.

Jūs varat ar mums sazināties, sūtot savus pieprasījumus uz e-pastu info@c&u.com. Mums ir pienākums atbildēt uz jūsu pieprasījumu viena mēneša laikā, bet, ja jūsu pieprasījums ir pārāk sarežģīts vai mēs saņemam lielu skaitu citu pieprasījumu, mēs jūs informēsim, ka šis periods var tikt pagarināts vēl par diviem mēnešiem.

Piekļuve jūsu personas datiem

Jums ir tiesības piekļūt saviem datiem, kas pēc pieprasījuma tiek izsniegti kopā ar informāciju par datu apstrādes pamatu, pieprasīt datu dzēšanu vai labojumus un tiesības lūgt uz jums neattiecināt pilnībā automatizētus lēmumus, kuros jūsu viedoklis netiek ņemts vērā. Jūs varat ar mums sazināties, sūtot savus pieprasījumus uz e-pastu info@c&u.com. Jums arī ir tiesības iebilst pret apstrādi, atsaukt piekrišanu un iesniegt sūdzību valsts uzraudzības iestādei, ja uzskatāt, ka šāda datu apstrāde ir pretrunā likumam, kā arī pieprasīt kompensāciju par zaudējumiem, kas radušies nelikumīgas apstrādes rezultātā.

Tiesības iesniegt sūdzību

VDAR ir noteikts pienākums pārzinim informēt datu subjektus par izpildes mehānismiem saskaņā ar valstu un ES tiesību aktiem personas datu aizsardzības pārkāpumu gadījumos. Pārzinim jāinformē datu subjekti par viņu tiesībām iesniegt sūdzību par personas datu aizsardzības pārkāpumiem uzraudzības iestādē un, ja nepieciešams, valsts tiesā[540]. EP tiesību aktos ir arī paredzētas datu subjektiem tiesības būt informētiem par viņu tiesību īstenošanas līdzekļiem, tostarp tiesības uz tiesiskās aizsardzības līdzekļiem, kas noteiktas 9. panta 1. punkta f) apakšpunktā.

Atbrīvojumi no pienākuma informēt

VDAR paredzēts izņēmums pienākumam informēt. Saskaņā ar VDAR 13. panta 4. punktu un 14. panta 5. punktu pienākums informēt datu subjektus nav attiecināms gadījumos, kad datu subjektam jau ir visa būtiskā informācija[541]. Turklāt, ja personas dati nav iegūti no datu subjekta, informēšanas pienākumu nepiemēro gadījumos, kad informācijas sniegšana nav iespējama vai ir nesamērīgi apgrūtinoša, jo īpaši, ja personas dati tiek apstrādāti arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos vai statistikas nolūkos[542].

Turklāt dalībvalstīm ir zināma rīcības brīvība saskaņā ar VDAR noteikt ierobežojumus pienākumiem un tiesībām, kas indivīdiem noteiktas saskaņā ar regulu, ja tas ir nepieciešams un samērīgs pasākums demokrātiskā sabiedrībā, piemēram, lai aizsargātu valsts un sabiedrisko drošību, aizsardzības, tiesu izmeklēšanas un tiesvedības vai ekonomisko un finanšu interešu, kā arī privāto interešu aizsardzības nolūkos, kas ir svarīgākas par datu aizsardzības interesēm[543].

Jebkādiem atbrīvojumiem vai ierobežojumiem jābūt nepieciešamiem demokrātiskā sabiedrībā un samērīgiem attiecībā uz izvirzīto mērķi. Ļoti retos gadījumos, piemēram, medicīnisku indikāciju dēļ, datu subjekta aizsardzībai var būt nepieciešama pārredzamības ierobežošana. Tas jo īpaši attiecas uz ikviena datu subjekta piekļuves tiesību ierobežošanu[544]. Tomēr valstu tiesību aktos vismaz ir jāievēro pamattiesību

540 Vispārīgā datu aizsardzības 13. panta 2. punkta d) apakšpunkts un 14. panta 2. punkta e) apakšpunkts; modernizētā Konvencija Nr. 108, 8. panta 1. punkta f) apakšpunkts.

541 Turpat, 13. panta 4. punkts, 14. panta 5. punkta a) apakšpunkts.

542 Turpat, 14. panta 5. punkta b) – e) apakšpunkts.

543 Vispārīgā datu aizsardzības regula, 23. panta 1. punkts.

544 Vispārīgā datu aizsardzības regula, 15. pants.

un brīvību, ko aizsargā ES tiesību akti, būtība[545]. Tādēļ valstu tiesību aktos jāietver īpaši noteikumi, kas precizē apstrādes nolūku, iekļauto personas datu kategorijas, aizsardzības pasākumus un citas procesuālās prasības[546].

Ja dati tiek vākti zinātniskās vai vēstures pētniecības nolūkos, statistikas nolūkos vai arhivēšanas nolūkos sabiedrības interesēs, Savienības vai dalībvalstu tiesību aktos var paredzēt atkāpes no pienākuma informēt, ja tas varētu padarīt neiespējamu vai nopietni apgrūtināt konkrētu mērķu sasniegšanu[547].

Līdzīgi ierobežojumi pastāv EP tiesību aktos, saskaņā ar kuriem tiesībām, kas datu subjektiem piešķirtas saskaņā ar modernizētās Konvencijas Nr. 108 9. pantu, ar stingriem nosacījumiem var piemērot iespējamos ierobežojumus atbilstoši modernizētās Konvencijas Nr. 108 11. pantam. Turklāt atbilstoši modernizētās Konvencijas Nr. 108 8. panta 2. punktam pārziņiem uzlikto apstrādes pārskatāmības pienākumu nepiemēro, ja datu subjekts jau ir informēts.

Indivīda tiesības piekļūt saviem datiem

Saskaņā ar EP tiesību aktiem modernizētās Konvencijas Nr. 108 9. pantā ir skaidri noteiktas tiesības piekļūt personas datiem. Ar tām paredz, ka ikvienam indivīdam ir tiesības pēc pieprasījuma saņemt saprotamā veidā nodotu informāciju par ar viņu saistīto personas datu apstrādi. Piekļuves tiesības ir atzītas ne tikai modernizētās Konvencijas Nr. 108 noteikumos, bet arī ECT judikatūrā. ECT vairākkārt ir atzinusi, ka indivīdiem ir tiesības piekļūt informācijai par viņu personas datiem un ka šīs tiesības izriet no nepieciešamības uz privātās dzīves neaizskaramību[548]. Tomēr noteiktos apstākļos tiesības uz piekļuvi personas datiem, ko glabā valsts vai privātas organizācijas, var tikt ierobežotas[549].

ES tiesiskajā regulējumā tiesības piekļūt saviem datiem ir skaidri noteiktas VDAR 15. pantā, un tās kā pamattiesības uz personas datu aizsardzību ir noteiktas arī ES

545 Vispārīgā datu aizsardzības regula, 23. panta 1. punkts.

546 Turpat, 23. panta 2. punkts.

547 Turpat, 89. panta 2. un 3. punkts.

548 ECT 1989. gada 7. jūlija spriedums lietā *Gaskin pret Apvienoto Karalisti*, Nr. 10454/83; ECT 2003. gada 13. februāra spriedums lietā *Odièvre pret Franciju* [GC], Nr. 42326/98; ECT 2009. gada 28. aprīļa spriedums lietā *K.H. un citi pret Slovākiju*, Nr. 32881/04; ECT 2012. gada 25. septembra spriedums lietā *Godelli pret Itāliju*, Nr. 33783/09.

549 ECT 1987. gada 26. marta spriedums lietā *Leander pret Zviedriju*, Nr. 9248/81.

Pamattiesību hartas 8. panta 2. punktā[550]. Indivīda tiesības piekļūt saviem personas datiem ir galvenais Eiropas datu aizsardzības tiesību aktu elements[551].

VDAR paredzēts, ka katram datu subjektam ir tiesības piekļūt saviem personas datiem un noteiktai informācijai par apstrādi, kuru pārziņiem ir pienākums sniegt[552]. Jo īpaši katram datu subjektam ir tiesības saņemt (no pārziņa) apstiprinājumu, vai dati, kas attiecas uz viņu, tiek apstrādāti, un informāciju par vismaz šādiem jautājumiem:

- apstrādes nolūkiem;
- attiecīgo datu kategorijām;
- saņēmējiem vai saņēmēju kategorijām, kuriem dati tiek atklāti;
- laikposmu, cik ilgi datus paredzēts glabāt, vai, ja tas nav iespējams, kritērijiem, kas izmantoti šāda laikposma noteikšanai;
- tiesībām labot vai dzēst personas datus vai ierobežot personas datu apstrādi;
- tiesībām iesniegt sūdzību uzraudzības iestādē;
- visu pieejamo informāciju par apstrādājamo datu avotu, ja dati nav savākti no datu subjekta;
- automatizētu lēmumu gadījumā – datu automatizētā apstrādē izmantoto loģiku.

Datu pārzinim ir pienākums izsniegt datu subjektam apstrādājamo personas datu kopiju. Jebkāda informācija datu subjektam jāsniedz tam saprotamā veidā, kas nozīmē, ka pārzinim jāpārliecinās, ka datu subjekts var saprast sniegto informāciju. Piemēram, parasti tehnisku saīsinājumu, kodētu terminu vai akronīmu iekļaušana, atbildot uz piekļuves pieprasījumu, nav pietiekama, ja vien šo terminu nozīme nav

550 Skatīt arī EST 2014. gada 17. jūlija spriedumu apvienotajās lietās C-141/12 un C-372/12 *YS pret Minister voor Immigratie, Integratie en Asiel* un *Minister voor Immigratie, Integratie en Asiel pret M un S*; EST 2015. gada 16. jūlija spriedumu lietā C-615/13 P *ClientEarth, Pesticide Action Network Europe (PAN Europe) pret Eiropas Pārtikas nekaitīguma iestādi (EFSA), Eiropas Komisiju*.

551 EST 2014. gada 17. jūlija spriedums apvienotajās lietās C-141/12 un C-372/12 *YS pret Minister voor Immigratie, Integratie en Asiel* un *Minister voor Immigratie, Integratie en Asiel pret M un S*.

552 Vispārīgā datu aizsardzības regula, 15. panta 1. punkts.

izskaidrota. Ja tiek veikta automatizēta lēmumu pieņemšana, tostarp profilēšana, ir jāpaskaidro vispārējā automatizētās lēmumu pieņemšanas loģika, iekļaujot kritērijus, kas ņemti vērā, novērtējot datu subjektu. **EP tiesību aktos** ir līdzīgas prasības[553].

Piemērs. Piekļuve saviem personas datiem ļauj datu subjektam noteikt, vai dati ir precīzi. Tāpēc ir svarīgi, lai datu subjekts saprotamā veidā tiktu informēts ne tikai par faktiski apstrādātajiem personas datiem, bet arī par kategorijām, kurās šie personas dati tiek apstrādāti un kas ir, piemēram, vārds, uzvārds, IP adrese, ģeogrāfiskās atrašanās vietas koordinātes, kredītkartes numurs u. tml.

Informācija par datu avotu, ja dati netiek vākti no datu subjekta, jāsniedz atbildē uz piekļuves pieprasījumu, ciktāl šī informācija ir pieejama. Šī norma ir jāsaprot godprātības, pārredzamības un pārskatatbildības principu kontekstā. Pārzinis nedrīkst iznīcināt informāciju par datu avotu nolūkā atbrīvot sevi no pienākuma to izpaust, izņemot gadījumus, kad dati tiktu dzēsti, kaut arī ir saņemts piekļuves pieprasījums, un pārzinim joprojām ir jāievēro vispārējās "pārskatatbildības" prasības.

Kā noteikts EST judikatūrā, tiesības piekļūt personas datiem nevar tikt nepamatoti ierobežotas ar termiņiem. Datu subjektiem jādod arī iespēja pamatoti saņemt informāciju par agrāk veiktajām datu apstrādes darbībām.

Piemērs. Lietā *Rijkeboer*[554] EST tika lūgts noteikt, vai indivīda tiesības piekļūt informācijai par personas datu saņēmējiem vai saņēmēju kategorijām un datu saturam var būt ierobežotas līdz vienam gadam pirms viņa vai viņas piekļuves pieprasījuma iesniegšanas.

Lai noteiktu, vai ES tiesību aktos atļauts piemērot šādu termiņu, EST nolēma interpretēt 12. pantu, ņemot vērā direktīvas mērķus. EST vispirms paziņoja, ka piekļuves tiesības ir nepieciešamas, lai datu subjekts varētu īstenot savas tiesības lūgt pārzinim labot, dzēst vai bloķēt viņa datus vai informēt trešās personas, kurām dati ir izpausti, par šādu labojumu, dzēšanu vai bloķēšanu.

553 Skatīt modernizēto Konvenciju Nr. 108, 8. panta 1. punkta c) apakšpunkts.

554 EST 2009. gada 7. maija spriedums lietā C-553/07 *College van burgemeester en wethouders van Rotterdam pret M. E. E. Rijkeboer*.

Efektīvas piekļuves tiesības ir arī nepieciešamas, lai datu subjekts varētu īstenot savas tiesības iebilst pret savu personas datu apstrādi vai tiesības iesniegt sūdzību un pieprasīt zaudējumu atlīdzību[555].

Lai nodrošinātu datu subjektiem piešķirto tiesību praktisko efektu, EST sprieda, ka "šīm tiesībām noteikti ir jāattiecas uz pagātni. Ja tas tā nebūtu, attiecīgā persona nevarētu efektīvi izmantot savas tiesības likt labot, dzēst vai neļaut iepazīties ar datiem, kas tiek uzskatīti par nelikumīgiem vai nepareiziem, kā arī celt prasību tiesā un panākt nodarīto zaudējumu atlīdzību".

6.1.2. Tiesības labot datus

Saskaņā ar ES un **EP tiesību aktiem** datu subjektiem ir tiesības labot savus personas datus. Personas datu precizitāte ir būtiska, lai nodrošinātu datu subjektiem augstu datu aizsardzības līmeni[556].

Piemērs. Lietā *Ciubotaru pret Moldovu*[557] prasītājam nebija iespējas mainīt savas etniskās izcelsmes reģistrāciju oficiālajā reģistrā no moldāvu uz rumāņu, it kā tāpēc, ka viņš nebija pamatojis savu pieprasījumu. ECT uzskatīja, ka valstis drīkst pieprasīt objektīvus pierādījumus, reģistrējot personas etnisko identitāti. Ja šādas prasības pamatā bija tīri subjektīvi un nepamatoti iemesli, iestādēm ir tiesības atteikt šo prasību. Tomēr prasītāja prasības pamatā bija vairāk nekā subjektīva viņa etniskās piederības uztvere. Viņš bija spējis nodrošināt objektīvi pārbaudāmas saiknes ar rumāņu etnisko grupu, piemēram, valodu, vārdu, empātiju un citas. Tomēr saskaņā ar valsts tiesību aktiem prasītājam bija jāsniedz pierādījumi par viņa vecāku piederību rumāņu etniskajai grupai. Ņemot vērā Moldovas vēsturisko realitāti, šāda prasība radīja nepārvaramu šķēršli reģistrēt etnisko identitāti, kas atšķīrās no tās, kuru padomju varas iestādes bija reģistrējušas attiecībā uz prasītāja vecākiem. Liekot šķēršļus prasītāja prasības pārbaudei, ņemot vērā objektīvi pārbaudāmus pierādījumus, valsts nebija izpildījusi savu pienākumu nodrošināt prasītājam efektīvu viņa privātās dzīves neaizskaramību. Tiesa secināja, ka ir pārkāpts ECTK 8. pants.

555 Vispārīgā datu aizsardzības regula, 15. panta 1. punkta c) un f) apakšpunkts, 16. pants, 17. panta 2. punkts un 21 .pants, kā arī VIII nodaļa.

556 Turpat, 16. pants un 65. apsvērums; modernizētā Konvencija Nr. 108, 9. panta 1. punkta e) apakšpunkts.

557 ECT 2010. gada 27. aprīļa spriedums lietā *Ciubotaru pret Moldovu*, Nr. 27138/04, 51. un 59. punkts.

Dažos gadījumos datu subjektam pietiek tikai ar lūgumu veikt labojumu, piemēram, saistībā ar vārda pareizrakstību, adreses maiņu vai tālruņa numuru. Atbilstoši **ES** un **EP tiesību aktiem** kļūdaini personas dati ir jālabo bez nepamatotas vai pārmērīgas kavēšanās[558]. Ja tomēr šādi pieprasījumi ir saistīti ar juridiski nozīmīgiem jautājumiem, piemēram, datu subjekta juridisko identitāti vai pareizo dzīvesvietu juridisko dokumentu piegādāšanai, var nepietikt tikai ar pieprasījumu veikt labojumu un pārzinim var būt tiesības pieprasīt iespējamās neprecizitātes pierādījumu. Šādas prasības nedrīkst radīt datu subjektam nesamērīgu pierādīšanas slogu, tādējādi liedzot datu subjektiem labot savus datus. ECT ir atzinusi ECTK 8. panta pārkāpumus vairākos gadījumos, kad prasītājam nav bijusi iespēja apstrīdēt slepenos reģistros glabātās informācijas precizitāti[559].

Piemērs. Lietā *Cemalettin Canli pret Turciju*[560] ECT konstatēja ECTK 8. panta pārkāpumu policijas nepareizi sniegtajā ziņojumā kriminālprocesa ietvaros.

Prasītājs bija divreiz iesaistīts kriminālprocesā iespējamās dalības nelikumīgās organizācijās dēļ, taču netika notiesāts. Kad prasītājs tika atkal apcietināts un apsūdzēts par citu noziedzīgu nodarījumu, policija kriminālprocesā iesniedza ziņojumu ar nosaukumu "informācijas veidlapa par papildu nodarījumiem", kurā apgalvoja, ka prasītājs ir divu nelikumīgu organizāciju biedrs. Prasītāja lūgums veikt labojumus ziņojumā un policijas reģistrā netika apmierināts. ECT uzskatīja, ka uz informāciju policijas ziņojumā attiecas ECTK 8. pants, jo sistemātiski vākta publiska informācija, kas glabājas iestāžu rīcībā esošajās lietās, varētu atbilst arī "privātās dzīves" jēdziena nozīmei. Turklāt policijas ziņojums bija nepareizi sagatavots, tā iesniegšana krimināltiesā neatbilda valsts tiesību aktiem. Tiesa atzina, ka šajā lietā ticis pārkāpts 8. pants.

Civillietās vai tiesvedības laikā publiskā iestādē, lai izlemtu, vai dati ir pareizi, datu subjekts var lūgt, lai viņa datu lietā tiktu pievienots ieraksts vai piezīme, norādot, ka precizitāte ir apstrīdēta un ka tiek gaidīts oficiāls lēmums[561]. Šajā laikā datu pārzinis nedrīkst uzrādīt datus kā pareizus un nedrīkst tos grozīt, jo īpaši ļaut to darīt trešām personām.

558 Vispārīgā datu aizsardzības regula, 16. pants; modernizētā Konvencija Nr. 108, 9. panta 1. punkts.

559 ECT 2000. gada 4. maija spriedums lietā *Rotaru pret Rumāniju* [GC], Nr. 28341/95.

560 ECT 2008. gada 18. novembra spriedums lietā *Cemalettin Canli pret Turciju*, Nr. 22427/04, 33. un 42.–43. punkts; ECT 2010. gada 2. februāra spriedums lietā *Dalea pret Franciju*, Nr. 964/07.

561 Vispārīgā datu aizsardzības regula, 16. panta 2. teikums.

6.1.3. Tiesības dzēst datus ("tiesības tikt aizmirstam")

Datu subjekta tiesību uz savu datu dzēšanu nodrošināšana ir īpaši svarīga, lai efektīvi piemērotu datu aizsardzības principus, jo īpaši datu minimizācijas principu (personas dati ir jāierobežo līdz tādam apjomam, kas nepieciešams nolūkiem, kuriem šie dati tiek apstrādāti). Tādēļ tiesības uz dzēšanu ietvertas gan EP, gan ES tiesību instrumentos[562].

Piemērs. Lietā *Segerstedt-Wiberg un citi pret Zviedriju*[563] prasītāji bija saistīti ar noteiktām liberālām un komunistiskām politiskām partijām. Prasītājiem bija aizdomas, ka informācija par viņiem ir ievadīta drošības policijas lietvedībā, un viņi pieprasīja tās dzēšanu. ECT pauda pārliecību, ka aplūkojamo datu glabāšanai bija likumīgs pamats un tai bija leģitīms mērķis. Tomēr attiecībā uz dažiem iesniedzējiem ECT secināja, ka pastāvīga datu glabāšana ir nesamērīga iejaukšanās viņu privātajā dzīvē. Piemēram, viena prasītāja gadījumā iestādes glabāja informāciju, ka 1969. gadā demonstrācijās viņš it kā iestājies par vardarbīgu pretošanos policijas kontrolei. ECT secināja, ka šī informācija nevar būt būtiska valsts drošības interesēm, īpaši ņemot vērā tās vēsturisko raksturu. Tiesa konstatēja ECK 8. panta pārkāpumu attiecībā uz četriem no pieciem prasītājiem, jo, ņemot vērā ilgo laika posmu kopš darbībām, kas prasītājiem tika piedēvētas, viņu datu ilgstoša glabāšana nebija būtiska.

Piemērs. Lietā *Brunet pret Franciju*[564] prasītāji vērsās pret viņu personiskās informācijas glabāšanu policijas datubāzē, kas satur informāciju par notiesātajām personām, apsūdzētajiem un cietušajiem. Kaut arī kriminālprocess pret prasītāju tika pārtraukts, informācija par viņu parādījās datubāzē. Tāpēc ECT atzina, ka šajā lietā ir pārkāpts ECTK 8. pants. Savā secinājumā Tiesa uzskatīja, ka praksē prasītājam nebija iespējas dzēst savus personas datus no datubāzes. ECT arī aplūkoja datubāzē iekļautās informācijas raksturu un uzskatīja, ka tā aizskar prasītāja privātumu, jo satur ziņas par viņa identitāti un personību. Tiesa arī konstatēja, ka personas datu 20 gadu glabāšanas periods datubāzē ir bijis pārmērīgi ilgs, jo īpaši tāpēc, ka prasītājs nevienā tiesā nebija notiesāts.

562 Turpat, 17. pants.

563 ECT 2006. gada 6. jūnija spriedums lietā *Segerstedt-Wiberg un citi pret Zviedriju*, Nr. 62332/00, 89. un 90. punkts; skatīt arī, piemēram, ECT 2013. gada 18. aprīļa spriedumu lietā *M.K. pret Franciju*, Nr. 19522/09.

564 ECT 2014. gada 18. septembra spriedums lietā *Brunet pret Franciju*, Nr. 21010/10.

Modernizētajā Konvencijā Nr. 108 ir skaidri noteikts, ka ikvienam indivīdam ir tiesības dzēst neprecīzus, nepatiesus vai nelikumīgi apstrādātus datus[565].

Saskaņā ar ES tiesību aktiem VDAR 17. pantā datu subjektam ir piešķirtas tiesības lūgt dzēst vai svītrot viņa datus. Tiesības uz personas datu dzēšanu bez nepamatotas aizkavēšanās ir spēkā, ja:

- personas dati vairs nav nepieciešami tiem nolūkiem, kādos tie tika vākti vai citādi apstrādāti;
- datu subjekts atsauc piekrišanu, kurā balstīta apstrāde, un apstrādei nav cita juridiska pamata;
- datu subjekts iebilst pret apstrādi, un apstrādei nav svarīgāka leģitīma pamata;
- personas dati ir apstrādāti nelikumīgi;
- personas dati ir jādzēš, lai nodrošinātu, ka tiek pildīts juridisks pienākums, kas noteikts Savienības vai dalībvalstu tiesību aktos, kuri ir piemērojami pārzinim;
- personas dati apkopoti saistībā ar informācijas sabiedrības pakalpojumu piedāvāšanu bērniem saskaņā ar VDAR 8. pantu[566].

Datu apstrādes likumīguma pierādīšanas pienākums gulstas uz datu pārziņiem, jo viņi ir atbildīgi par apstrādes likumību[567]. Saskaņā ar pārskatatbildības principu pārzinim jebkurā brīdī jāspēj pierādīt, ka tā datu apstrādei ir stabils juridiskais pamats, pretējā gadījumā apstrāde ir jāpārtrauc[568]. VDAR definēti izņēmumi tiesībām tikt aizmirstam, tostarp gadījumos, ja personas datu apstrāde ir nepieciešama:

- lai īstenotu tiesības uz vārda brīvību un informāciju;
- lai izpildītu juridisku pienākumu, kas prasa veikt apstrādi, kā paredzēts Savienības vai dalībvalstu tiesību aktos, kuri piemērojami pārzinim, vai lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai saistībā ar pārzinim likumīgi piešķirto oficiālo pilnvaru īstenošanu;

565 Modernizētā Konvencija Nr. 108, 9. panta 1. punkta e) apakšpunkts.

566 Vispārīgā datu aizsardzības regula, 17. panta 1. punkts.

567 Turpat.

568 Turpat, 5. panta 2. punkts.

- sabiedrības interesēs sabiedrības veselības jomā;
- arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos vai statistikas nolūkos;
- lai celtu, īstenotu vai aizstāvētu likumīgas prasības[569].

EST ir apstiprinājusi tiesību dzēst datus nozīmi, lai nodrošinātu augsta līmeņa datu aizsardzību.

Piemērs. Lietā *Google Spain*[570] EST apsvēra, vai *Google* bija pienākums no sava meklēšanas saraksta rezultātiem dzēst novecojušu informāciju par prasītāja finansiālajām grūtībām. Cita starpā *Google* apstrīdēja tā atbildību, apgalvojot, ka nodrošina tikai hipersaiti uz izdevēja tīmekļa vietni, kurā ir izvietota informācija, šajā gadījumā laikrakstu, kurā tiek ziņots par prasītāja maksātnespējas problēmām[571]. *Google* iebilda, ka pieprasījums dzēst novecojušu informāciju no tīmekļa vietnes ir jāiesniedz tīmekļa vietnes mitinātājam, nevis *Google*, kas vienkārši nodrošina saiti uz sākotnējo lapu. EST secināja, ka *Google*, meklējot tīmeklī informāciju un tīmekļa vietnes un indeksējot saturu, lai nodrošinātu meklēšanas rezultātus, kļūst par datu pārzini, uz kuru attiecas ES tiesību aktos ietvertie pienākumi un saistības.

EST paskaidroja, ka ar interneta meklētājprogrammām un meklēšanas rezultātiem ar personas datiem var izveidot detalizētu personas profilu[572]. Meklētājprogrammas padara informāciju, kas ietverta šādā rezultātu sarakstā, par visuresošu. Ņemot vērā iespējamo nopietnību, šo iejaukšanos nevar attaisnot tikai ar meklētājprogrammas operatora ekonomiskām interesēm šajā apstrādē. Jo īpaši jārod līdzsvars starp interneta lietotāju likumīgajām interesēm piekļūt informācijai un datu subjekta pamattiesībām saskaņā ar

569 Turpat, 17. panta 3. punkts.

570 EST 2014. gada 13. maija spriedums lietā C-131/12 *Google Spain SL un Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 55.–58. punkts.

571 *Google* apstrīdēja arī ES datu aizsardzības noteikumu piemērošanu, pamatojoties uz to, ka *Google Inc.* ir reģistrēts ASV un lietā aplūkoto personas datu apstrāde arī tika veikta ASV. Otrs arguments par ES datu aizsardzības tiesību aktu nepiemērojamību bija saistīts ar apgalvojumu, ka par "pārziņiem" attiecībā uz rezultātos redzamajiem datiem nevar uzskatīt meklētājprogrammas, jo *Google* nepārzina šos datus, kā arī tos nekontrolē. EST noraidīja abus argumentus, uzskatot, ka šajā gadījumā ir piemērojama Direktīva 95/46/EK, un turpināja pārbaudīt garantēto tiesību tvērumu, jo īpaši tiesības uz personas datu dzēšanu.

572 Turpat, 36., 38., 80.–81. un 97. pants.

ES Pamattiesību hartas 7. un 8. pantu. Ņemot vērā sabiedrības pieaugošo digitalizāciju, prasība, lai personas dati būtu precīzi un nepārsniegtu nepieciešamo (t. i., sniegt informāciju sabiedrībai), ir būtiska, lai nodrošinātu indivīdiem augstu datu aizsardzības līmeni. "Personas datu apstrādātājam ir savas atbildības, kompetenču un iespēju ietvaros jānodrošina, ka tā atbilst (..) prasībām", kas noteiktas ES tiesību aktos, lai ieviestajām juridiskajām garantijām būtu pilnīgs spēks[573]. Tas nozīmē, ka tiesības uz personas datu dzēšanu, kad apstrāde ir novecojusi vai vairs nav nepieciešama, attiecas arī uz datu pārziņiem, kuri atkārtoti sniedz informāciju[574].

Pārbaudot, vai uzņēmumam *Google* bija jāizņem ar pieteikuma iesniedzēju saistītās saites, EST nosprieda, ka noteiktos apstākļos indivīdiem ir tiesības pieprasīt savu personīgo datu dzēšanu. Šīs tiesības var tikt izmantotas, ja informācija, kas attiecas uz personu, ir neprecīza, neadekvāta, neatbilstoša vai pārmērīga datu apstrādes nolūkos. EST atzina, ka šīs tiesības nav absolūtas. Tās jālīdzsvaro ar citām tiesībām un interesēm, jo īpaši ar plašas sabiedrības interesēm un tiesībām piekļūt noteiktai informācijai. Katrs dzēšanas pieprasījums jāizvērtē atsevišķi, lai nodrošinātu līdzsvaru starp datu subjekta pamattiesībām uz personas datu aizsardzību un privāto dzīvi, no vienas puses, un visu interneta lietotāju, tostarp izdevēju, likumīgajām interesēm, no otras puses. EST sniedza norādījumus par faktoriem, kas jāņem vērā izsvēršanas gaitā. Īpaši svarīgs faktors ir konkrētās informācijas raksturs. Ja informācija skar indivīda privāto dzīvi un ja attiecībā uz informācijas pieejamību nav sabiedrības intereses, datu aizsardzība un privātums ir svarīgāki par plašas sabiedrības tiesībām piekļūt informācijai. Tieši pretēji, ja datu subjekts, šķiet, ir publiska persona vai informācijas raksturs attaisno piekļuves šādai informācijai piešķiršanu plašākai sabiedrībai, tad īpašās plašākas sabiedrības intereses piekļūt informācijai var attaisnot iejaukšanos datu aizsardzības un privātuma pamattiesībās.

Pēc sprieduma 29. panta darba grupa pieņēma pamatnostādnes par EST nolēmuma īstenošanu[575]. Pamatnostādnēs ir iekļauts kopējais kritēriju saraksts, kas uzraudzības

573 Turpat, 81.–83. punkts.

574 EST 2014. gada 13. maija spriedums lietā C-131/12 *Google Spain SL un Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 88. punkts. Skatīt arī 29. panta darba grupas (2014) *EST sprieduma "Google Spain SL un Google Inc pret Agencia Española de Protección de Datos (AEPD) un Mario Costeja González" (C-131/12) īstenošanas pamatnostādnes*, WP 225, Brisele, 2014. gada 26. novembris, un Ministru komitejas Ieteikumu CM/Rec 2012(3) dalībvalstīm cilvēktiesību aizsardzībai attiecībā uz meklētājprogrammām, 2012. gada 4. aprīlis.

575 29. panta darba grupa (2014), *EST sprieduma "Google Spain SL un Google Inc pret Agencia Española de Protección de Datos (AEPD) un Mario Costeja González" (C-131/12) īstenošanas pamatnostādnes*, WP 225, Brisele, 2014. gada 26. novembris.

iestādēm jāizmanto, izskatot sūdzības saistībā ar personu dzēšanas pieprasījumiem, paskaidrojot, ko šādas tiesības uz datu dzēšanu sevī ietver, un norādes iestādēm, līdzsvarojot šīs tiesības. Pamatnostādnēs atkārtoti uzsvērts, ka novērtējumi jāveic katrā gadījumā atsevišķi. Tā kā tiesības tikt aizmirstam nav absolūtas, atbilde uz pieprasījumu var atšķirties atkarībā no izskatāmā gadījuma. To ilustrē arī EST judikatūra pēc *Google* lietas.

Piemērs. Lietā *Camera di Commercio di Lecce pret Manni*[576] EST bija jānosaka, vai privātpersonai ir tiesības pieprasīt dzēst savus personas datus, kas publicēti Uzņēmumu publiskajā reģistrā, tiklīdz tās uzņēmums beidzis pastāvēt. *Manni* kungs bija lūdzis Lečes Tirdzniecības palātai dzēst viņa personas datus no šā reģistra, jo bija atklājis, ka potenciālie klienti izmanto reģistru un redz, ka viņš agrāk ir bijis administrators kādam uzņēmumam, ko pirms vairāk nekā desmit gadiem pasludināja par bankrotējušu. Prasītājs uzskatīja, ka šī informācija varētu atturēt viņa potenciālos klientus.

Līdzsvarojot *Manni* kunga tiesības uz personas datu aizsardzību ar plašas sabiedrības interesēm piekļūt informācijai, EST vispirms pārbaudīja publiskā reģistra mērķi. Tiesa norādīja uz faktu, ka datu izpaušana bija paredzēta likumā un jo īpaši ES direktīvā, kuras mērķis ir padarīt informāciju par uzņēmumiem vieglāk pieejamu trešām personām. Tādējādi trešām personām jābūt piekļuvei un iespējai pārbaudīt uzņēmuma pamatdokumentus un citu informāciju par uzņēmumu, "īpaši ar sīkiem datiem par personām, kuras ir pilnvarotas uzņemties saistības sabiedrības vārdā". Informācijas izpaušanas mērķis bija arī garantēt juridisko noteiktību, ņemot vērā intensīvāku tirdzniecību starp dalībvalstīm, nodrošinot, ka trešām personām ir pieejama visa būtiskā informācija par uzņēmumiem visā ES.

EST arī atzīmēja, ka pat pēc laika un pat pēc uzņēmuma likvidācijas ar uzņēmumu saistītās tiesības un juridiskie pienākumi bieži turpina pastāvēt. Ar uzņēmuma likvidāciju saistītie strīdi var būt ilgstoši, un vēl daudzus gadus pēc uzņēmuma darbības izbeigšanas var rasties jautājumi par uzņēmumu, tā vadītājiem un likvidatoriem. EST nosprieda, ka, ņemot vērā daudzus un dažādus iespējamos scenārijus un atšķirības katrā dalībvalstī paredzētajos noilguma periodos, "pašreiz šķiet neiespējami identificēt vienotu termiņu, skaitot no sabiedrības likvidācijas, pēc kura beigām minēto datu ieraksts reģistrā un to atklātība vairs nav vajadzīga". Izpaušanas likumīgā mērķa dēļ

576 EST 2017. gada 9. marta spriedums lietā C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce pret Salvatore Manni*.

un saistībā ar grūtībām noteikt termiņu, kurā personas datus varētu dzēst no reģistra, nekaitējot trešo personu interesēm, EST secināja, ka ES datu aizsardzības noteikumi negarantē tiesības dzēst personas datus personām *Manni* kunga situācijā.

Ja pārzinis ir publiskojis personas datus un viņam ir pienākums dzēst informāciju, datu pārzinim ir pienākums un tam jāīsteno "pamatoti" pasākumi, lai informētu citus pārziņus, kuri apstrādā tos pašus datus, par datu subjekta pieprasījumu dzēst datus. Pārzinim, veicot darbības, jāņem vērā pieejamās tehnoloģijas un ieviešanas izmaksas[577].

6.1.4. Tiesības uz apstrādes ierobežošanu

VDAR 18. pants sniedz datu subjektam tiesības uz laiku ierobežot pārziņa veikto viņa personas datu apstrādi. Datu subjekti var pieprasīt pārzinim ierobežot apstrādi šādos gadījumos:

- tiek apstrīdēta personas datu precizitāte;
- apstrāde ir nelikumīga, un datu subjekts pieprasa ierobežot personas datu izmantošanu, nevis dzēst datus;
- dati ir jāsaglabā, lai īstenotu vai aizstāvētu likumīgas prasības;
- tiek gaidīts lēmums, vai datu pārziņa likumīgās intereses ir svarīgākas par datu subjekta interesēm[578].

Metodes, ar kādām pārzinis var ierobežot personas datu apstrādi, var ietvert, piemēram, izvēlēto datu īslaicīgu pārvietošanu uz citu apstrādes sistēmu, datu padarīšanu lietotājiem nepieejamu vai personas datu pagaidu izņemšanu[579]. Pārzinim jāinformē datu subjekts pirms apstrādes ierobežojuma atcelšanas[580].

577 Vispārīgā datu aizsardzības regula, 17. panta 2. punkts un 66. apsvērums.

578 Turpat, 18. panta 1. punkts.

579 Turpat, 67. apsvērums.

580 Turpat, 18. panta 3. punkts.

Pienākums informēt par personas datu labošanu, dzēšanu vai apstrādes ierobežošanu

Pārzinim ir pienākums informēt par jebkādiem personas datu labojumiem vai dzēšanu vai visiem apstrādes ierobežojumiem katram saņēmējam, kuram pārzinis ir atklājis personas datus, ciktāl tas nav nedz neiespējami, nedz nesamērīgi[581]. Ja datu subjekts pieprasa informāciju par šādiem saņēmējiem, pārzinim ir pienākums sniegt šādu informāciju[582].

6.1.5. Tiesības uz datu pārnesamību

Saskaņā ar VDAR datu subjektiem ir tiesības uz datu pārnesamību situācijās, kad personas dati, kurus viņi ir snieguši pārzinim, tiek apstrādāti, izmantojot automatizētus līdzekļus uz piekrišanas pamata, vai kad personas datu apstrāde ir nepieciešama līguma izpildei un to veic ar automatizētiem līdzekļiem. Tas nozīmē, ka tiesības uz datu pārnesamību nav piemērojamas situācijās, kad personas datu apstrādei ir juridisks pamats, kas nav ne piekrišana, ne līgums[583].

Ja tiesības uz datu pārnesamību ir piemērojamas, datu subjektiem ir tiesības nosūtīt savus personas datus tieši no viena pārziņa otram, ja tas ir tehniski iespējams[584]. Lai to atvieglotu, pārzinim jāizstrādā savstarpēji izmantojami formāti, kas datu subjektiem nodrošina datu pārnesamību[585]. VDAR norādīts, ka šiem formātiem jābūt strukturētiem, plaši izmantotiem un mašīnlasāmiem, lai atvieglotu savietojamību[586]. Savstarpēju izmantojamību var definēt plašā nozīmē kā informācijas sistēmu spēju apmainīties ar datiem un nodrošināt informācijas apmaiņu[587]. Lai gan izmantoto formātu mērķis ir panākt savietojamību, VDAR nav īpaši ieteikumi par konkrētu formātu, kas jānodrošina, jo formāti dažādās nozarēs var atšķirties[588].

Atbilstoši 29. panta darba grupas pamatnostādnēm tiesības uz datu pārnesamību "atbalsta lietotāju izvēli, lietotāju kontroli un patērētāju iespējas", lai sniegtu datu

581 Turpat, 19. pants.

582 Turpat.

583 Turpat, 68. apsvērums un 20. panta 1. punkts.

584 Turpat, 20. panta 2. punkts.

585 Turpat, 68. apsvērums un 20. panta 1. punkts.

586 Turpat, 68. apsvērums.

587 Eiropas Komisija, paziņojums "Spēcīgākas un viedākas robežu un drošības informācijas sistēmas", COM(2016) 205 *final*, 2016. gada 2. aprīlis.

588 29. panta darba grupa (2016), *Pamatnostādnes par tiesībām uz datu pārnesamību*, WP 242, 2016. gada 13. decembris, pārskatītas 2017. gada 5. aprīlī, 13. lpp.

subjektiem kontroli pār viņu pašu personas datiem[589]. Pamatnostādnēs precizēti galvenie datu pārnesamības elementi, kas ietver:

- datu subjektu tiesības saņemt savus personas datus, kurus apstrādā pārzinis, strukturētā, plaši izmantojamā, mašīnlasāmā un savstarpēji izmantojamā formātā;
- tiesības netraucēti pārsūtīt personas datus no viena datu pārziņa citam datu pārzinim, ja tas ir tehniski iespējams;
- kontrolēšanas režīms – kad pārzinis atbild uz datu pārnesamības pieprasījumu, tas rīkojas saskaņā ar datu subjekta norādījumiem, kas nozīmē, ka pārzinis neatbild par saņēmēja atbilstību datu aizsardzības tiesību aktiem, ņemot vērā, ka datu subjekts izlemj, kam dati tiks pārnesti;
- datu pārnesamības tiesību izmantošana neierobežo citas tiesības, tāpat kā attiecībā uz visām pārējām VDAR paredzētajām tiesībām.

6.1.6. Tiesības iebilst

Datu subjekti var atsaukties uz tiesībām iebilst pret personas datu apstrādi, pamatojoties uz viņu īpašo situāciju, kā arī datiem, kas apstrādāti tiešās tirgvedības nolūkos. Tiesības iebilst var īstenot, izmantojot automatizētus līdzekļus.

Tiesības iebilst, pamatojoties uz datu subjekta īpašo situāciju

Datu subjektiem nav vispārēju tiesību iebilst pret savu datu apstrādi[590]. VDAR 21. panta 1. punktā datu subjektam paredzētas tiesības celt iebildumus, pamatojoties uz viņa īpašo situāciju, ja apstrādes juridiskais pamats ir pārziņa izpildīts uzdevums sabiedrības interesēs vai ja apstrāde ir balstīta pārziņa likumīgajās interesēs[591].

589 Turpat.

590 Skatīt arī ECT 1997. gada 27. augusta spriedumu lietā *M.S. pret Zviedriju*, Nr. 20837/92, (par medicīnisko datu paziņošanu bez piekrišanas vai iespējas iebilst); ECT 1987. gada 26. marta spriedumu lietā *Leander pret Zviedriju*, Nr. 9248/81; ECT 2011. gada 10. maija spriedumu lietā *Mosley pret Apvienoto Karalisti*, Nr. 48009/08.

591 Vispārīgā datu aizsardzības regula, 69. apsvērums; 6. panta 1. punkta e) un f) apakšpunkts.

Tiesības iebilst attiecas uz profilēšanas darbībām. Līdzīgas tiesības ir atzītas modernizētajā Konvencijā Nr. 108[592].

Tiesību iebilst, pamatojoties uz iemesliem, kas saistīti ar datu subjekta īpašo situāciju, mērķis ir panākt pareizu līdzsvaru starp datu subjekta datu aizsardzības tiesībām un citu personu likumīgajām tiesībām, apstrādājot viņu datus. Tomēr EST ir paskaidrojusi, ka datu subjekta tiesības "parasti" ir svarīgākas par datu pārziņa ekonomiskajām interesēm atkarībā no "attiecīgās informācijas būtības un tās jutīguma attiecībā pret datu subjekta privāto dzīvi, kā arī sabiedrības interesēm saņemt šo informāciju"[593]. Saskaņā ar VDAR pierādīšanas pienākums ir pārziņiem, kam jāspēj pierādīt pārliecinošu pamatu apstrādes turpināšanai[594]. Tāpat modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā ir paskaidrots, ka datu apstrādes likumīgais pamats (kas var būt svarīgāks par datu subjektu tiesībām iebilst pret apstrādi) jāpierāda katrā atsevišķā gadījumā[595].

Piemērs. Lietā *Manni*[596] EST sprieda, ka personas datu izpaušanas uzņēmumu reģistrā likumīgā mērķa dēļ, jo īpaši pamatojoties uz nepieciešamību aizsargāt trešo personu intereses un nodrošināt juridisko noteiktību, principā *Manni* kungam nebija tiesību panākt viņa personas datu dzēšanu no uzņēmumu reģistra. Tomēr tiesa atzina, ka pastāv tiesības iebilst pret apstrādi, jo "nevar (..) izslēgt, ka varētu pastāvēt īpašas situācijas, kurās ar attiecīgās personas konkrētu gadījumu saistīti nepārvarami un likumīgi iemesli izņēmuma kārtā pamato to, ka piekļuve reģistrā iekļautajiem personas datiem, kas skar attiecīgo personu, beidzoties pietiekami ilgam termiņam (..), tiek ierobežota, sniedzot to tikai trešajām personām, kuras pamato savas īpašās intereses ar tiem iepazīties".

592 Modernizētā Konvencija Nr. 108, 9. panta 1. punkta d) apakšpunkts; Ieteikums par profilēšanu, 5.3. punkts.

593 EST 2014. gada 13. maija spriedums lietā C-131/12 *Google Spain SL un Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 81. punkts.

594 Skatīt arī modernizētās Konvencijas Nr. 108 98. panta 1. punkta d) apakšpunktu, kurā teikts, ka datu subjekts var iebilst pret savu datu apstrādi, "izņemot gadījumus, kad pārzinis uzrāda likumīgu apstrādes iemeslu, kas ir svarīgāks par viņa vai viņas interesēm vai tiesībām un pamatbrīvībām".

595 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 78. punkts.

596 EST 2017. gada 9. marta spriedums lietā C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce pret Salvatore Manni*, 47. un 60. pants.

EST uzskatīja, ka katra gadījuma izvērtēšana, ņemot vērā visus attiecīgos indivīda apstākļus un to, vai pastāv likumīgi un svarīgāki iemesli, kas izņēmuma kārtā varētu attaisnot trešo personu ierobežotu piekļuvi uzņēmumu reģistros esošajiem personas datiem, ir valstu tiesu atbildība. Tomēr tiesa precizēja, ka *Manni* kunga gadījumā faktu, ka viņa personas datu izpaušana reģistrā, iespējams, ietekmēja viņa klientūru, nevar uzskatīt par šādu likumīgu un nepārvaramu iemeslu. Potenciālajiem *Manni* kunga klientiem ir likumīgas intereses piekļūt informācijai par viņa iepriekšējā uzņēmuma bankrotu.

Pamatota iebilduma rezultātā pārzinis vairs nedrīkst apstrādāt attiecīgos datus. Apstrādes darbības, kas veiktas ar datu subjekta datiem pirms iebilduma, joprojām ir likumīgas.

Tiesības iebilst pret datu apstrādi tiešās tirgvedības nolūkos

VDAR 21. panta 2. punktā paredzētas īpašas tiesības iebilst pret personas datu izmantošanu tiešās tirgvedības nolūkos, papildus precizējot E-privātuma direktīvas 13. pantu. Šādas tiesības ir noteiktas arī modernizētajā Konvencijā Nr. 108, kā arī EP Ieteikumā par tiešo tirgvedību[597]. Modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā ir paskaidrots, ka iebildumu pret datu apstrādi tiešās tirgvedības nolūkos rezultātā attiecīgie personas dati ir jādzēš vai jāizņem bez papildu nosacījumiem[598].

Datu subjektam ir tiesības jebkurā laikā un bez maksas iebilst pret savu personas datu izmantošanu tiešās tirgvedības nolūkos. Datu subjekti ir skaidri jāinformē par šīm tiesībām, atsevišķi no citas sniegtās informācijas.

Tiesības iebilst, izmantojot automatizētus līdzekļus

Ja personas informāciju izmanto un apstrādā informācijas sabiedrības pakalpojumiem, datu subjekts var izmantot savas tiesības iebilst pret savu personas datu apstrādi, izmantojot automatizētus līdzekļus.

597 Eiropas Padomes Ministru komiteja (1985), Ieteikums Nr. Rec(85)20 dalībvalstīm par personas datu aizsardzību, ko izmanto tiešās tirgvedības nolūkos, 1985. gada 25. oktobris, 4. punkta 1. apakšpunkts.

598 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 79. punkts.

Informācijas sabiedrības pakalpojumi ir definēti kā "jebkāds pakalpojums, ko parasti sniedz par atlīdzību no attāluma, ar elektroniskiem līdzekļiem un pēc pakalpojumu saņēmēja individuāla pieprasījuma"[599].

Datu pārziņiem, kuri piedāvā informācijas sabiedrības pakalpojumus, jāievieš attiecīgi tehniskie noteikumi un procedūras, lai nodrošinātu iespēju efektīvi īstenot tiesības iebilst, izmantojot automatizētus līdzekļus[600]. Piemēram, tie var ietvert sīkdatņu bloķēšanu tīmekļa vietnēs vai interneta pārlūkošanas izsekošanas izslēgšanu.

Tiesības iebilst pret apstrādi zinātniskās vai vēstures pētniecības nolūkos, kā arī statistikas nolūkos

Saskaņā ar ES tiesību aktiem zinātniskā pētniecība ir jāinterpretē plaši, iekļaujot, piemēram, tehnoloģiju attīstību un demonstrēšanu, fundamentālos zinātnes pētījumus, lietišķos pētījumus un privāti finansētus pētījumus[601]. Vēstures pētījumos ietilpst arī pētījumi ģenealoģiskos nolūkos, paturot prātā, ka regulu nepiemēro mirušām personām[602]. Statistikas nolūki ir jebkura tādu personas datu vākšanas un apstrādes darbība, kuri nepieciešami statistikas apsekojumiem vai statistikas rezultātu izstrādei[603]. Atkal datu subjekta īpašā situācija ir juridiskais pamats tiesībām iebilst pret personas datu apstrādi pētniecības nolūkos[604]. Vienīgais izņēmums ir apstrādes nepieciešamība, lai izpildītu uzdevumu, kas veikts sabiedrības interesēs. Tomēr tiesības dzēst datus nepiemēro, ja apstrāde ir nepieciešama (ar vai bez sabiedriskas nozīmes apsvērumiem) zinātniskās vai vēstures pētniecības nolūkos vai statistikas nolūkos[605].

VDAR 89. pantā līdzsvarotas zinātniskās, statistikas vai vēstures pētniecības prasības un datu subjektu tiesības ar īpašiem aizsardzības pasākumiem un atkāpēm no tām. Tādējādi Savienības vai dalībvalstu tiesību aktos var paredzēt atkāpes no tiesībām iebilst, ciktāl šādas tiesības var padarīt neiespējamu vai nopietni apdraudēt pētniecības mērķu sasniegšanu, un ja šādas atkāpes ir vajadzīgas šo mērķu sasniegšanai.

599 Direktīva 98/34/EK, kas grozīta ar Direktīvu 98/48/EK, ar ko nosaka informācijas sniegšanas kārtību tehnisko standartu un noteikumu jomā, 1. panta 2. punkts.

600 Vispārīgā datu aizsardzības regula, 21. panta 5. punkts.

601 Turpat, 159. apsvērums.

602 Turpat, 160. apsvērums.

603 Turpat, 162. apsvērums.

604 Turpat, 21. panta 6. punkts.

605 Turpat, 17. panta 3. punkta d) apakšpunkts.

Saskaņā ar **EP tiesību aktiem** modernizētās Konvencijas Nr. 108 9. panta 2. punktā noteikts, ka likumos par datu apstrādi arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos vai statistikas nolūkos var tikt noteikti ierobežojumi datu subjektu tiesībām, tostarp tiesībām iebilst, ja nav redzamu datu subjektu tiesību un pamatbrīvību pārkāpuma risku.

Tomēr skaidrojošajā ziņojumā (41. punkts) arī atzīts, ka datu subjektiem vajadzētu būt iespējai dot piekrišanu tikai noteiktās pētniecības jomās vai pētniecības projektu daļām, ciktāl to atļauj paredzētais nolūks, un tiesībām iebilst, ja viņi uztver apstrādi pārmērīgu iejaukšanos viņu tiesībās un brīvībās bez likumīga pamata.

Citiem vārdiem sakot, šāda apstrāde tādējādi tiek uzskatīta par *a priori* saderīgu ar nosacījumu, ka pastāv citi aizsardzības pasākumi un ja darbības principā izslēdz jebkādu iegūtās informācijas izmantošanu lēmumu pieņemšanai vai pasākumiem, kas skar konkrētu personu.

6.1.7. Automatizēta individuālo lēmumu pieņemšana, tostarp profilēšana

Automatizēti lēmumi ir lēmumi, kas tiek pieņemti, izmantojot personas datus, kurus apstrādā tikai ar automatizētiem līdzekļiem, bez jebkādas cilvēka līdzdalības. **Saskaņā ar ES tiesību aktiem** uz datu subjektiem nedrīkst attiecināt automatizētus lēmumus, kas rada juridiskas vai līdzīgas nozīmības sekas. Ja šādi lēmumi, iespējams, būtiski ietekmē indivīdu dzīvi, jo tie ir saistīti, piemēram, ar kredītspēju, elektronisku darbā pieņemšanu, sniegumu darbā, uzvedības vai uzticamības analīzi, tad, lai izvairītos no negatīvām sekām, ir nepieciešama īpaša aizsardzība. Automatizētā lēmumu pieņemšana ietver profilēšanu, kurā jebkādā veidā automatizēti vērtē "ar fizisku personu saistītus personiskus aspektus, lai jo īpaši analizētu vai prognozētu aspektus saistībā ar datu subjekta sniegumu darbā, ekonomisko situāciju, veselību, personīgām vēlmēm vai interesēm, uzticamību vai uzvedību, atrašanās vietu vai pārvietošanos"[606].

Piemērs. Lai ātri novērtētu topošā klienta kredītspēju, kredītinformācijas aģentūras (*CRA*) apkopo noteiktus datus, piemēram, kā klients ir uzturējis savus kredīta un pakalpojumu/komunālo pakalpojumu kontus, ziņas par klienta iepriekšējām adresēm, kā arī informāciju no publiski pieejamiem avotiem, piemēram, vēlētāju sarakstu, publiskos ierakstus (tostarp tiesas

606 Turpat, 71. apsvērums, 4. panta 4. punkts un 22. pants.

spriedumus) vai datus par bankrotu un maksātnespēju. Pēc tam šie personas dati tiek ievadīti vērtēšanas algoritmā, kura aprēķinātā kopējā vērtība atspoguļo potenciālā klienta kredītspēju.

Atbilstoši 29. panta darba grupu viedoklim tiesības netikt pakļautam lēmumiem, kuru pamatā ir tikai automatizēta apstrāde, kas datu subjektam var radīt juridiskas sekas vai viņu būtiski ietekmēt, ir pielīdzināms vispārīgam aizliegumam un datu subjektam nav proaktīvi jāmeklē iebildumi pret šādu lēmumu[607].

Tomēr atbilstoši VDAR automatizēta lēmumu pieņemšana, kam ir juridiskas sekas vai kas būtiski ietekmē indivīdus, var būt pieņemama, ja tā ir nepieciešama līguma starp datu pārzini un datu subjektu noslēgšanai vai līguma izpildei vai ja datu subjekts ir devis nepārprotamu piekrišanu. Automatizēta lēmumu pieņemšana ir pieņemama arī tad, ja to atļauj likums un ja datu subjekta tiesības, brīvības un leģitīmās intereses tiek pienācīgi aizsargātas[608].

VDAR arī paredzēts, ka pārziņa pienākumos attiecībā uz informāciju, kas sniedzama, vācot personas datus, ietilpst arī datu subjektu informēšana par automatizētas lēmumu pieņemšanas, tostarp profilēšanas, esamību[609]. Tiesības piekļūt pārziņa apstrādātajiem personas datiem netiek skartas[610]. Informācijā ir jānorāda ne tikai tas, ka profilēšana tiks veikta, tai vajadzētu saturēt arī jēgpilnu informāciju par profilēšanā izmantoto loģiku un apstrādes paredzamajām sekām uz indivīdiem[611]. Piemēram, veselības apdrošināšanas sabiedrībai, kas izmanto automatizētu lēmumu pieņemšanu pieteikumu izskatīšanā, datu subjektiem ir jāsniedz vispārīga informācija par to, kā algoritms strādā un kādus faktorus algoritmā izmanto, aprēķinot viņu apdrošināšanas prēmijas. Tāpat, izmantojot savas "piekļuves tiesības", datu subjekti var pieprasīt pārzini sniegt informāciju par automatizētu lēmumu pieņemšanu, kā arī jēgpilnu informāciju par izmantoto loģiku[612].

Datu subjektiem sniegtā informācija ir paredzēta, lai nodrošinātu pārredzamību un ļautu datu subjektiem sniegt apzinātu piekrišanu, ja viņi piekrīt, vai arī panāktu cilvēka līdzdalību. Datu pārzinim jāievieš atbilstoši pasākumi, lai aizsargātu datu

607 29. panta darba grupa, *Pamatnostādnes par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem*, WP 251, 2017. gada 3. oktobris, 15. lpp.

608 Vispārīgā datu aizsardzības regula, 22. panta 2. punkts.

609 Turpat, 12. pants.

610 Turpat, 15. pants.

611 Turpat, 13. panta 2. punkta f) apakšpunkts.

612 Turpat, 15. panta 1. punkta h) apakšpunkts.

subjekta tiesības, brīvības un leģitīmās intereses. Tiem jāietver vismaz tiesības uz cilvēka līdzdalību no pārziņa puses un datu subjekta iespēju paust viedokli un apstrīdēt lēmumu, kura pamatā ir viņa personas datu automatizēta apstrāde[613].

29. panta darba grupa ir sniegusi papildu norādījumus par automatizētas lēmumu pieņemšanas izmantošanu saskaņā ar VDAR[614].

Saskaņā ar EP tiesību aktiem indivīdiem ir tiesības netikt pakļautiem lēmumiem, kam būs būtiska ietekme uz viņiem un kuru pamatā ir tikai automatizēta apstrāde, neņemot vērā viņu viedokli[615]. Prasība ņemt vērā datu subjekta viedokli gadījumos, kad lēmumi ir balstīti tikai uz automatizētu apstrādi, nozīmē, ka viņiem ir tiesības apstrīdēt šādus lēmumus un vajadzētu būt iespējai apstrīdēt jebkādas pārziņa izmantoto personas datu neprecizitātes, kā arī apstrīdēt uz viņiem attiecinātā profila piemērotību[616]. Tomēr indivīds nevar izmantot šīs tiesības, ja automatizēta lēmumu pieņemšana atļauta ar likumu, ko piemēro pārzinim un kurā arī paredzēti piemēroti pasākumi, lai aizsargātu datu subjekta tiesības, brīvības un leģitīmas intereses. Turklāt datu subjektiem ir tiesības pēc pieprasījuma saņemt informāciju par veiktās datu apstrādes pamatojumu[617]. Modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā sniegts kredītspējas novērtējuma piemērs. Personām vajadzētu būt tiesīgām uzzināt ne tikai pašu pozitīvo vai negatīvo lēmumu par vērtējumu, bet arī *loģiku*, kas ir viņu personas datu apstrādes pamatā, kā rezultātā ticis pieņemts šāds lēmums. "Izpratne par šiem elementiem veicina citu būtisku drošības pasākumu īstenošanu, piemēram, tiesību iebilst un tiesību iesniegt sūdzību kompetentajai iestādei, efektīvu izmantošanu"[618].

Ieteikumā par profilēšanu, kaut arī tas nav juridiski saistošs, precizēti personas datu vākšanas un apstrādes nosacījumi saistībā ar profilēšanu[619]. Tas ietver noteikumus attiecībā uz nepieciešamību nodrošināt, ka apstrāde profilēšanas kontekstā ir godprātīga, likumīga, samērīga un veikta konkrētiem un likumīgiem mērķiem. Šeit

613 Turpat, 22. panta 3. punkts.

614 29. panta darba grupa (2017), *Pamatnostādnes par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem*, WP 251, 2017. gada 3. oktobris.

615 Modernizētā Konvencija Nr. 108, 9. panta 1. punkta a) apakšpunkts.

616 Modernizētās konvencijas Nr. 108 skaidrojošais ziņojums, 75. punkts

617 Modernizētā Konvencija Nr. 108, 9. panta 1. punkta c) apakšpunkts.

618 Modernizētās konvencijas Nr. 108 skaidrojošais ziņojums, 77. punkts

619 Eiropas Padome, Ministru komitejas Ieteikums CM/Rec(2010)13 dalībvalstīm par fizisko personu aizsardzību attiecībā uz personas datu automātisku apstrādi datu profilu veidošanas kontekstā, 5. punkta 5. apakšpunkts.

iekļauti arī noteikumi par informāciju, kas pārziņiem ir jāsniedz datu subjektiem. Ieteikumā ietverts arī datu kvalitātes princips, saskaņā ar kuru pārziņiem jāveic pasākumi, lai labotu datu neprecizitātes faktorus, ierobežotu riskus vai kļūdas, ko var radīt profilēšana, un periodiski novērtētu izmantoto datu un algoritmu kvalitāti.

6.2. Tiesiskās aizsardzības līdzekļi, atbildība, sodi un kompensācija

Svarīgākie aspekti

- Saskaņā ar modernizēto Konvenciju Nr. 108 līgumslēdzēju pušu tiesību aktos jāparedz attiecīgi tiesiskās aizsardzības līdzekļi un sankcijas par datu aizsardzības tiesību pārkāpumiem.
- ES tiesiskās aizsardzības līdzekļi datu subjektiem viņu tiesību pārkāpuma gadījumos, kā arī sankcijas pret pārziņiem un apstrādātājiem, kuri neievēro regulas noteikumus, ir paredzēti VDAR. Regulā arī paredzētas tiesības uz kompensāciju un atbildība.
    - Datu subjektiem ir tiesības iesniegt sūdzību uzraudzības iestādei par iespējamiem regulas pārkāpumiem, kā arī tiesības uz efektīvu tiesisko aizsardzību un kompensāciju.
    - Īstenojot savas tiesības uz efektīvu tiesisko aizsardzību, personas var pārstāvēt bezpeļņas organizācijas, kas darbojas datu aizsardzības jomā.
    - Pārzinis vai apstrādātājs ir atbildīgs par jebkādiem no pārkāpuma izrietošiem materiālajiem un morālajiem zaudējumiem.
    - Uzraudzības iestādēm ir tiesības piemērot administratīvus naudas sodus par regulas pārkāpumiem līdz pat 20 000 000 EUR apmērā vai, ja pārkāpējs ir uzņēmums, 4 % no kopējā apgrozījuma gadā globālā līmenī: atkarībā no tā, kurš ir lielāks.
- Datu subjektiem kā galējais līdzeklis un ar zināmiem nosacījumiem ir iespēja iesniegt datu aizsardzības tiesību aktu pārkāpumus izskatīšanai ECT.
- Ikvienai fiziskai vai juridiskai personai ir tiesības iesniegt sūdzību EST par jebkuru Eiropas Datu aizsardzības kolēģijas lēmumu saskaņā ar Līgumos paredzētajiem nosacījumiem.

Tikai tiesību instrumentu pieņemšana nav pietiekama, lai Eiropā nodrošinātu personas datu aizsardzību. Lai Eiropas datu aizsardzības noteikumi būtu efektīvi, ir jāizveido mehānismi, kas ļauj indivīdiem cīnīties pret viņu tiesību pārkāpumiem un

pieprasīt kompensāciju par nodarīto kaitējumu. Tāpat ir svarīgi, lai uzraudzības iestādēm būtu pilnvaras piemērot sankcijas, kas ir efektīvas, preventīvas un samērīgas ar attiecīgo pārkāpumu.

Datu aizsardzības tiesību aktos noteiktās tiesības var izmantot persona, kuras tiesības ir apdraudētas. Šī persona būs datu subjekts. Tomēr arī citas personas, kuras atbilst valstu tiesību aktos noteiktajām prasībām, var pārstāvēt datu subjektus, kuri īsteno savas tiesības. Saskaņā ar vairākiem valstu tiesību aktiem aizbildņi pārstāv bērnus un personas ar intelektuālās attīstības traucējumiem[620]. Saskaņā ar ES tiesību aktiem datu aizsardzības jomā apvienība, kuras likumīgais mērķis ir datu aizsardzības tiesību veicināšana, var pārstāvēt datu subjektus uzraudzības iestādē vai tiesā[621].

6.2.1. Tiesības iesniegt sūdzību uzraudzības iestādē

Saskaņā gan ar **ES**, gan **EP tiesību aktiem** indivīdiem ir tiesības iesniegt pieprasījumus un sūdzības kompetentajai uzraudzības iestādei, ja viņi uzskata, ka viņu personas datu apstrāde netiek veikta atbilstoši likumam.

Modernizētajā Konvencijā Nr. 108 atzītas datu subjektu tiesības saņemt uzraudzības iestādes palīdzību, izmantojot savas konvencijā noteiktās tiesības, neatkarīgi no viņu valstspiederības vai dzīvesvietas[622]. Palīdzības pieprasījumu var noraidīt tikai izņēmuma gadījumos, un datu subjektiem nav jāsedz ar palīdzību saistītās izmaksas un nodevas[623].

Līdzīgi nosacījumi ir arī ES tiesību sistēmā. VDAR ietverta prasība uzraudzības iestādēm veikt pasākumus, lai atvieglotu sūdzību iesniegšanu, piemēram, elektroniskas sūdzību iesniegšanas veidlapas izveide[624]. Datu subjekts var iesniegt sūdzību uzraudzības iestādē dalībvalstī, kurā atrodas viņa pastāvīgā dzīvesvieta, darba vieta vai iespējamā pārkāpuma izdarīšanas vieta[625]. Sūdzības ir jāizmeklē, un uzraudzības

620 *FRA* (2015), Rokasgrāmata par Eiropas tiesību aktiem bērnu tiesību jomā, Luxembourg, Publications Office; *FRA* (2013), Legal capacity of persons with intellectual disabilities and persons with mental health problems, Luxembourg, Publications Office.

621 Vispārīgā datu aizsardzības regula, 80. pants.

622 Modernizētā Konvencija Nr. 108, 18. pants.

623 Turpat, 16.–17. pants.

624 Vispārīgā datu aizsardzības regula, 57. panta 2. punkts.

625 Turpat, 77. panta 1. punkts.

iestādei ir pienākums informēt attiecīgo personu par tiesvedības iznākumu saistībā ar prasību[626].

Par iespējamiem ES iestāžu vai struktūru pārkāpumiem var informēt Eiropas Datu aizsardzības uzraudzītāju[627]. Ja atbildi no EDAU nesaņem sešu mēnešu laikā, sūdzību uzskata par noraidītu. Apelācijas par EDAU lēmumiem var iesniegt EST saskaņā ar Regulu (EK) Nr. 45/2001, ar ko ES iestādēm un struktūrām uzliek pienākumu ievērot datu aizsardzības noteikumus.

Ir jābūt iespējai pārsūdzēt tiesās valsts uzraudzības iestādes lēmumus. Tas attiecas gan uz datu subjektu, gan arī uz pārziņiem un apstrādātājiem, kuri ir bijuši uzraudzības iestādes procesa dalībnieki.

Piemērs. Spānijas Datu aizsardzības aģentūra 2017. gada septembrī piemēroja naudas sodu *Facebook* par vairāku datu aizsardzības noteikumu pārkāpšanu. Uzraudzības iestāde sodīja sociālo tīklu par personas datu, tostarp īpašu kategoriju personas datu, vākšanu, glabāšanu un apstrādi reklāmas nolūkos un bez datu subjekta piekrišanas. Lēmuma pamatā bija pēc uzraudzības iestādes iniciatīvas veikta izmeklēšana.

6.2.2. Tiesības uz efektīvu tiesību aizsardzību tiesā

Papildus tiesībām iesniegt sūdzību uzraudzības iestādē, indivīdiem jābūt tiesībām uz efektīvu tiesisko aizsardzību un tiesībām iesniegt prasību izskatīšanai tiesā. Tiesības uz tiesiskās aizsardzības līdzekļiem ir labi nostiprinātas Eiropas tiesību tradīcijās, un tās ir atzītas par pamattiesībām gan saskaņā ar ES Pamattiesību hartas 47. pantu, gan ECTK 13. pantu[628].

ES tiesību aktos datu subjektu nodrošināšanas ar efektīviem tiesiskās aizsardzības līdzekļiem, ja tiek pārkāptas viņu tiesības, nozīmīgums izriet gan no VDAR noteikumiem, kuros paredzētas tiesības uz efektīvu tiesisko aizsardzību pret uzraudzības iestādēm, pārziņiem un apstrādātājiem, gan no EST judikatūras.

626 Turpat, 77. panta 2. punkts.

627 Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti, OV 2001 L 8.

628 Skatīt, piemēram, ECT 2016. gada 7. jūnija spriedumu lietā *Karabeyoğlu pret Turciju*, Nr. 30083/10; ECT 2017. gada 18. jūlija spriedumu lietā *Mustafa Sezgin Tanrıkulu pret Turciju*, Nr. 27473/06.

Piemērs. Lietā *Schrems*[629] EST pasludināja lēmumu par datu aizsardzības līmeņa pietiekamību attiecībā uz drošības zonu par spēkā neesošu. Šis lēmums ļāva veikt starptautisku datu nosūtīšanu no ES uz organizācijām ASV, kuras ir sevis sertificētas saskaņā ar drošības zonas shēmu. EST uzskatīja, ka drošības zonas shēmai ir vairāki trūkumi, kas apdraudēja ES pilsoņu pamattiesības uz privātās dzīves aizsardzību, personas datu aizsardzību, kā arī tiesības uz efektīvu tiesisko aizsardzību.

Attiecībā uz tiesību uz privātumu un datu aizsardzību pārkāpumiem EST uzsvēra, ka ASV tiesību akti atļauj noteiktām publiskām iestādēm piekļūt personas datiem, kas nosūtīti no dalībvalstīm uz ASV, un tos apstrādāt veidā, kāds nav savienojams ar sākotnējiem nosūtīšanas mērķiem un pārsniedz to, kas ir noteikti nepieciešami un samērīgi valsts drošības aizsardzībai. Saistībā ar tiesībām uz efektīvu tiesisko aizsardzību tiesa atzīmēja, ka datu subjektiem nebija ne administratīvu, ne tiesisku tiesiskās aizsardzības līdzekļu, lai atkarībā no situācijas varētu piekļūt datiem, kas uz viņiem attiecas, tos labot vai dzēst. EST secināja, ka tiesību aktos, kuros nav paredzētas nekādas iespējas izmantot tiesiskus aizsardzības līdzekļus, lai piekļūtu personas datiem, labotu vai dzēstu tos, "nav ņemta vērā Hartas 47. pantā iedibināto pamattiesību uz efektīvu aizsardzību tiesā būtība". Tā uzsvēra, ka tiesiskumam ir raksturīga tiesiskās aizsardzības iespēja, ar ko garantē tiesību normu ievērošanu.

Personas, pārziņi vai apstrādātāji, kuri vēlas apstrīdēt uzraudzības iestādes juridiski saistošu lēmumu, var iesniegt prasības pieteikumu tiesā[630]. Termins "lēmums" ir jāinterpretē plaši, aptverot uzraudzības iestāžu pilnvaras veikt izmeklēšanu, piemērot sankcijas un piešķirt atļaujas, kā arī pieņemt lēmumus par sūdzības pieņemšanas atteikšanu vai noraidīšanu. Tomēr juridiski nesaistoši pasākumi, piemēram, uzraudzības iestādes sniegtie atzinumi vai ieteikumi, nevar būt prasības priekšmets tiesā[631]. Prasības pieteikums jāiesniedz tās dalībvalsts tiesās, kurā atrodas attiecīgā uzraudzības iestāde[632].

629 EST 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems pret Datu aizsardzības komisāru* [GC].

630 Vispārīgā datu aizsardzības regula, 78. pants.

631 Turpat, 143. apsvērums.

632 Turpat, 78. panta 3. punkts.

Gadījumos, kad pārzinis vai apstrādātājs pārkāpj datu subjekta tiesības, datu subjektiem ir tiesības iesniegt sūdzību tiesā[633]. Tiesvedībā, kas uzsākta pret pārzini vai apstrādātāju, ir īpaši svarīgi, lai indivīdiem būtu iespēja izvēlēties, kur iesniegt prasības pieteikumu. Viņi var izvēlēties to darīt vai nu dalībvalstī, kurā atrodas pārziņa vai apstrādātāja uzņēmums, vai arī dalībvalstī, kurā atrodas attiecīgo datu subjektu pastāvīgā dzīvesvieta[634]. Otrā iespēja indivīdiem ievērojami atvieglo viņu tiesību īstenošanu, jo dod iespēju celt prasību valstī, kurā viņi dzīvo, un zināmā jurisdikcijā. Ierobežojot tiesvedības uzsākšanas pret pārziņiem un apstrādātājiem vietu, attiecinot to tikai uz dalībvalsti, kurā ir to juridiskā adrese, varētu atturēt datu subjektus, kuri dzīvo citās dalībvalstīs, iesniegt prasības pieteikumu tiesā, jo tas būtu saistīts ar ceļa un papildu izmaksām, un tiesvedība, iespējams, notiktu svešvalodā un svešā jurisdikcijā. Vienīgais izņēmums attiecas uz gadījumiem, kad pārzinis vai apstrādātājs ir publiskas iestādes un apstrāde tiek veikta, īstenojot viņu publiskās pilnvaras. Šajā gadījumā tikai attiecīgās publiskās iestādes valsts tiesas ir kompetentas izskatīt prasību[635].

Lai gan vairumā gadījumu lietas par datu aizsardzības noteikumiem tiks izlemtas dalībvalstu tiesās, dažas lietas var tikt iesniegtas izskatīšanai EST. Pirmā iespēja ir tad, ja datu subjekts, pārzinis, apstrādātājs vai uzraudzības iestāde ceļ prasību atcelt EDAK lēmumu. Tomēr uz prasību attiecas LESD 263. panta nosacījumi, kas nozīmē, ka šīm personām un organizācijām, lai prasība būtu pieņemama, ir jāpierāda, ka kolēģijas lēmums viņus skar tieši un individuāli.

Otrais scenārijs attiecas uz gadījumiem, kad ES iestādes vai struktūras veic nelikumīgu personas datu apstrādi. Gadījumos, kad ES iestādes pārkāpj datu aizsardzības tiesību aktus, datu subjekti var celt prasību tieši ES Vispārējā tiesā (Vispārējā tiesa ietilpst EST). Vispārējā tiesa, kā pirmā instance, ir atbildīga par sūdzībām par ES institūciju izdarītiem ES tiesību aktu pārkāpumiem. Tādējādi arī sūdzības par EDAU kā par ES iestādi var tikt iesniegtas Vispārējā tiesā[636].

Piemērs. Lietā *Bavarian Lager*[637] uzņēmums lūdza Eiropas Komisiju nodrošināt piekļuvi pilnam Komisijas rīkotās sanāksmes protokolam, kas, iespējams, bija saistīts ar juridiskiem jautājumiem, kuri skāra uzņēmumu. Komisija noraidīja

633 Turpat, 79. pants.

634 Turpat, 79. panta 2. punkts.

635 Turpat.

636 Regula (EK) Nr. 45/2001, 32. panta 3. punkts.

637 EST lieta C-28/08 P *Eiropas Komisija pret The Bavarian Lager Co. Ltd* [GC], 2010.

uzņēmuma piekļuves pieprasījumu, pamatojoties uz datu aizsardzības interesēm, kas ir svarīgākas[638]. Atbilstoši ES iestāžu datu aizsardzības regulas 32. pantam *Bavarian Lager* šo lēmumu pārsūdzēja Pirmās instances tiesā (Vispārējās tiesas priekštecē). Savā lēmumā (lieta T-194/04, *The Bavarian Lager Co. Ltd pret Eiropas Kopienu Komisiju*) Pirmās instances tiesa atcēla Komisijas lēmumu noraidīt pieprasījumu nodrošināt piekļuvi. Eiropas Komisija šo lēmumu pārsūdzēja EST.

EST izdeva spriedumu (virspalātā), atceļot Pirmās instances tiesas spriedumu un apstiprinot Eiropas Komisijas lūguma piekļūt pilnam sanāksmes protokolam noraidījumu, lai aizsargātu to personu personas datus, kuras piedalījušās sanāksmē. EST uzskatīja, ka Komisija ir pareizi rīkojusies, atsakoties izpaust šo informāciju, ņemot vērā, ka dalībnieki nebija devuši piekrišanu viņu personas datu izpaušanai. Turklāt *Bavarian Lager* nebija pierādījis nepieciešamību piekļūt šai informācijai.

Visbeidzot, datu subjekti, uzraudzības iestādes, pārziņi vai apstrādātāji valsts tiesvedības gaitā var pieprasīt valsts tiesu lūgt EST skaidrot ES iestāžu, struktūru, biroju vai aģentūru aktu interpretāciju un spēkā esamību. Šādus skaidrojumus sauc par prejudiciālajiem nolēmumiem. Tas nav tiešs tiesiskās aizsardzības līdzeklis sūdzības iesniedzējam, bet tas dod iespēju valstu tiesām nodrošināt, ka tās pareizi interpretē ES tiesību aktus. Tieši ar šā prejudiciālā nolēmuma mehānisma starpniecību svarīgas lietas, piemēram, *Digital Rights Ireland* un Kärntner Landesregierung un citi[639] un *Schrems*[640], kuras turpmāk būtiski ietekmēja ES datu aizsardzības tiesību aktu attīstību, nonāca EST.

Piemērs. *Digital Rights Ireland* un *Kärntner Landesregierung un citi*[641] bija apvienota lieta, ko iesniedza Īrijas Augstākā tiesa un Austrijas Konstitucionālā tiesa par Direktīvas 2006/24/EK (Datu saglabāšanas direktīva) atbilstību ES

638 Argumenta analīzei skatīt EDAU detalizētās apspriedes (2011), *Publiska piekļuve dokumentiem, kas satur personas datus pēc nolēmuma lietā* Bavarian Lager, Brisele, EDAU

639 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C-293/12 un C-594/12 *Digital Rights Ireland Ltd pret Minister for Communications, Marine and Natural Resources un citiem un Kärntner Landesregierung un citiem* [GC].

640 EST 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems pret Datu aizsardzības komisāru* [GC].

641 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C-293/12 un C-594/12 *Digital Rights Ireland Ltd pret Minister for Communications, Marine and Natural Resources un citiem* un Kärntner Landesregierung un citiem [GC].

tiesību aktiem datu aizsardzības jomā. Austrijas Konstitucionālā tiesa uzdeva EST jautājumus par Direktīvas 2006/24/EK 3. līdz 9. panta spēkā esamību, ņemot vērā ES Pamattiesību hartas 7., 9. un 11. pantu. Tostarp, vai atsevišķas Austrijas Federālā telekomunikāciju likuma, ar ko transponē Datu saglabāšanas direktīvu, normas ir savietojamas ar bijušās Datu aizsardzības direktīvas un ES institūciju datu aizsardzības regulas aspektiem.

Lietā *Kärntner Landesregierung un citi Seitlinger* kungs, būdams viens no prasības iesniedzējiem Konstitucionālās tiesas procesā, apgalvoja, ka viņš tālruni, internetu un e-pastu izmanto gan darba vajadzībām, gan privātajai dzīvei. Rezultātā viņa nosūtītā un saņemtā informācija tika nodota, izmantojot publiski pieejamus telekomunikāciju tīklus. Saskaņā ar Austrijas 2003. gada Telekomunikāciju likumu viņa telekomunikāciju pakalpojumu sniedzējam bija likumā noteikts pienākums vākt un glabāt datus par tīkla izmantošanu. *Seitlinger* kungs uzskatīja, ka šī viņa personas datu vākšana un glabāšana nav nepieciešama tehniskajiem informācijas nosūtīšanas un saņemšanas caur tīklu nolūkiem. Patiešām, šo datu vākšana un glabāšana nebija nepieciešama rēķinu sagatavošanai. *Seitlinger* kungs paziņoja, ka viņš nav piekritis šādai viņa personas datu izmantošanai, kuri tika vākti un glabāti, tikai pamatojoties uz 2003. gada Austrijas Telekomunikāciju likumu.

Tādēļ *Seitlinger* kungs iesniedza prasības pieteikumu Austrijas Konstitucionālajā tiesā, kurā apgalvoja, ka telekomunikāciju pakalpojumu sniedzēja likumiskie pienākumi pārkāpj viņa pamattiesības saskaņā ar ES Pamattiesību hartas 8. pantu. Tā kā ar Austrijas tiesību aktiem tika īstenoti ES tiesību akti (toreizējā Datu saglabāšanas direktīva), Austrijas Konstitucionālā tiesa nodeva lietu EST, lūdzot lemt, vai direktīva ir savietojama ar ES Pamattiesību hartā noteiktajām tiesībām uz privātumu un datu aizsardzību.

EST virspalāta izlēma lietu, kā rezultātā tika atcelta ES Datu saglabāšanas direktīva. EST secināja, ka direktīva īpaši nopietni iejaucas privātās dzīves un datu aizsardzības pamattiesībās, neierobežojot to līdz noteikti nepieciešamajam. Direktīvai bija leģitīms mērķis, jo tā deva valstu iestādēm papildu iespējas izmeklēt smagus noziegumus un saukt pie atbildības par tiem, līdz ar to tā bija vērtīgs kriminālizmeklēšanas līdzeklis. Tomēr EST atzīmēja, ka pamattiesību ierobežojumi ir jāpiemēro tikai tad, ja tas ir noteikti nepieciešams, un tie ir jāpapildina ar skaidriem un precīziem noteikumiem par to piemērošanas jomu, kā arī aizsardzības pasākumiem indivīdiem.

> EST uzskatīja, ka direktīva neatbilst šim nepieciešamības testam. Tajā nebija noteikti skaidri un precīzi noteikumi, ar ko ierobežo iejaukšanās apmēru. Tā vietā, lai izvirzītu prasību par saistību starp saglabātajiem datiem un smago noziegumu, direktīva tika piemērota visiem visu elektroniskās komunikācijas līdzekļu lietotāju metadatiem. Tādējādi tā bija iejaukšanās praktiski visu ES iedzīvotāju tiesībās uz privātumu un datu aizsardzību, ko varēja uzskatīt par nesamērīgu. Nebija ietverti nosacījumi, ar ko ierobežotu to personu loku, kurām ir atļauts piekļūt personas datiem, un uz šādu piekļuvi netika attiecināti procesuālie nosacījumi, piemēram, prasība pirms piekļuves saņemt administratīvas iestādes vai tiesas atļauju. Visbeidzot, direktīvā nebija noteikti skaidri aizsardzības pasākumi saglabāto datu aizsardzībai. Līdz ar to tā nenodrošināja efektīvu datu aizsardzību pret ļaunprātīgas izmantošanas risku, kā arī pret jebkādu nelikumīgu piekļuvi datiem un to nelikumīgu izmantošanu[642].

Parasti EST ir jāatbild uz uzdotajiem jautājumiem, un tā nevar atteikties sniegt prejudiciālu nolēmumu, pamatojoties uz to, ka šī atbilde nav ne būtiska, ne savlaicīga attiecībā uz sākotnējo lietu. Tomēr tiesa var atteikties, ja jautājums nav tās kompetencē[643]. EST pieņem lēmumu tikai par lūgumu sniegt prejudiciālu nolēmumu veidojošajiem elementiem, savukārt valsts tiesas kompetencē ir izlemt sākotnējo lietu[644].

Saskaņā ar EP tiesību aktiem līgumslēdzējām pusēm jāizveido atbilstoši tiesiskās aizsardzības un ārpustiesas aizsardzības līdzekļi modernizētās Konvencijas Nr. 108 noteikumu pārkāpumu gadījumā[645]. Apsūdzības par datu aizsardzības tiesību pārkāpumiem, kas ir pretrunā ECTK 8. pantam, pret ECTK līgumslēdzēju pusi var iesniegt arī ECT, kad visi pieejamie valsts tiesiskās aizsardzības līdzekļi ir izsmelti. ECT iesniegtajai prasībai par ECTK 8. panta pārkāpumu ir jāatbilst arī citiem pieņemamības kritērijiem (ECTK 34.–35. pants)[646].

642 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C-293/12 un C-594/12 *Digital Rights Ireland Ltd pret Minister for Communications, Marine and Natural Resources un citiem* un Kärntner Landesregierung un citiem [GC], 69. punkts.

643 EST 1981. gada 16. decembra spriedums lietā C-244/80 *Pasquale Foglia pret Mariella Novello (Nr. 2)*; EST 2006. gada 28. septembra spriedums lietā C-467/04 *Kriminālprocess pret Gasparini un citiem*.

644 EST 2007. gada 11. decembra spriedums lietā C-438/05 *Starptautiskā transporta darbinieku federācija, Somijas Jūrnieku apvienība pret Viking Line ABP, OÜ Viking Line Eesti* [GC], 85. punkts.

645 Modernizētā Konvencija Nr. 108, 12. pants.

646 ECTK, 34.–37. pants.

Lai arī prasības ECT var vērst tikai pret līgumslēdzējām pusēm, tās var arī netieši skart privātu pušu darbības vai bezdarbību, ciktāl līgumslēdzēja puse nav izpildījusi savas saistības saskaņā ar ECTK un nav nodrošinājusi pietiekamu aizsardzību pret datu aizsardzības tiesību pārkāpumiem valsts tiesību aktos.

Piemērs. Lietā *K.U. pret Somiju*[647] prasītājs, kurš bija nepilngadīgs, iesniedza sūdzību par to, ka interneta iepazīšanās vietnē attiecībā uz viņu bija ievietots seksuāla rakstura sludinājums. Pakalpojumu sniedzējs neatklāja tās personas identitāti, kura bija ievietojusi sludinājumu, atsaucoties uz Somijas tiesību aktos noteiktajām konfidencialitātes prasībām. Prasītājs apgalvoja, ka Somijas tiesību akti nenodrošina pietiekamu aizsardzību pret šādām darbībām, ko bija veikusi privātpersona, kura bija publicējusi inkriminējošus datus par pieteikuma iesniedzēju internetā. ECT uzskatīja, ka valstīm ir ne tikai pienākums atturēties no patvaļīgas iejaukšanās personu privātajā dzīvē, bet tām var būt arī saistības, kas ietver "tādu pasākumu īstenošanu, kuru mērķis ir nodrošināt privātās dzīves neaizskaramību pat indivīdu savstarpējo attiecību jomā". Šajā gadījumā, lai nodrošinātu praktisku un efektīvu pieteikuma iesniedzēja aizsardzību, bija jāveic efektīvi pasākumi ar mērķi noskaidrot un saukt pie atbildības likumpārkāpēju. Taču valsts šādu aizsardzību nenodrošināja, un tiesa atzina, ka šajā lietā ir pārkāpts ECTK 8. pants.

Piemērs. Lietā *Köpke pret Vāciju*[648] prasītāja tika turēta aizdomās par zādzībām viņas darba vietā un attiecībā uz viņu tika veikta slēpta videonovērošana. ECT secināja, ka "nekas neliecina par to, ka valsts iestādes savas rīcības brīvības ietvaros nav radušas taisnīgu līdzsvaru starp prasītājas tiesībām uz privātās dzīves neaizskaramību saskaņā ar 8. pantu un abām viņas darba devēja interesēm aizsargāt savu īpašuma tiesības un sabiedrības interesēm par pienācīgu tiesvedību". Tāpēc prasība tika atzīta par nepieņemamu.

Ja ECT konstatē, ka kāda līgumslēdzēja puse ir pārkāpusi kādas no ECTK aizsargātajām tiesībām, šai līgumslēdzējai pusei ir pienākums izpildīt ECT spriedumu (ECTK 46. pants). Ar izpildes pasākumiem vispirms jāizbeidz pārkāpums un pēc iespējas jānovērš tā nelabvēlīgās sekas prasītājam. Spriedumu izpildei var būt nepieciešami arī vispārīgi pasākumi, lai novērstu pārkāpumus, kas līdzīgi tiesas konstatētajiem, veicot izmaiņas likumdošanā, judikatūrā vai izmantojot citus pasākumus.

647 ECT 2008. gada 2. decembra spriedums lietā *K.U. pret Somiju*, Nr. 2872/02.

648 ECT 2010. gada 5. oktobra spriedums lietā *Köpke pret Vāciju* (dec.), Nr. 420/07.

Ja ECT konstatē ECTK pārkāpumu, ECTK 41. pantā paredzēts, ka tā var piešķirt prasītājam "taisnīgu kompensāciju", ko sedz līgumslēdzēja puse.

Tiesības pilnvarot bezpeļņas struktūru, organizāciju vai apvienību

VDAR paredzēta iespēja privātpersonām, kuras iesniedz sūdzību uzraudzības iestādei vai ceļ prasību tiesā, pilnvarot bezpeļņas struktūru, organizāciju vai apvienību tās pārstāvēt[649]. Šīm bezpeļņas organizācijām jābūt likumā noteiktiem mērķiem sabiedrības interešu jomā, un tām aktīvi jādarbojas datu aizsardzības jomā. Tās datu subjekta(-u) vārdā var iesniegt sūdzību vai īstenot tiesības uz tiesisko aizsardzību. Regulā dalībvalstīm paredzēta iespēja saskaņā ar valsts tiesību aktiem izlemt, vai struktūra var iesniegt sūdzības datu subjektu vārdā bez datu subjektu pilnvarojuma.

Šīs pārstāvības tiesības ļauj privātpersonām izmantot šādu bezpeļņas organizāciju kompetenci, organizatoriskās un finansiālās iespējas, tādējādi ievērojami atvieglojot privātpersonām to tiesību īstenošanu. VDAR ļauj šīm struktūrām iesniegt kolektīvas prasības vairāku datu subjektu vārdā. Tas palīdz arī nodrošināt tiesu sistēmas darbību un efektivitāti, jo līdzīgas prasības tiek grupētas un izskatītas kopā.

6.2.3. Atbildība un tiesības uz kompensāciju

Tiesībām uz efektīvu tiesisko aizsardzību ir jādod privātpersonām iespēja pieprasīt kompensāciju par jebkādiem zaudējumiem, kas radušies to personas datu apstrādes rezultātā, pārkāpjot piemērojamos tiesību aktus. Pārziņu un apstrādātāju atbildība par nelikumīgu apstrādi ir nepārprotami atzīta VDAR[650]. Regulā privātpersonām ir sniegtas tiesības saņemt kompensāciju no pārziņa vai apstrādātāja gan par materiālo, gan morālo kaitējumu, savukārt tās apsvērumos noteikts, ka "kaitējuma jēdziens būtu plaši jāinterpretē, ņemot vērā Tiesas judikatūru, tādā veidā, kas pilnībā atbilst šīs regulas mērķiem"[651]. Pārziņus var saukt pie atbildības, un viņiem var tikt izvirzītas prasības izmaksāt kompensāciju, ja tie nepilda savus regulā ietvertos pienākumus. Personas datu apstrādātājs atbild par kaitējumu, kas nodarīts ar apstrādi, tikai tad, ja tas nav izpildījis šajā regulā paredzētos pienākumus, kas konkrēti adresēti apstrādātājam, vai ja tas ir rīkojies neatbilstoši vai pretēji pārziņa likumīgiem norādījumiem. Ja pārzinis vai apstrādātājs ir samaksājis pilnu kompensāciju, VDAR paredz, ka pārzinis vai apstrādātājs no citiem pārziņiem vai apstrādātājiem,

649 Vispārīgā datu aizsardzības regula, 80. pants.

650 Turpat, 82. pants.

651 Turpat, 146. apsvērums.

kuri iesaistīti vienā un tajā pašā apstrādē, var pieprasīt segt daļu kompensācijas, kas atbilst viņu atbildības pakāpei par zaudējumiem[652]. Tajā pašā laikā atbrīvojumi no atbildības ir ļoti ierobežoti un ir jāpierāda, ka pārzinis vai apstrādātājs nekādā veidā nav atbildīgs par notikumu, kas izraisījis kaitējumu.

Kompensācijai jābūt "pilnai un iedarbīgai" attiecībā uz nodarīto kaitējumu. Ja kaitējums nodarīts vairāku pārziņu un apstrādātāju apstrādes rezultātā, katrs pārzinis vai apstrādātājs saucams pie atbildības par visu kaitējuma apmēru. Šā noteikuma mērķis ir nodrošināt datu subjektiem iedarbīgu kompensāciju un apstrādes darbībās iesaistīto pārziņu un apstrādātāju koordinētu pieeju atbilstības nodrošināšanai.

Piemērs. Datu subjektiem nav jāierosina lieta un jāpieprasa kompensācija no visām organizācijām, kas ir atbildīgas par kaitējumu, jo tas var novest pie dārgas un ilgstošas tiesvedības. Pietiek, ja lieta tiek ierosināta pret vienu no kopīgajiem pārziņiem, kuru pēc tam var saukt pie atbildības par pilnu kaitējuma apmēru. Šādos gadījumos pārzinim vai apstrādātājam, kurš atlīdzina kaitējumu, vēlāk ir tiesības atgūt samaksāto summu no citām apstrādē iesaistītajām vienībām, kas ir atbildīgas par pārkāpumu, viņu atbildības par kaitējumu apmērā. Šīs tiesvedības starp dažādiem kopīgajiem pārziņiem un apstrādātājiem notiek pēc tam, kad datu subjekts ir saņēmis kompensāciju, un datu subjekts tajās neiesaistās.

EP tiesiskajā regulējumā modernizētās Konvencijas Nr. 108 12. pantā ietverta prasība līgumslēdzējām pusēm izveidot piemērotus tiesiskās aizsardzības līdzekļus attiecībā uz valsts tiesību aktu, ar kuriem īsteno konvencijas prasības, pārkāpumiem. Modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā norādīts, ka tiesiskās aizsardzības līdzekļiem jāietver iespēja tiesā apstrīdēt lēmumu vai praksi, vienlaikus nodrošinot arī ārpustiesas aizsardzības līdzekļus[653]. Katra līgumslēdzēja puse var noteikt šo noteikumu piemērošanas kārtību un dažādus noteikumus, kā arī procedūras, kas jāievēro. Līgumslēdzējām pusēm un valstu tiesām ir jāapsver arī finansiālās kompensācijas noteikumi par materiālo un morālo kaitējumu, ko nodarījusi apstrāde, kā arī par iespēju īstenot kolektīvu rīcību[654].

652 Turpat, 82. panta 2. un 5. punkts.

653 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 100. punkts.

654 Turpat.

6.2.4. Sankcijas

Saskaņā ar EP tiesību aktiem modernizētās Konvencijas Nr. 108 12. pantā paredzēts, ka ikvienai līgumslēdzējai pusei ir jānosaka attiecīgas sankcijas un tiesiskās aizsardzības līdzekļi par tādu valsts tiesību aktu pārkāpumiem, ar kuriem tiek īstenoti Konvencija Nr. 108 noteiktie datu aizsardzības pamatprincipi. Konvencijā nenosaka un neuzliek īpašu sankciju kopumu. Tieši otrādi, tajā ir skaidri norādīts, ka ikvienai līgumslēdzējai pusei ir rīcības brīvība noteikt raksturu tiesas vai ārpustiesas sankcijām, kas var būt krimināltiesiskas, administratīvas vai civiltiesiskas. Modernizētās Konvencijas Nr. 108 skaidrojošajā ziņojumā paredzēts, ka sankcijām jābūt efektīvām, samērīgām un atturošām[655]. Līgumslēdzējām pusēm ir jāievēro šis princips, nosakot savā valsts tiesiskajā regulējumā pieejamo sankciju raksturu un smagumu.

Saskaņā ar ES tiesību aktiem VDAR 83. pants pilnvaro dalībvalstu uzraudzības iestādes piemērot administratīvus naudas sodus par regulas pārkāpumiem. Naudas sodu apmērs un apstākļi, ko valsts iestādes ņem vērā, lemjot par naudas soda piemērošanu, kā arī šā naudas soda kopējā maksimālā robeža arī ir paredzēti 83. pantā. Tādējādi sankciju režīms ir saskaņots visā ES.

VDAR ievēro diferencētu pieeju naudas sodiem. Uzraudzības iestādēm ir tiesības piemērot administratīvus naudas sodus par regulas pārkāpumiem līdz pat 20 000 000 EUR apmērā vai, ja pārkāpējs ir uzņēmums, 4 % no tā kopējā gadā apgrozījuma visā pasaulē: atkarībā no tā, kurš ir lielāks. Pārkāpumi, kuru rezultātā var tikt piemēroti šāda līmeņa naudas sodi, ietver apstrādes pamatprincipu un piekrišanas nosacījumu pārkāpumus, datu subjektu tiesību pārkāpumus un regulas noteikumu, kas reglamentē personas datu nosūtīšanu saņēmējiem trešās valstīs, pārkāpumus. Par citiem pārkāpumiem uzraudzības iestādes var uzlikt naudas sodus līdz 10 000 000 EUR vai, ja tas ir uzņēmums, divus procentus no tā kopējā gada apgrozījuma visā pasaulē, atkarībā no tā, kurš ir lielāks.

Nosakot piemērojamā naudas soda veidu un apmēru, uzraudzības iestādēm jāņem vērā virkne faktoru[656]. Piemēram, tām ir pienācīgi jāņem vērā pārkāpuma raksturs, smagums un ilgums, skarto personas datu kategorijas, kā arī tas, vai pārkāpumam ir tīšs vai nolaidīgs raksturs. Jāņem vērā arī tas, ja pārzinis vai apstrādātājs ir veicis pasākumus, lai mazinātu datu subjektiem nodarīto kaitējumu. Tāpat sadarbības līmenis ar uzraudzības iestādi pēc pārkāpuma un veids, kādā uzraudzības iestāde uzzinājusi par pārkāpumu (piemēram, vai par to ziņoja par apstrādi atbildīgā

655 Turpat.

656 Vispārīgā datu aizsardzības regula, 83. panta 2. punkts.

struktūra vai datu subjekts, kura tiesības bija pārkāptas) ir citi svarīgi faktori, kas uzraudzības iestādēm palīdz pieņemt lēmumu[657].

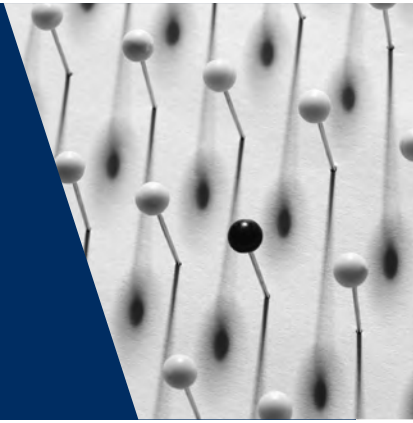
Papildus iespējai uzlikt administratīvos naudas sodus uzraudzības iestāžu rīcībā ir plašs citu korektīvo pilnvaru klāsts. Tā sauktās uzraudzības iestāžu "korektīvās" pilnvaras ir noteiktas VDAR 58. pantā. To amplitūda ir no rīkojumu izdošanas, brīdinājumu un rājienu izteikšanas pārziņiem un apstrādātājiem līdz pagaidu vai pat pastāvīgai apstrādes darbību aizliegšanai.

Attiecībā uz sankcijām par ES tiesību aktu pārkāpumiem, ko izdarījušas ES iestādes vai struktūras, balstoties uz ES iestāžu datu aizsardzības regulas īpašo uzdevumu, var paredzēt sankcijas disciplināras atbildības veidā. Atbilstoši šīs regulas 49. pantam "ja Eiropas Kopienu ierēdnis vai cits darbinieks tīšām vai nolaidības dēļ neievēro šajā regulā paredzētos pienākumus, viņš ir disciplināri atbildīgs (..)".

657 29. panta darba grupa (2017), *Pamatnostādnes administratīvo naudas sodu piemērošanai un noteikšanai Regulas 2016/679 vajadzībām*, WP 253, 2017. gada 3. oktobris.

7

Starptautiska datu nosūtīšana un personas datu plūsmas



ES	Aptvertie jautājumi	EP
Personas datu nosūtīšana		
Vispārīgā datu aizsardzības regula, 44. pants	Jēdziens	Modernizētā Konvencija Nr. 108, 14. panta 1. un 2. punkts
Personas datu brīva plūsma		
Vispārīgā datu aizsardzības regula, 1. panta 3. punkts un 170. apsvērums	Starp ES dalībvalstīm	
	Starp Konvencijas Nr. 108 līgumslēdzējām pusēm	Modernizētā Konvencija Nr. 108, 14. panta 1. punkts
Personas datu nosūtīšana trešām valstīm vai starptautiskām organizācijām		
Vispārīgā datu aizsardzības regula, 45. pants EST lieta C-362/14 *Maximillian Schrems pret Datu aizsardzības komisāru* [GC], 2015.	Lēmums par aizsardzības līmeņa pietiekamību/trešās valstis vai starptautiskās organizācijas ar atbilstošu aizsardzības līmeni	Modernizētā Konvencija Nr. 108, 14. panta 2. punkts
Vispārīgā datu aizsardzības regula, 46. panta 1. un 2. punkts	Attiecīgi drošības pasākumi, tostarp īstenojamas tiesības un tiesiskās aizsardzības līdzekļi datu subjektiem, ko nodrošina ar līgumu standartklauzulām, saistošiem uzņēmuma noteikumiem, rīcības kodeksiem un sertifikācijas mehānismiem.	Modernizētā Konvencija Nr. 108, 14. panta 2., 3., 5. un 6. punkts

ES	Aptvertie jautājumi	EP
Vispārīgā datu aizsardzības regula, 46. panta 3. punkts	Ar kompetentās uzraudzības iestādes atļauju: līguma klauzulas un noteikumi, kas iekļauti administratīvos pasākumos starp publiskām iestādēm	
Vispārīgā datu aizsardzības regula, 46. panta 5. punkts	Esošās atļaujas, pamatojoties uz Direktīvu 95/46/EK	
Vispārīgā datu aizsardzības regula, 47. pants	Saistošie uzņēmuma noteikumi	
Vispārīgā datu aizsardzības regula, 49. pants	Atkāpes īpašās situācijās	Modernizētā Konvencija Nr. 108, 14. panta 4. punkts
Piemēri. ES–ASV nolīgums par PDR ES–ASV nolīgums par *SWIFT*	Starptautiski nolīgumi	Modernizētā Konvencija Nr. 108, 14. panta 3. punkta a) apakšpunkts

Saskaņā ar ES tiesību aktiem Vispārīgajā datu aizsardzības regulā paredzēta brīva datu plūsma Eiropas Savienībā. Tomēr tajā ir ietvertas īpašas prasības attiecībā uz personas datu nosūtīšanu trešām valstīm ārpus ES, kā arī starptautiskām organizācijām. Regulā atzīta šādas nosūtīšanas nozīme, jo īpaši ņemot vērā starptautisko tirdzniecību un sadarbību, taču ir atzīts arī paaugstināts personas datu risks. Tādēļ regulas mērķis ir piedāvāt personas datiem, ko nosūta trešām valstīm, tāda paša līmeņa aizsardzību, kāda tiem ir ES iekšienē[658]. EP tiesību aktos ir atzīta arī pārrobežu datu plūsma, kuru pamatā ir brīva plūsma starp pusēm un īpašas prasības nosūtīšanai trešām valstīm, īstenošanas noteikumu nozīme.

7.1. Personas datu nosūtīšanas raksturs

Svarīgākie aspekti

- ES un EP tiesību aktos ir ietverti noteikumi par personas datu nosūtīšanu saņēmējiem trešās valstīs vai starptautiskām organizācijām.
- Ja datu subjekta tiesības tiek aizsargātas, datus nosūtot ārpus ES, tas ļauj nodrošināt, ka ES tiesību aktos noteiktā aizsardzība attiecas uz personas datiem, kuru izcelsme ir ES.

658 Vispārīgā datu aizsardzības regula, 101. un 116. apsvērums.

Saskaņā ar **EP tiesību aktiem** datu pārrobežu plūsmas tiek aprakstītas kā personas datu nosūtīšana saņēmējiem, uz kuriem attiecas ārvalstu jurisdikcija[659]. Pārrobežu datu plūsmas saņēmējam, kurš nav līgumslēdzējas puses jurisdikcijā, ir atļautas tikai tad, ja tiek nodrošināts attiecīgs aizsardzības līmenis[660].

ES tiesību akti regulē tādu personas datu nosūtīšanu, "kas tiek apstrādāti vai kurus ir paredzēts apstrādāt pēc nosūtīšanas uz trešo valsti vai starptautisku organizāciju (..)"[661]. Šādas datu plūsmas ir atļautas tikai tad, ja tās atbilst VDAR V nodaļā izklāstītajiem noteikumiem.

Personas datu pārrobežu plūsmas ir atļautas saņēmējam, kurš ir attiecīgi līgumslēdzējas puses vai dalībvalsts jurisdikcijā saskaņā ar EP vai ES tiesību aktiem. Abas tiesību sistēmas arī ļauj nosūtīt datus valstij, kas nav līgumslēdzēja puse vai dalībvalsts, ja ir izpildīti konkrēti nosacījumi.

7.2. Personas datu brīva aprite/plūsma starp dalībvalstīm vai līgumslēdzējām pusēm

Svarīgākie aspekti

- Personas datu plūsmai visā ES, kā arī personas datu nosūtīšanai starp modernizētās Konvencijas Nr. 108 līgumslēdzējām pusēm nedrīkst būt ierobežojumu. Tomēr, tā kā ne visas modernizētās Konvencijas Nr. 108 līgumslēdzējas puses ir ES dalībvalstis, datu nosūtīšana no ES dalībvalsts uz trešo valsti, kas ir Konvencijas Nr. 108 līgumslēdzēja puse, tomēr nav iespējama, ja tā neatbilst VDAR izvirzītajiem nosacījumiem.

Saskaņā ar EP tiesību aktiem starp modernizētās Konvencijas Nr. 108 līgumslēdzējām pusēm jābūt brīvai personas datu plūsmai. Tomēr nosūtīšanu var aizliegt, ja pastāv "reāls un nopietns risks, ka nosūtīšana citai Pusei novedīs pie Konvencijas noteikumu apiešanas" vai ja Pusei ir šāds pienākums atbilstoši "saskaņotajiem aizsardzības noteikumiem, kurus kopīgi izmanto reģionālai starptautiskai organizācijai piederošās valstis"[662].

659 Modernizētās Konvencijas Nr. 108 skaidrojošais ziņojums, 102. punkts.

660 Modernizētā Konvencija Nr. 108, 14. panta 2. punkts.

661 Vispārīgā datu aizsardzības regula, 44. pants.

662 Modernizētā Konvencija Nr. 108, 14. panta 1. punkts.

ES tiesību aktos ir aizliegts piemērot ierobežojumus vai aizliegumus brīvai personas datu apritei starp ES dalībvalstīm, pamatojoties uz fizisku personu aizsardzību attiecībā uz personas datu apstrādi[663]. **Brīvas datu plūsmas zona ir paplašināta**, ietverot Eiropas Ekonomikas zonas līgumu (EEZ)[664], ar kuru iekšējā tirgū iekļauj Islandi, Lihtenšteinu un Norvēģiju.

Piemērs. Ja starptautiskas uzņēmumu grupas, kas atrodas vairākās dalībvalstīs, tostarp Slovēnijā un Francijā, saistītais uzņēmums pārsūta personas datus no Slovēnijas uz Franciju, Slovēnijas valsts tiesību aktos šādu datu plūsmu nedrīkst ierobežot vai aizliegt, pamatojot ar iemesliem, kas saistīti ar personas datu aizsardzību.

Taču, ja tas pats saistītais uzņēmums Slovēnijā vēlas nosūtīt tos pašus personas datus mātesuzņēmumam Malaizijā, tad Slovēnijas datu nosūtītājam ir jāņem vērā VDAR V nodaļā ietvertie noteikumi. Šo noteikumu mērķis ir aizsargāt ES jurisdikcijā esošos datu subjektus.

Saskaņā ar ES tiesību aktiem personas datu plūsmām uz EEZ dalībvalstīm nolūkā, kas saistīts ar noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu, kriminālvajāšanu vai kriminālsodu izpildi, piemēro Direktīvu (ES) 2016/680[665]. Tādējādi arī tiek nodrošināts, ka kompetento iestāžu veiktā personas datu apmaiņa Savienībā netiek ierobežota vai aizliegta datu aizsardzības apsvērumu dēļ. Saskaņā ar EP tiesību aktiem visu personas datu apstrāde (tostarp datu pārrobežu plūsma ar citām Konvencijas Nr. 108 līgumslēdzējām pusēm), neattiecinot nolūkā vai darbības jomās balstītus izņēmumus, ir iekļauta Konvencijas Nr. 108 piemērošanas jomā, taču līgumslēdzējas puses var noteikt atbrīvojumus. Visas EEZ dalībnieces ir arī Konvencijas Nr. 108 līgumslēdzējas puses.

663 Vispārīgā datu aizsardzības regula, 1. panta 3. punkts.

664 Padomes un Komisijas 1993. gada 13. decembra Lēmums par Eiropas Ekonomiskās zonas līguma noslēgšanu starp Eiropas Kopienām, tās dalībvalstīm un Austrijas Republiku, Somijas Republiku, Islandes Republiku, Lihtenšteinas Grāfisti, Norvēģijas Karalisti, Zviedrijas Karalisti un Šveices Konfederāciju, OV 1994 L 1.

665 Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Direktīva (ES) 2016/680 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI, OV 2016 L 119.

7.3. Personas datu nosūtīšana trešām valstīm/valstīm, kuras nav līgumslēdzējas puses, vai starptautiskām organizācijām

Svarīgākie aspekti

- Gan **EP**, gan **ES** ļauj personas datus nosūtīt trešām valstīm vai starptautiskām organizācijām, ja tiek ievēroti noteikti personas datu aizsardzības nosacījumi.
  - **Saskaņā ar EP tiesību aktiem** attiecīgu aizsardzības līmeni var sasniegt ar valsts vai starptautiskas organizācijas likumiem vai ar attiecīgu standartu ieviešanu.
  - **Saskaņā ar ES tiesību aktiem** datu nosūtīšanu var veikt, ja trešā valsts nodrošina pienācīgu aizsardzības līmeni vai ja datu pārzinis vai apstrādātājs nodrošina attiecīgus aizsardzības pasākumus, tostarp īstenojamas datu subjektu tiesības un tiesiskās aizsardzības līdzekļus, izmantojot tādus līdzekļus kā standarta datu aizsardzības klauzulas vai saistošos uzņēmuma noteikumus.
- **Gan EP tiesību aktos, gan ES tiesību aktos** ir paredzētas izņēmuma klauzulas, kas ļauj nosūtīt personas datus īpašos apstākļos pat tad, ja nav ieviests nedz pietiekams aizsardzības līmenis, nedz arī attiecīgi aizsardzības pasākumi.

Lai gan EP un ES tiesību akti pieļauj datu plūsmu uz trešām valstīm vai uz starptautiskām organizācijām, tajos paredzēti atšķirīgi nosacījumi. Katrā nosacījumu kopumā tiek ņemta vērā attiecīgās organizācijas atšķirīgā struktūra un mērķi.

Saskaņā ar **ES tiesību aktiem** principā paredzēti divi veidi, kā atļaut personas datu nosūtīšanu trešām valstīm vai starptautiskām organizācijām. Personas datu nosūtīšana var notikt, pamatojoties uz Eiropas Komisijas lēmumu par aizsardzības līmeņa pietiekamību[666] vai, ja šāda lēmuma par aizsardzības līmeņa pietiekamību nav, gadījumos, kad pārzinis vai apstrādātājs nodrošina attiecīgus aizsardzības pasākumus, tostarp datu subjektam īstenojamas tiesības un tiesiskās aizsardzības līdzekļus[667]. Ja nav ne lēmuma par aizsardzības līmeņa pietiekamību, ne attiecīgu aizsardzības pasākumu, ir iespējamas vairākas atkāpes.

666 Vispārīgā datu aizsardzības regula, 45. pants

667 Turpat, 46. pants.

Saskaņā ar **EP tiesību aktiem** tomēr brīva datu nosūtīšana valstīm, kas nav Konvencijas līgumslēdzējas puses, ir atļauta tikai šādos gadījumos:

- šīs valsts vai starptautiskās organizācijas likumi, tostarp piemērojamie starptautiskie līgumi vai nolīgumi, garantē attiecīgus aizsardzības pasākumus;

- *ad hoc* vai apstiprināti standartizēti aizsardzības pasākumi, ko nodrošina ar juridiski saistošiem un izpildāmiem instrumentiem, kurus pieņēmušas un ieviesušas datu nosūtīšanā un turpmākā apstrādē iesaistītās personas[668].

Līdzīgi kā ES tiesību aktos, ja nav piemērota datu aizsardzības līmeņa, ir iespējamas vairākas atkāpes.

7.3.1. Nosūtīšana, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību

Saskaņā ar ES tiesību aktiem VDAR 45. pantā ir paredzēta brīva personas datu plūsma uz trešām valstīm ar pietiekamu datu aizsardzības līmeni. EST ir precizējusi, ka termins "pietiekams aizsardzības līmenis" pieprasa trešai valstij nodrošināt ES tiesību aktos paredzētajām garantijām "būtībā ekvivalentu"[669] pamattiesību un brīvību aizsardzības līmeni. Tajā pašā laikā līdzekļi, kurus trešā valsts izmanto šāda aizsardzības līmeņa nodrošināšanai, var atšķirties no tiem, kas tiek izmantoti ES, atbilstības standartā nav prasības precīzi punkts punktā atkārtot ES noteikumus[670].

Eiropas Komisija novērtē datu aizsardzības līmeni ārvalstīs, aplūkojot to valstu likumus un piemērojamās starptautiskās saistības. Vērā jāņem arī valsts dalība daudzpusējās vai reģionālās sistēmās, jo īpaši attiecībā uz personas datu aizsardzību. Ja Eiropas Komisija konstatē, ka trešā valsts vai starptautiska organizācija nodrošina atbilstošu aizsardzības līmeni, tā var izdot lēmumu par aizsardzības līmeņa pietiekamību, kas ir saistošs[671]. Tomēr EST ir paziņojusi, ka valstu uzraudzības iestādes joprojām ir kompetentas izskatīt personas prasību par tās personas datu, kas ir nosūtīti

668 Modernizētā Konvencija Nr. 108, 14. panta 3. punkta a) un b) apakšpunkts.

669 EST 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems pret Datu aizsardzības komisāru* [GC], 96. punkts.

670 Turpat, 74. punkts. Skatīt arī, Eiropas Komisija (2017), Komisijas paziņojums Eiropas Parlamentam un Padomei "Personas datu apmaiņa un aizsardzība globalizētajā pasaulē", COM(2017)7 *final*, 2017. gada 10. janvāris, 6. lpp.

671 Pastāvīgi atjauninātu to valstu sarakstu, kuras saņēmušas atbilstības atzinumu, skatīt Eiropas Komisijas Tieslietu ģenerāldirektorāta mājaslapā.

trešai valstij, kuras nodrošināto aizsardzības līmeni Komisija ir atzinusi par atbilstošu, aizsardzību, ja šī persona apgalvo, ka trešā valstī spēkā esošie likumi un prakse nenodrošina atbilstošu aizsardzības līmeni[672].

Eiropas Komisija var arī vērtēt teritorijas trešās valsts iekšienē atbilstību vai vērtēt tikai noteiktas nozares, kā tas bija, piemēram, attiecībā uz Kanādas privātajiem komerciālajiem tiesību aktiem[673]. Tāpat ir arī aizsardzības līmeņa pietiekamības atzinumi par nosūtīšanu, pamatojoties uz nolīgumiem starp ES un trešām valstīm. Šie lēmumi attiecas tikai uz viena veida datu nosūtīšanu, piemēram, uz aviosabiedrības pārsūtītu pasažieru datu reģistru (PDR) ārvalstu robežu kontroles iestādēm, aviosabiedrībām lidojot no ES uz konkrētiem aizjūras galamērķiem (skatīt 7.3.4. iedaļu).

Lēmumi par aizsardzības līmeņa pietiekamību regulāri tiek uzraudzīti. Eiropas Komisija regulāri pārskata šādus lēmumus, lai izsekotu tendencēm, kas varētu ietekmēt to statusu. Tādējādi, ja Eiropas Komisija konstatē, ka trešā valsts vai starptautiskā organizācija vairs neatbilst nosacījumiem, kas attaisno lēmumu par aizsardzības līmeņa pietiekamību, tā var grozīt, apturēt vai atcelt lēmumu. Komisija var arī sākt sarunas ar attiecīgo trešo valsti vai starptautisko organizāciju, lai novērstu problēmu, kas ir tās lēmuma pamatā.

Lēmumi par aizsardzības līmeņa pietiekamību, ko Eiropas Komisija pieņēmusi, pamatojoties uz Direktīvu 95/46/EK, paliek spēkā, līdz tos groza, aizstāj vai atceļ ar Komisijas lēmumu, kas pieņemts saskaņā ar VDAR 45. panta noteikumiem.

Līdz šim Eiropas Komisija ir atzinusi, ka Andora, Argentīna, Kanāda (komercorganizācijas, uz kurām attiecas Personiskās informācijas aizsardzības un elektronisko dokumentu likums – *PIPEDA*), Fēru salas, Gērnsija, Menas sala, Izraēla, Džērsija, Jaunzēlande, Šveice un Urugvaja nodrošina atbilstošu aizsardzību. Attiecībā uz datu nosūtīšanu uz ASV Eiropas Komisija 2000. gadā pieņēma lēmumu par aizsardzības līmeņa pietiekamību, ļaujot nosūtīt datus ASV uzņēmumiem, kas pašsertifikācijas sistēmas ietvaros ir apliecinājuši, ka aizsargā no ES nosūtītos personas datus un ievēro tā

672 EST 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems pret Datu aizsardzības komisāru* [GC], 63. un 65.–66. punkts.

673 Eiropas Komisija (2002), 2001. gada 20. decembra Lēmums 2002/2/EK atbilstoši Eiropas Parlamenta un Padomes Direktīvai 95/46/EK par personas datu pienācīgu aizsardzību, ko nodrošina ar Kanādas likumu par personas datu un elektronisko dokumentu aizsardzību, OV 2002 L 2.

dēvētos "drošības zonas principus"[674]. EST šo lēmumu 2015. gadā atzina par spēkā neesošu, un 2016. gada jūlijā tika pieņemts jauns lēmums par pietiekamību, ļaujot uzņēmumiem pievienoties no 2016. gada 1. augusta.

Piemērs. Lietā *Schrems*[675] Austrijas pilsonis *Maximilian Schrems* jau vairākus gadus bija vietnes *Facebook* lietotājs. Visi dati vai daļa datu, ko *Schrems* kungs sniedza *Facebook*, tika nosūtīti no *Facebook* Īrijas meitasuzņēmumiem uz serveriem ASV, kur tie tika apstrādāti. *Schrems* kungs iesniedza sūdzību Īrijas datu aizsardzības iestādē, uzskatot, ka, ņemot vērā ASV trauksmes cēlēja Edvarda Snoudena atklājumus par ASV izlūkdienestu uzraudzības darbībām, ASV likumi un prakse nenodrošina atbilstošu uz šo valsti nosūtīto datu aizsardzību. Īrijas iestāde sūdzību noraidīja, pamatojoties uz to, ka Komisija savā 2000. gada 26. jūlija lēmumā uzskatīja, ka "drošības zonas" shēmas ietvaros ASV nodrošina atbilstošu nosūtīto personas datu aizsardzības līmeni. Lieta tika iesniegta Īrijas Augstākajā tiesā, kas to nosūtīja EST prejudiciāla nolēmuma sniegšanai.

EST pasludināja Komisijas lēmumu par aizsardzības līmeņa pietiekamību drošības zonas programmas ietvaros par spēkā neesošu. EST vispirms atzīmēja, ka lēmums ļāva ierobežot drošības zonas datu aizsardzības principu piemērošanu, atsaucoties uz valsts drošību, sabiedrības interesēm vai tiesībaizsardzības prasībām vai pamatojoties uz ASV vietējiem tiesību aktiem. Tādēļ lēmums ļāva iejaukties to personu pamattiesībās, kuru personas dati tika vai varēja tikt nosūtīti uz ASV[676]. Tiesa arī atzīmēja, ka lēmumā nav nekādu atzinumu par ASV pastāvošajiem noteikumiem, kuru mērķis ir ierobežot šādu iejaukšanos, nedz arī par efektīvas tiesiskās aizsardzības esamību pret šādu iejaukšanos[677]. EST uzsvēra, ka ES garantētā pamattiesību un pamatbrīvību aizsardzības līmeņa nodrošināšanai tiesiskajā regulējumā, kurā ir ietverta iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās, jāparedz skaidri un precīzi noteikumi, kas reglamentētu attiecīgā pasākuma apjomu

674 Komisijas 2000. gada 26. jūlija Lēmums 2000/520/EK atbilstoši Eiropas Parlamenta un Padomes Direktīvai 95/46/EK par pienācīgu aizsardzību, kas noteikta ar privātuma drošības zonas principiem, un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija, OJ L 215. Šis lēmums ir pasludināts par spēkā neesošu ar EST spriedumu lietā C-632/14, *Maximilian Schrems pret Datu aizsardzības komisāru* [GC].

675 EST 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems pret Datu aizsardzības komisāru* [GC].

676 Turpat, 84. punkts.

677 Turpat, 88.–89. punkts.

un piemērošanu un noteiktu minimālās prasības, atkāpes un ierobežojumus attiecībā uz personas datu aizsardzību[678]. Tā kā Komisijas lēmumā nebija teikts, ka ASV faktiski nodrošina šādu aizsardzības līmeni, pamatojoties uz tās valsts tiesību aktiem vai starptautiskajām saistībām, EST secināja, ka tas neatbilst Datu aizsardzības direktīvas attiecīgās nosūtīšanas normas prasībām un tāpēc ir spēkā neesošs[679].

Tādējādi ASV aizsardzības līmenis nebija "būtībā ekvivalents" ES garantētajām pamattiesībām un brīvībām[680]. EST apgalvoja, ka ir pārkāpti vairāki ES Pamattiesību hartas panti. Pirmkārt, tika apdraudēta 7. panta būtība, jo saskaņā ar ASV tiesību aktiem "valsts iestādēm vispārīgi tiek ļauts piekļūt elektronisko komunikāciju saturam". Otrkārt, tika pārkāpta arī 47. panta būtība, jo tiesību akti nenodrošināja personām tiesiskās aizsardzības līdzekļus attiecībā uz piekļuvi personas datiem vai personas datu labošanu vai dzēšanu. Visbeidzot, tā kā ar drošības zonas vienošanos tika pārkāpti iepriekš minētie panti, personas datu apstrāde vairs nebija likumīga, tāpēc tika pārkāpts 8. pants.

Pēc tam, kad EST pasludināja drošības zonas vienošanos par spēkā neesošu, Komisija un ASV vienojās par jaunu regulējumu – ES un ASV privātuma vairogu. Komisija 2016. gada 12. jūlijā pieņēma lēmumu, ar kuru paziņoja, ka ASV nodrošina atbilstošu aizsardzības līmeni personas datiem, kurus privātuma vairoga ietvaros no Savienības nosūta organizācijām ASV[681].

Līdzīgi kā drošības zonas vienošanās, arī ES un ASV privātuma vairoga regulējuma mērķis ir aizsargāt personas datus, kuri komerciālos nolūkos no ES tiek nosūtīti uz ASV[682]. ASV uzņēmumi var brīvprātīgi pašsertificēties privātuma vairoga sarakstam,

678 Turpat, 91.–92. punkts.

679 Turpat, 96.–97. punkts.

680 Turpat, 73.–74. un 96. punkts.

681 Komisijas 2016. gada 12. jūlija Īstenošanas lēmums (ES) 2016/1250 saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK par pienācīgu aizsardzību, ko nodrošina ES un ASV privātuma vairogs, OV L 207. 29. panta darba grupa atzinīgi novērtēja privātuma vairoga mehānisma ietvaros radītos uzlabojumus salīdzinājumā ar lēmumu par drošības zonu un izteica atzinību Komisijai un ASV iestādēm par to, ka privātuma vairoga dokumentu galīgajā versijā ir ņemtas vērā viņu atzinumā WP238 paustās bažas par ES un ASV privātuma vairoga atbilstības lēmuma projektu. Tomēr grupa uzsvēra vairākus neatrisinātus jautājumus. Sīkāku informāciju skatīt 29. panta datu aizsardzības darba grupas *Atzinumā 01/2016 par projektu lēmumam par aizsardzības līmeņa pietiekamību attiecībā uz ES un ASV privātuma vairogu*, kas pieņemts 2016. gada 13. aprīlī, 16/EN WP 238.

682 Plašāka informācija ES un ASV privātuma vairoga faktu lapā.

apņemoties ievērot sistēmas datu aizsardzības standartus. Kompetentās ASV iestādes uzrauga un pārbauda sertificēto uzņēmumu atbilstību šiem standartiem.

Konkrēti, privātuma vairoga shēmā paredzēts:

- datu aizsardzības pienākumi uzņēmumiem, kuri saņem personas datus no ES;
- personu aizsardzība un kaitējuma kompensēšana, jo īpaši no ASV izlūkdienestiem neatkarīga ombuda mehānisma izveidošana, kas nodarbojas ar tādu personu sūdzībām, kuras uzskata, ka ASV iestādes viņu personas datus ir nelikumīgi izmantojušas valsts drošības jomā;
- ikgadējs kopīgs pārskats, lai uzraudzītu regulējuma ieviešanu[683]; pirmā pārskatīšana notika 2017. gada septembrī[684].

ASV valdība ir sniegusi rakstveida apņemšanās un apliecinājumus, kas ir pievienoti lēmumam par privātuma vairogu. Tie paredz ierobežojumus un aizsardzības pasākumus ASV valdības piekļuvei personas datiem tiesībaizsardzības un valsts drošības nolūkos.

7.3.2. Nosūtīšana, kurai piemērojamas attiecīgas garantijas

Gan **ES,** gan **EP tiesību aktos** attiecīgi aizsardzības pasākumi starp datu nosūtītāju pārzini un saņēmēju trešā valstī vai starptautiskā organizācijā ir atzīti kā iespējams līdzeklis, nodrošinot saņēmējam pietiekamu datu aizsardzības līmeni.

Saskaņā ar **ES tiesību aktiem** personas datu nosūtīšana trešai valstij vai starptautiskai organizācijai ir atļauta, ja pārzinis vai apstrādātājs nodrošina attiecīgus aizsardzības pasākumus un īstenojamas tiesības un ja datu subjektiem ir pieejami efektīvi tiesiskās aizsardzības līdzekļi[685]. Pieņemamo "attiecīgo aizsardzības pasākumu" saraksts ir sniegts tikai ES datu aizsardzības tiesību aktos. Attiecīgus aizsardzības pasākumus var noteikt:

683 Plašāka informācija Eiropas Komisijas tīmekļa vietnē par ES un ASV privātuma vairogu.

684 Eiropas Komisija, Komisijas ziņojums Eiropas Parlamentam un Padomei saistībā ar pirmo gada pārskatu par ES un ASV privātuma vairoga darbību COM(2017) 611 *final*, 2017.gada 18. oktobris. Skatīt arī 29. panta darba grupa, *ES un ASV privātuma vairoga pirmais ikgadējais kopējais pārskats*, pieņemts 2017. gada 28. novembrī, 17/EN WP 255.

685 Vispārīgā datu aizsardzības regula, 46. pants.

- starp publiskām iestādēm vai struktūrām juridiski saistošā un tiesiski īstenojamā instrumentā;
- saistošajos uzņēmuma noteikumos;
- standarta datu aizsardzības klauzulās, kuras pieņēmusi vai nu Eiropas Komisija, vai uzraudzības iestāde;
- rīcības kodeksos;
- sertifikācijas mehānismos[686].

Pielāgotas līguma klauzulas starp pārzini vai apstrādātāju ES un datu saņēmēju trešā valstī ir vēl viens veids, kā nodrošināt attiecīgus aizsardzības pasākumus. Tomēr šādas līguma klauzulas jāapstiprina kompetentajai uzraudzības iestādei, pirms tās var izmantot kā personas datu nosūtīšanas instrumentu. Tāpat valsts iestādes var izmantot datu aizsardzības noteikumus, kas ietverti to administratīvajās vienošanās, ja uzraudzības iestāde tos ir apstiprinājusi[687].

Saskaņā ar EP tiesību aktiem datu plūsma uz valsti vai starptautisku organizāciju, kas nav modernizētās Konvencijas Nr. 108 līgumslēdzēja puse, ir atļauta, ja tiek nodrošināts attiecīgs aizsardzības līmenis. To var panākt, izmantojot:

- valsts vai starptautiskas organizācijas tiesību aktus; vai
- *ad hoc* vai standartizētus aizsardzības pasākumus, kas iestrādāti juridiski saistošā dokumentā[688].

Datu nosūtīšana saskaņā ar līguma klauzulām

Gan **EP,** gan **ES tiesību aktos** līguma klauzulas starp datu nosūtītāju pārzini un saņēmēju trešā valstī ir atzīti kā iespējams līdzeklis, nodrošinot saņēmējam pietiekamu datu aizsardzības līmeni[689].

686 Vispārīgā datu aizsardzības regula, 46. panta 1. punkta c) un d) apakšpunkts, 2. punkta a), b), e) un f) apakšpunkts un 47. pants.

687 Turpat, 46. panta 3. punkts.

688 Modernizētā Konvencija Nr. 108, 14. panta 3. punkta b) apakšpunkts.

689 Vispārīgā datu aizsardzības regula, 46. panta 3. punkts; modernizētā Konvencija Nr. 108, 14. panta 3. punkta b) apakšpunkts.

ES mērogā Eiropas Komisija ar 29. panta darba grupas palīdzību izstrādāja standarta datu aizsardzības klauzulas, kuras oficiāli apstiprinātas ar Komisijas lēmumu kā atbilstošas datu aizsardzības pierādījums[690]. Tā kā Komisijas lēmumi dalībvalstīs ir saistoši pilnībā, valsts iestādēm, kas uzrauga datu nosūtīšanu, savās procedūrās ir jāatzīst šīs līguma standartklauzulas[691]. Tādējādi, ja datu nosūtītājs pārzinis un saņēmējs trešā valstī vienojas un paraksta šīs klauzulas, tam būtu jāsniedz uzraudzības iestādei pietiekams pierādījums, ka ir ieviesti atbilstoši aizsardzības pasākumi. Tomēr lietā *Schrems* EST uzskatīja, ka Eiropas Komisija nav kompetenta ierobežot valstu uzraudzības iestāžu pilnvaras uzraudzīt personas datu nosūtīšanu trešai valstij, uz kuru attiecas Komisijas lēmums par aizsardzības līmeņa pietiekamību[692]. Tādējādi valstu uzraudzības iestādēm nav liegts izmantot savas pilnvaras, tostarp pilnvaras apturēt vai aizliegt personas datu nosūtīšanu, ja nosūtīšana tiek veikta, pārkāpjot ES vai valstu datu aizsardzības tiesību aktus, piemēram, ja datu saņēmējs neievēro līguma standartklauzulas[693].

Standarta datu aizsardzības klauzulu esamība ES tiesiskajā regulējumā neliedz pārziņiem formulēt citas *ad hoc*, individuālas līguma klauzulas, ciktāl uzraudzības iestāde tās ir apstiprinājusi[694]. Taču viņiem jānodrošina tāds pats aizsardzības līmenis, kāds paredzēts standarta datu aizsardzības klauzulās. Apstiprinot *ad hoc* klauzulas, uzraudzības iestādēm jāpiemēro konsekvences mehānisms, lai nodrošinātu visā ES konsekventu regulatīvo pieeju[695]. Tas nozīmē, ka kompetentajai uzraudzības iestādei jāinformē EDAK par lēmuma projektu par klauzulām. EDAK sniegs atzinumu par šo jautājumu, un uzraudzības iestādei, pieņemot lēmumu, tas maksimāli jāņem vērā. Ja tā neplāno ievērot EDAK atzinumu, EDAK tiek iedarbināts strīdu izšķiršanas mehānisms, un kolēģija pieņem saistošu lēmumu[696].

Līguma standartklauzulās vissvarīgākās iezīmes ir šādas:

690 Turpat, 46. panta 2. punkta b) apakšpunkts un 46. panta 5. punkts.

691 Turpat, 46. panta 3. punkts.

692 EST 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems pret Datu aizsardzības komisāru* [GC], 96.–98. un 102.–105. punkts.

693 Lai ņemtu vērā EST nostāju lietā *Schrems*, Komisija grozīja lēmumu par līguma standartklauzulām. Komisijas 2016. gada 16. decembra Īstenošanas lēmums (ES) 2016/2297, ar ko groza Lēmumus 2001/497/EK un 2010/87/ES par līguma standartklauzulām attiecībā uz personas datu nosūtīšanu trešām valstīm un šādās valstīs reģistrētiem apstrādātājiem saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK, OV 2016 L 344.

694 Vispārīgā datu aizsardzības regula, 46. panta 3. punkta a) apakšpunkts.

695 Turpat, 63. pants un 64. panta 1. punkta e) apakšpunkts.

696 Turpat, 64. un 65. pants.

- trešās personas saņēmēja klauzula, kas ļauj datu subjektiem īstenot līgumiskās tiesības, pat ja viņi nav līgumslēdzējas puses;

- datu saņēmējs vai importētājs strīda gadījumā piekrīt pakļauties datu nosūtītāja pārziņa valsts uzraudzības iestādei un/vai tiesām.

Šobrīd datu nosūtīšanai no viena pārziņa otram ir pieejami divi standartklauzulu komplekti, no kuriem datu nosūtītājs pārzinis var izvēlēties[697]. Nosūtīšanai no pārziņa apstrādātājam ir tikai viens līguma standartklauzulu komplekts[698]. Tomēr attiecībā uz šīm līguma standartklauzulām pašlaik noris tiesvedība.

Piemērs. Pēc tam, kad EST pasludināja lēmumu par drošības zonu par spēkā neesošu[699], personas datu nosūtīšanu uz ASV vairs nevarēja balstīt šajā lēmumā par aizsardzības līmeņa pietiekamību. Kamēr notika sarunas ar ASV iestādēm un vēl nebija pieņemts jauns lēmums par aizsardzības līmeņa pietiekamību (visbeidzot pieņemts 2016. gada 12. jūlijā)[700], nosūtīšanu varēja veikt tikai, izmantojot citu juridisko pamatu, piemēram, līguma standartklauzulas vai saistošos uzņēmuma noteikumus. Vairāki uzņēmumi, tostarp *Facebook Ireland* (pret kuru tika ierosināta lieta, kuras rezultātā lēmums par drošības zonu tika atzīts par spēkā neesošu), turpināja datu nosūtīšanu no ES uz ASV, izmantojot līguma standartklauzulas.

Schrems kungs iesniedza sūdzību Īrijas uzraudzības iestādei, lūdzot apturēt datu nosūtīšanu uz ASV, pamatojoties uz līguma standartklauzulām. Būtībā viņš apgalvoja, ka, nosūtot viņa personas datus no *Facebook* Īrijas

697 I komplekts ir ietverts Pielikumā (Eiropas Komisija, 2001) Komisijas 2001. gada 15. jūnija Lēmumam 2001/497/EK par līguma standartklauzulām attiecībā uz personas datu nosūtīšanu trešām valstīm saskaņā ar Direktīvu 95/46/EK, OV 2001 L 181; II komplekts ir ietverts Pielikumā (Eiropas Komisija, 2004) Komisijas 2004. gada 27. decembra Lēmumam 2004/915/EK, ar ko groza Lēmumu 2001/497/EK attiecībā uz alternatīvu līguma standartklauzulu ieviešanu personas datu nosūtīšanai trešām valstīm, OV 2004 L 385.

698 Eiropas Komisija (2010), Komisijas 2010. gada 5. februāra Lēmums 2010/87/ES par līguma standartklauzulām attiecībā uz personas datu pārsūtīšanu trešās valstīs reģistrētiem apstrādātājiem saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK, OV 2010 L 39. Rokasgrāmatas izstrādes laikā par līguma standartklauzulu izmantošanu par pamatu personas datu nosūtīšanai uz ASV noritēja tiesvedība Īrijas Augstākajā tiesā *High Court*.

699 EST 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximillian Schrems pret Datu aizsardzības komisāru* [GC].

700 Komisijas 2016. gada 12. jūlija Īstenošanas lēmums (ES) 2016/1250 saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK par pienācīgu aizsardzību, ko nodrošina ES un ASV privātuma vairogs, OV L 207.

meitasuzņēmuma *Facebook Inc.* uz serveriem, kas atrodas ASV, nebija garantijas, ka tie tiks aizsargāti. *Facebook Inc.* ir saistoši Amerikas tiesību akti, kas uzņēmumam varētu uzlikt pienākumu izpaust personas datus ASV tiesībaizsardzības iestādēm, un indivīdiem no Eiropas nav pieejami tiesiskās aizsardzības līdzekļi, ar ko apstrīdēt šo praksi[701]. Šo iemeslu dēļ EST secināja, ka lēmums par drošības zonu ir spēkā neesošs, un, lai arī tiesas spriedums skāra tikai šā lēmuma pārbaudi, prasītājs uzskatīja, ka izvirzītie jautājumi ir būtiski, ja nodošana ir balstīta uz līguma klauzulām. Rokasgrāmatas sastādīšanas laikā lieta tika izskatīta Īrijas Augstākajā tiesā. Acīmredzot prasītājs plāno vērsties EST, kur viņa mērķis ir apstrīdēt Eiropas Komisijas lēmuma par līguma standartklauzulām spēkā esamību. Kā aprakstīts 5. nodaļā, tikai EST ir kompetenta pasludināt kādu ES instrumentu par spēkā neesošu.

Nosūtīšana saskaņā ar saistošiem uzņēmuma noteikumiem

ES tiesību akti pieļauj arī personas datu nosūtīšanu, pamatojoties uz saistošiem uzņēmuma noteikumiem starptautiskai datu nosūtīšanai vienas uzņēmumu grupas ietvaros vai starp uzņēmumiem, kurus saista kopīga saimnieciskā darbība[702]. Pirms atsaukties uz saistošajiem uzņēmuma noteikumiem kā uz personas datu pārsūtīšanas instrumentu, kompetentajai uzraudzības iestādei tie ir jāapstiprina atbilstoši saistošajiem uzņēmuma noteikumiem, izmantojot konsekvences mehānismu.

Lai saistošos uzņēmuma noteikumus varētu apstiprināt, tiem jābūt juridiski saistošiem, tiem jāaptver visi būtiskie datu aizsardzības principi un tie jāpiemēro un jāīsteno visiem grupas dalībniekiem. Tiem ir skaidri jāpiešķir datu subjektiem īstenojamas tiesības, jāietver visi būtiskie datu aizsardzības principi un jāatbilst noteiktām formālām prasībām, piemēram, jābūt norādītai uzņēmuma struktūrai, jāapraksta datu nodošana un tas, kā tiks piemēroti datu aizsardzības principi. Šeit ietilpst šādas informācijas sniegšana datu subjektiem. Saistošajos uzņēmuma noteikumos cita starpā jāprecizē datu subjektu tiesības un normas par atbildību par noteikumu pārkāpumiem[703]. Apstiprinot saistošos uzņēmuma noteikumus, tiks iedarbināts konsekvences mehānisms uzraudzības iestāžu sadarbībai (aprakstīts 5. nodaļā).

Konsekvences mehānisma ietvaros vadošā uzraudzības iestāde pārskata ierosinātos saistošos uzņēmuma noteikumus, pieņem lēmuma projektu un informē par to EDAK.

701 Plašāka informācija pārskatītajā sūdzībā pret *Facebook Ireland Ltd*, kuru *Maximilian Schrems* 2015. gada 1. decembrī iesniedza Īrijas Datu aizsardzības komisāram.

702 Vispārīgā datu aizsardzības regula, 47. pants.

703 Vairāk informācijas Vispārīgās datu aizsardzības regulas 47. pantā.

Kolēģija izdod atzinumu par šo jautājumu, un vadošā uzraudzības iestāde var oficiāli apstiprināt saistošos uzņēmuma noteikumus, "maksimāli ņemot vērā" kolēģijas atzinumu. Šis atzinums nav juridiski saistošs, taču, ja uzraudzības iestāde neplāno ņemt vērā atzinumu, tiek iedarbināts strīdu izšķiršanas mehānisms un kolēģijai būs jāpieņem juridiski saistošs lēmums ar divu trešdaļu tās locekļu balsu vairākumu[704].

Saskaņā ar **EP tiesību aktiem** *ad hoc* vai standartizēti aizsardzības pasākumi, kas ir iestrādāti juridiski saistošā dokumentā[705], ietver arī saistošos uzņēmuma noteikumus.

7.3.3. Atkāpes īpašās situācijās

Saskaņā ar ES tiesību aktiem personas datu nosūtīšana trešai valstij var būt attaisnojama pat tad, ja nav pieņemts atbilstošs lēmums vai aizsardzības pasākumi, piemēram, līguma standartklauzulas vai saistošie uzņēmuma noteikumi, jebkurā no šiem gadījumiem:

- datu subjekts nepārprotami piekrīt datu nosūtīšanai;
- datu subjekts uzsāk vai gatavojas uzsākt līgumattiecības, kas ietver datu nosūtīšanu uz ārzemēm;
- lai noslēgtu līgumu starp datu pārzini un trešo personu datu subjekta interesēs;
- svarīgu sabiedrības interešu dēļ;
- lai celtu, īstenotu vai aizstāvētu likumīgas prasības;
- lai aizsargātu datu subjekta vitālās intereses;
- datu nosūtīšanai no publiskiem reģistriem (šādā gadījumā svarīgāka ir plašas sabiedrības interese piekļūt publiskajos reģistros glabātajai informācijai)[706].

Ja nav piemērojams neviens no šiem nosacījumiem un nosūtīšanu nevar pamatot ar lēmumu par aizsardzības līmeņa pietiekamību vai attiecīgiem aizsardzības

704 Turpat, 57. panta 1. punkta s) apakšpunkts, 58. panta 1. punkta j) apakšpunkts, 64. panta 1. punkta f) apakšpunkts, 65. panta 1. un 2. punkts.

705 Modernizētā Konvencija Nr. 108, 14. panta 3. punkta b) apakšpunkts.

706 Vispārīgā datu aizsardzības regula, 49. pants.

pasākumiem, nosūtīšanu var veikt tikai tad, ja tā neatkārtojas, attiecas uz ierobežotu skaitu datu subjektu un ir nepieciešama, lai aizstāvētu datu pārziņa būtiskas leģitīmas intereses, ar nosacījumu, ka datu subjekta tiesības nav svarīgākas par tām[707]. Šajos gadījumos pārzinim jānovērtē ar nosūtīšanu saistītie apstākļi un jānodrošina aizsardzības pasākumi. Tam jāinformē arī uzraudzības iestāde un skartie datu subjekti gan par nosūtīšanu, gan par tās pamatā esošajām leģitīmajām interesēm.

Fakts, ka atkāpes ir galējais likumīgas datu nosūtīšanas līdzeklis[708] (izmantojams tikai tad, ja nav pieņemts lēmums par aizsardzības līmeņa pietiekamību, kā arī nav citu garantiju), izceļ to izņēmuma raksturu, kas jo īpaši uzsvērts VDAR apsvērumos[709]. Pašas par sevi atkāpes tiek pieņemtas kā iespēja, kas "ļauj nosūtīt datus noteiktos gadījumos", balstoties uz piekrišanu, un gadījumos, kad "nosūtīšana ir gadījuma rakstura un nepieciešama"[710] saistībā ar līgumu vai likumīgu prasību.

Turklāt saskaņā ar 29. panta darba grupas norādījumiem atsaukšanās uz atkāpēm konkrētās situācijās drīkst būt tikai izņēmuma kārtā, pamatojoties uz atsevišķiem gadījumiem, un tās nevar izmantot masveidā vai atkārtoti nosūtot[711]. Eiropas Datu aizsardzības uzraudzītājs arī uzsvēris atkāpju izņēmuma raksturu, izmantojot tās kā nosūtīšanas juridisko pamatu saskaņā ar Regulu (EK) Nr. 45/2001, atzīmējot, ka šis risinājums ir jāizmanto "atsevišķos gadījumos" un "nosūtīšanai, kam ir gadījuma raksturs"[712].

Piemērs. Globālās izplatīšanas sistēmas (*GDS*) pakalpojumu sniedzējs, proti, uzņēmums, kura galvenā mītne atrodas ASV, nodrošina tiešsaistes rezervēšanas sistēmu daudzām aviosabiedrībām, viesnīcām un kruīziem visā pasaulē, apstrādājot desmitiem miljonu personu datus ES. Sākotnēji, nosūtot datus uz saviem serveriem ASV, *GDS* uzņēmums atsaucas uz atkāpi kā likumīgu nosūtīšanas pamatu, t. i., nepieciešamību noslēgt līgumu. Tādējādi uzņēmums nepiedāvā nekādus citus aizsardzības pasākumus datiem, kuru

707 Turpat.

708 Turpat, 49. panta 1. punkts.

709 Skatīt Vispārīgās datu aizsardzības regulas 49. panta 1. punkta a), b) un e) apakšpunktu un 113. apsvērumu.

710 Turpat.

711 29. panta darba grupa (2005), *Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta vienotu interpretāciju*, WP 114, Brisele, 2005. gada 25. novembris.

712 Eiropas Datu aizsardzības uzraudzītājs, *Personas datu nosūtīšana trešām valstīm un starptautiskām organizācijām, ko veic ES iestādes un struktūras*, nostājas dokuments, Brisele, 2014. gada 14. jūlijs, 15. lpp.

izcelsme ir Eiropa un ko nosūta uz ASV un pēc tam atkārtoti izplata viesnīcām visā pasaulē (tas nozīmē, ka nav arī aizsardzības pasākumu tālākai nosūtīšanai). Uzņēmums *GDS* neievēro VDAR noteiktās prasības likumīgai starptautiskai datu nosūtīšanai, jo atsaucas uz atkāpi kā likumīgu pamatu masveida nosūtīšanai.

Ja nav pieņemts lēmums par aizsardzības līmeņa pietiekamību, ES vai tās dalībvalstis ir pilnvarotas noteikt ierobežojumus īpašu kategoriju personas datu nosūtīšanai trešai valstij svarīgu sabiedrības interešu dēļ neatkarīgi no citiem šādas nosūtīšanas nosacījumiem. Šie ierobežojumi būtu jāuztver kā izņēmuma gadījumi, un dalībvalstīm tiek prasīts informēt Komisiju par attiecīgajiem noteikumiem[713].

EP tiesību aktos ir pieļauta datu plūsma uz teritorijām, kurās nav attiecīgas datu aizsardzības šādos gadījumos:

- datu subjekts ir sniedzis piekrišanu;
- datu nosūtīšana nepieciešama datu subjekta interesēs;
- pastāv svarīgākas leģitīmās intereses, jo īpaši svarīgas sabiedrības intereses, kas paredzētas likumā;
- tas ir nepieciešams un samērīgs pasākums demokrātiskā sabiedrībā[714].

7.3.4. Nosūtīšana, pamatojoties uz starptautiskajiem nolīgumiem

ES var noslēgt starptautiskus nolīgumus ar trešām valstīm, ar ko regulē personas datu nosūtīšanu konkrētos nolūkos. Šajos nolīgumos jāietver attiecīgi aizsardzības pasākumi, lai nodrošinātu attiecīgo personu personas datu aizsardzību. VDAR pastāv, neskarot šos starptautiskos nolīgumus[715].

713 Skatīt Vispārīgās datu aizsardzības regulas 49. panta 5. punktu.

714 Modernizētā Konvencija Nr. 108, 14. panta 4. punkts.

715 Vispārīgā datu aizsardzības regula, 102. apsvērums.

Dalībvalstis var arī noslēgt starptautiskus nolīgumus ar trešām valstīm vai starptautiskām organizācijām, kas nodrošina pienācīgu personu pamattiesību un brīvību aizsardzības līmeni, ciktāl šie nolīgumi neietekmē VDAR piemērošanu.

Līdzīgs noteikums ir paredzēts modernizētās Konvencijas Nr. 108 12. panta 3. punkta a) apakšpunktā.

Starptautisko nolīgumu, kas saistīti ar personas datu nosūtīšanu, piemēri ir pasažieru datu reģistra (PDR) nolīgumi.

Pasažieru datu reģistrs

Gaisa pārvadātāji PDR datus vāc lidojuma rezervācijas procesa laikā, un tajos cita starpā iekļauj gaisa pasažieru vārdus, adreses, kredītkartes datus un sēdvietu numurus. Gaisa pārvadātāji vāc šo informāciju arī saviem komerciāliem nolūkiem. ES ir noslēgusi nolīgumus ar dažām trešām valstīm (Austrāliju, Kanādu un ASV) par PDR datu nosūtīšanu, lai novērstu, atklātu, izmeklētu teroristu nodarījumus vai smagus starptautiskus noziegumus, kā arī sauktu pie atbildības par tiem. Turklāt Savienība 2016. gadā pieņēma Direktīvu (ES) 2016/861, kas zināma kā ES PDR direktīva[716]. Ar šo direktīvu nodrošina tiesisko regulējumu ES dalībvalstīm, nosūtot PDR datus kompetentām iestādēm trešās valstīs, līdzīgi nolūkā novērst, atklāt, izmeklēt teroristu nodarījumus un smagus noziegumus vai saukt pie atbildības par tiem. PDR nosūtīšana trešo valstu iestādēm tiek veikta katrā atsevišķā gadījumā, un tiek individuāli vērtēts, vai nosūtīšana ir nepieciešama direktīvā noteiktos nolūkos, un ar nosacījumu, ka tiek ievērotas pamattiesības.

Attiecībā uz PDR nolīgumiem starp ES un trešām valstīm ir tikusi apstrīdēta to saderība ar ES Pamattiesību hartā noteiktajām pamattiesībām uz privātumu un datu aizsardzību. Kad pēc sarunām ar Kanādu ES 2014. gadā parakstīja nolīgumu par PDR datu nosūtīšanu un apstrādi, Eiropas Parlaments nolēma nodot lietu EST, lai izvērtētu nolīguma likumību attiecībā uz ES tiesību aktiem un jo īpaši Hartas 7. un 8. punktu.

716 Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Direktīva (ES) 2016/681 par pasažieru datu reģistra (PDR) datu izmantošanu teroristu nodarījumu un smagu noziegumu novēršanai, atklāšanai, izmeklēšanai un saukšanai pie atbildības par tiem, OV 2016 L 119.

Piemērs. EST savā atzinumā par ES un Kanādas PDR apstrādes nolīguma likumību[717] uzskatīja, ka paredzētais nolīgums pašreizējā formā nav savienojams ar Hartā atzītajām pamattiesībām, tāpēc to nedrīkstēja noslēgt. Tā kā nolīgums bija saistīts ar personas datu apstrādi, tas iejaucās Hartas 8. pantā aizsargātajās tiesībās uz personas datu aizsardzību. Tajā pašā laikā tas ir arī 7. pantā noteikto tiesību uz privātās dzīves neaizskaramību ierobežojums, ņemot vērā, ka kopumā PDR datus var apkopot un analizēt veidā, kas atklāj ceļošanas paradumus, attiecības starp dažādiem indivīdiem, informāciju par viņu finansiālo stāvokli, ēšanas paradumiem un veselības stāvokli, tādējādi ietekmējot viņu privāto dzīvi.

Iejaukšanās pamattiesībās paredzētā nolīguma ietvaros tika īstenota vispārējas nozīmes mērķim, proti, sabiedrības drošības interesēs un cīņai pret terorismu un smagiem starpvalstu noziegumiem. Tomēr EST atgādināja, ka iejaukšanās ir pamatota tikai tad, ja tā ir absolūti nepieciešama izvirzītā mērķa sasniegšanai. Pēc nolīguma nosacījumu analīzes EST secināja, ka paredzētais nolīgums neatbilst "absolūtas nepieciešamības" kritērijam. Starp faktoriem, kas EST lika izdarīt šādu secinājumu, bija šādi:

- Fakts, ka paredzētais nolīgums ietvēra sensitīvu datu nosūtīšanu. Paredzētā nolīguma vietā vāktais PDR varētu ietvert sensitīvus datus, piemēram, informāciju, kas atklāj rasi vai etnisko izcelsmi, reliģisko pārliecību vai informāciju par pasažiera veselības stāvokli. Sensitīvu datu nosūtīšana un apstrāde, ko veic Kanādas iestādes, varētu apdraudēt nediskriminācijas principu, un tāpēc ir nepieciešams precīzs un drošs pamatojums, kas nav balstīts sabiedrības drošības un cīņas pret smagiem noziegumiem apsvērumos. Paredzētajā nolīgumā nav paredzēts šāds pamatojums[718].

- Tika uzskatīts, ka arī turpmāka visu pasažieru PDR datu glabāšana piecus gadus pēc pasažieru izlidošanas no Kanādas pārsniedz absolūtas nepieciešamības robežas. EST uzskatīja, ka Kanādas iestādes drīkstētu glabāt datus par pasažieriem, attiecībā uz kuriem ir objektīvi pierādījumi, ka viņi var radīt draudus sabiedrības drošībai, pat pēc šo personu aizbraukšanas no Kanādas. Turpretī *visu* pasažieru personas datu glabāšana, par kuriem nav pat netiešu pierādījumu par sabiedrības drošības apdraudējumu, nav pamatota[719].

717 EST, *Tiesas (virspalātas) atzinums 1/15*, 2017. gada 26. jūlijs.

718 Turpat, 165. punkts.

719 Turpat, 204.–207. punkts.

Konvencijas Nr. 108 konsultatīvā komiteja ir sniegusi atzinumu par PDR nolīgumu datu aizsardzības sekām saskaņā ar Eiropas Padomes tiesību aktiem[720].

Ziņojumapmaiņas dati

Beļģijā bāzētā Vispasaules Starpbanku finanšu telekomunikāciju sabiedrība (*SWIFT*), kura apstrādā lielāko daļu pasaules naudas pārskaitījumu no Eiropas bankām, darbojās, izmantojot operāciju centru ASV, un saņēma pieprasījumu izpaust datus ASV Valsts kases departamentam terorisma izmeklēšanas nolūkiem saskaņā ar Teroristu finansēšanas izsekošanas programmu[721].

No ES viedokļa nebija pietiekama juridiskā pamata, lai šos datus, galvenokārt par ES pilsoņiem, izpaustu ASV tikai tāpēc, ka viens no *SWIFT* datu pakalpojumu apstrādes centriem atradās šajā valstī.

Starp ES un ASV 2010. gadā tika noslēgts īpašs nolīgums, kas pazīstams kā *SWIFT* nolīgums, lai nodrošinātu nepieciešamo juridisko pamatu un nodrošinātu atbilstošus datu aizsardzības standartus[722].

Saskaņā ar šo nolīgumu *SWIFT* glabātie finanšu dati joprojām tiek sniegti ASV Valsts kases departamentam terorisma vai teroristu finansēšanas novēršanas, izmeklēšanas, atklāšanas vai kriminālvajāšanas nolūkā. ASV Valsts kases departaments var pieprasīt *SWIFT* izsniegt finanšu datus ar nosacījumu, ka pieprasījums:

- pēc iespējas skaidri identificē finanšu datus;
- skaidri pamato datu nepieciešamību;

720 Eiropas Padome, *Atzinums par Pasažieru datu reģistra apstrādes datu aizsardzības sekām*, T-PD(2016)18rev, 2016. gada 19. augusts.

721 Šajā kontekstā skatīt 29. panta darba grupas (2011) *Atzinumu 14/2011 par datu aizsardzības jautājumiem, kas attiecas uz nelikumīgi iegūtu līdzekļu legalizēšanas un terorisma finansēšanas novēršanu*, WP 186, Brisele, 2011. gada 13. jūnijs; 29. panta darba grupas (2006) *Atzinumu 10/2006 par personas datu apstrādi, ko veic Vispasaules Starpbanku finanšu telekomunikāciju sabiedrība (SWIFT)*, WP 128, Brisele, 2006. gada 22. novembris; Beļģijas Komisijas privātās dzīves aizsardzībai (*Commission de la protection de la vie privée*) (2008) 2008. gada 9. decembra lēmumu "*Kontroles un ieteikuma procedūra, kas sākta attiecībā uz uzņēmumu SWIFT scrl*".

722 Padomes 2010. gada 13. jūlija Lēmums 2010/412/ES par to, lai noslēgtu Nolīgumu starp Eiropas Savienību un Amerikas Savienotajām Valstīm par tādu finanšu ziņojumapmaiņas datu apstrādi un nodošanu, kurus Eiropas Savienība dara pieejamus ASV, lai īstenotu Teroristu finansēšanas izsekošanas programmu, OV 2010 L 195, 3. un 4. lpp. Nolīguma teksts ir pievienots šim lēmumam, OV 2010 L 195, 5.–14. lpp.

- ir pielāgots pēc iespējas šauri, lai samazinātu pieprasīto datu daudzumu;

- neprasa izsniegt datus par Vienoto euro maksājumu telpu (*SEPA*)[723].

Eiropolam jāsaņem ikviena ASV Valsts kases departamenta pieprasījuma kopija un jāpārbauda, vai tiek ievēroti *SWIFT* nolīguma principi[724]. Ja tas tiek apstiprināts, *SWIFT* ir jāsniedz finanšu dati tieši ASV Valsts kases departamentam. Departamentam finanšu dati jāuzglabā drošā fiziskā vidē, kur tiem var piekļūt tikai analītiķi, kuri izmeklē terorismu vai tā finansēšanu, un finanšu dati nedrīkst būt savienoti ar citām datubāzēm. Parasti no *SWIFT* saņemtie finanšu dati ir jādzēš ne vēlāk kā piecus gadus pēc to saņemšanas. Finanšu datus, kas attiecas uz konkrētu izmeklēšanu vai kriminālvajāšanu, var glabāt tikai tik ilgi, kamēr dati ir nepieciešami šai izmeklēšanai vai kriminālvajāšanai.

ASV Valsts kases departaments var nosūtīt informāciju no *SWIFT* saņemtajiem datiem konkrētām tiesībaizsardzības, sabiedriskās drošības vai pretterorisma iestādēm ASV vai ārpus tās tikai terorisma un tā finansēšanas izmeklēšanas, atklāšanas, novēršanas vai kriminālvajāšanas nolūkos. Ja finanšu datu tālākā nosūtīšanā ir iesaistīts kāds ES dalībvalsts pilsonis vai pastāvīgais iedzīvotājs, jebkādai datu kopīgai izmantošanai ar trešās valsts iestādēm ir vajadzīga iepriekšēja attiecīgās dalībvalsts kompetento iestāžu piekrišana. Izņēmumi var tikt pieļauti, ja datu apmaiņa ir būtiska, lai novērstu tiešus un nopietnus draudus sabiedrības drošībai.

Neatkarīgi pārraugi, tostarp Eiropas Komisijas iecelta persona, uzrauga *SWIFT* nolīguma principu ievērošanu. Viņiem ir iespēja reālā laikā un ar atpakaļejošu datumu pārskatīt visus sniegto datu meklējumus, pieprasīt papildu informāciju, lai pamatotu šo meklējumu saistību ar terorismu, kā arī pilnvaras bloķēt jebkādus meklējumus, kas, šķiet, pārkāpj nolīgumā noteiktos drošības pasākumus.

Datu subjektiem ir tiesības saņemt no kompetentās ES uzraudzības iestādes apstiprinājumu, ka ir ievērotas viņu personas datu aizsardzības tiesības. Datu subjektiem ir arī tiesības labot, dzēst vai bloķēt savus datus, ko saskaņā ar *SWIFT* nolīgumu ir savācis un glabā ASV Valsts kases departaments. Tomēr uz datu subjektu piekļuves tiesībām var attiekties daži juridiski ierobežojumi. Ja piekļuvi atsaka, datu subjekts rakstiski jāinformē par atteikumu, kā arī viņa tiesībām uz administratīviem un tiesiskās aizsardzības līdzekļiem ASV.

723 Turpat, 4. panta 2. punkts.

724 Eiropola Apvienotā uzraudzības iestāde ir veikusi revīzijas par Eiropola darbībām šajā jomā.

SWIFT nolīgums ir spēkā piecus gadus, tā pirmais darbības termiņš bija līdz 2015. gada augustam. Tas automātiski pagarinās uz nākamajiem viena gada periodiem, ja vien kāda no pusēm vismaz sešus mēnešus iepriekš neinformē otru par nodomu nepagarināt nolīgumu. Automātiskā pagarināšana tika piemērota 2015. gada, 2016. gada un 2017. gada augustā, un tādējādi *SWIFT* nolīguma spēkā esamība ir nodrošināta vismaz līdz 2018. gada augustam[725].

725 Turpat, 23. panta 2. punkts.

8

Datu aizsardzība policijas un krimināltiesību kontekstā

ES	Aptvertie jautājumi	EP
Datu aizsardzības direktīva policijas un krimināltiesību jomā	**Vispārīgi**	Modernizētā Konvencija Nr. 108
	Policija	Policijas ieteikums Praktiskas norādes par personas datu lietojumu policijas jomā
	Uzraudzība	ECT lieta *B.B. pret Franciju* [GC], Nr. 5335/06, 2009 ECT lieta *S. un Marper pret Apvienoto Karalisti* [GC], Nr. 30562/04 un Nr. 30566/04, 2008 ECT lieta *Allan pret Apvienoto Karalisti*, Nr. 48539/99, 2002 ECT lieta *Mallon pret Apvienoto Karalisti*, Nr. 8691/79, 1984 ECT lieta *Klass un citi pret Vāciju*, Nr. 5029/71, 1978 ECT lieta *Szabo un Vissy pret Ungāriju*, Nr. 37138/14, 2016 ECT lieta *Vetter pret Franciju*, Nr. 59842/00, 2005
	Kibernoziedzība	Konvencija par kibernoziedzību

ES	Aptvertie jautājumi	EP
Citi īpaši tiesību instrumenti		
Prīmes lēmums	**Īpašiem datiem: pirkstu nospiedumi, DNS, huligānisms, informācija par gaisa pārvadājumu pasažieriem, telekomunikāciju dati u. tml.**	Modernizētā Konvencija Nr. 108, 6. pants Policijas ieteikums, Praktiskas norādes par personas datu lietojumu policijas jomā
Zviedrijas iniciatīva (Padomes Pamatlēmums 2006/960/TI)	**Informācijas un izlūkdatu apmaiņas vienkāršošana starp tiesībaizsardzības iestādēm**	ECT lieta *S. un Marper pret Apvienoto Karalisti* [GC], Nr. 30562/04 un Nr. 30566/04, 2008
Direktīva (ES) 2016/681 par pasažieru datu reģistra (PDR) datu izmantošanu teroristu nodarījumu un smagu noziegumu novēršanai, atklāšanai, izmeklēšanai un saukšanai pie atbildības par tiem EST apvienotās lietas C-293/12 un C-594/12 *Digital Rights Ireland* un Kärntner Landesregierung un citi [GC], 2014 EST apvienotās lietas C-203/15 un C-698/15 *Tele2 Sverige* un *Home Department pret Tom Watson un citiem* [GC], 2016	**Personas datu saglabāšana**	ECT lieta *B.B. pret Franciju* [GC], Nr. 5335/06, 2009
Eiropola regula *Eurojust* lēmums	**Ko veic īpašas aģentūras**	Policijas ieteikums
Šengenas II lēmums VIS regula *Eurodac* regula MIS lēmums	**Ko veic īpašas kopīgās informācijas sistēmas**	Policijas ieteikums ECT lieta *Dalea pret Franciju*, Nr. 964/07, 2010

Lai līdzsvarotu indivīda datu aizsardzības intereses un sabiedrības intereses vākt datus, lai apkarotu noziedzību un nodrošinātu valsts un sabiedrības drošību, EP un ES ir pieņēmušas konkrētus tiesību instrumentus. Šajā sadaļā sniegts pārskats par EP (8.1. iedaļa) un ES tiesību aktiem (8.2. iedaļa) attiecībā uz datu aizsardzību policijas un krimināltiesību jautājumos.

8.1. EP tiesību akti par datu aizsardzību valsts drošības, policijas un krimināltiesību jautājumos

Svarīgākie aspekti

- Modernizētā konvencija Nr. 108 un EP Policijas ieteikums attiecas uz datu aizsardzību visās policijas darba jomās.
- Konvencija par kibernoziegumiem (Budapeštas konvencija) ir saistošs starptautisks tiesību instruments attiecībā uz noziegumiem, kas izdarīti pret elektroniskajiem tīkliem un izmantojot tos. Tas ir svarīgi arī tādu noziegumu izmeklēšanā, kas nav kibernoziegumi, taču ir saistīti ar elektroniskiem pierādījumiem.

Viena būtiska atšķirība starp EP un ES tiesību aktiem ir tā, ka **EP tiesību akti** atšķirībā no ES tiesību aktiem attiecas arī uz valsts drošības jomu. Tas nozīmē, ka līgumslēdzējām pusēm jāievēro ECK 8. panta tvērums pat attiecībā uz darbībām, kas saistītas ar valsts drošību. Vairāki ECT spriedumi ir bijuši saistīti ar valsts darbībām sensitīvajās valsts drošības tiesību un prakses jomās[726].

Attiecībā uz policijas un krimināltiesību jautājumiem Eiropas mērogā modernizētā Konvencija Nr. 108 attiecas uz visām personas datu apstrādes jomām, un tās noteikumu mērķis ir reglamentēt personas datu apstrādi kopumā. Līdz ar to modernizētā Konvencija Nr. 108 attiecas uz datu aizsardzību policijas un krimināltiesību jomā. Ģenētisko datu, personas datu, kas saistīti ar noziedzīgiem nodarījumiem, kriminālprocesu un notiesājošu spriedumu, un jebkādiem ar to saistītajiem drošības pasākumiem, biometrisko datu, kas unikāli identificē personu, kā arī jebkādu sensitīvu personas datu apstrāde ir atļauta tikai tad, ja pastāv attiecīgi aizsardzības pasākumi pret risku, ka šādu datu apstrāde var ietekmēt datu subjekta intereses, tiesības un pamatbrīvības, jo īpaši diskriminācijas risku[727].

Policijas un krimināltiesību iestāžu tiesisko uzdevumu izpildei nereti ir nepieciešama personas datu apstrāde, kas var nopietni ietekmēt skartās personas. Policijas ieteikumā, ko Eiropas Padome pieņēma 1987. gadā, sniegti norādījumi EP dalībvalstīm

726 Skatīt, piemēram, ECT 1978. gada 6. septembra spriedumu lietā *Klass un citi pret Vāciju*, Nr. 5029/71; ECT 2000. gada 4. maija spriedumu lietā *Rotaru pret Rumāniju* [GC], Nr. 28341/95; un ECT 2016. gada 12. janvāra spriedumu lietā *Szabó un Vissy pret Ungāriju*, Nr. 37138/14.

727 Modernizētā Konvencija Nr. 108, 6. pants.

par to, kā ir jāīsteno Konvencijas Nr. 108 principi saistībā ar personas datu apstrādi, ko veic policijas iestādes[728]. Ieteikumu papildināja praktiskas norādes par personas datu izmantošanu policijas jomā, kuras pieņēmusi Konvencijas Nr. 108 konsultatīvā komiteja[729].

Piemērs. Lietā *D.L. pret Bulgāriju*[730] sociālie dienesti saskaņā ar tiesas rīkojumu ievietoja prasītāju drošā izglītības iestādē. Visai rakstiskai korespondencei un telefona sarunām iestāde veica vispārēju un nekritisku novērošanu. ECT uzskatīja, ka ir pārkāpts 8. pants, ņemot vērā, ka attiecīgais pasākums nebija nepieciešams demokrātiskā sabiedrībā. Tiesa paziņoja, ka bija jādara viss, lai nepilngadīgajiem, kuri ievietoti iestādē, būtu nodrošināts pietiekams kontakts ar ārpasauli, jo tā bija viņu tiesību uz cieņpilnu izturēšanos neatņemama sastāvdaļa un bija absolūti nepieciešama, sagatavojoties viņu reintegrācijai sabiedrībā. Tas attiecās gan uz apmeklējumiem, gan rakstisko korespondenci vai telefona sarunām. Turklāt novērošanā netika nodalīta saziņa ar ģimenes locekļiem un NVO, kas pārstāv bērnu tiesības, vai juristiem. Turklāt lēmums pārtvert saziņu nebija balstīts individualizētā risku analīzē katrā konkrētajā gadījumā.

Piemērs. Lietā *Dragojević pret Horvātiju*[731] prasītājs tika turēts aizdomās par iesaistīšanos narkotiku tirdzniecībā. Viņš tika atzīts par vainīgu pēc tam, kad izmeklēšanas tiesnesis atļāva izmantot slepenus novērošanas pasākumus, lai pārtvertu prasītāja telefona zvanus. ECT uzskatīja, ka pasākums, par kuru tika celta sūdzība, bija iejaukšanās tiesībās uz privātās dzīves un korespondences neaizskaramību. Izmeklēšanas tiesneša piešķirtais pilnvarojums bija balstīts tikai uz prokuratūras apgalvojumu, ka "izmeklēšanu nav iespējams veikt citiem līdzekļiem". ECT arī atzīmēja, ka krimināltiesas savu vērtējumu par novērošanas pasākumu izmantošanu veica šauri un ka valdība nebija noteikusi pieejamos tiesiskās aizsardzības līdzekļus. Līdz ar to bija pārkāpts 8. pants.

728 Eiropas Padomes Ministru komiteja (1987), Ieteikums Rec(87)15 dalībvalstīm, kas regulē personas datu izmantošanu policijas darbā, 1987. gada 17. septembris.

729 Eiropas Padome (2018), Konvencijas Nr. 108 konsultatīvā komiteja, Praktiskas norādes par personas datu lietojumu policijas jomā, T-PD(2018)1.

730 ECT 2016. gada 19. maija spriedums lietā *D.L. pret Bulgāriju*, Nr. 7472/14.

731 ECT 2015. gada 15. janvāra spriedums lietā *Dragojević pret Horvātiju*, Nr. 68955/11.

8.1.1. Policijas ieteikums

ECT konsekventi ir noteikusi, ka personas datu glabāšana un turēšana, ko veic policija vai valsts drošības iestādes, ir iejaukšanās ECTK 8. panta 1. punktā. Daudzos ECT spriedumos aplūkots šādas iejaukšanās pamatojums[732].

Piemērs. Lietā *B.B. pret Franciju*[733] prasītājs bija sodīts par iesaistīšanos dzimumnoziegumos pret 15 gadus vecām nepilngadīgām personām, izmantojot savu uzticības personas stāvokli. Viņš 2000. gadā bija izcietis savu cietumsodu. Gadu vēlāk viņš pieprasīja, lai atsauce uz šo sodu tiktu izņemta no viņa sodāmības reģistra, taču lūgums tika noraidīts. Francijā 2004. gadā ar likumu tika izveidota dzimumnoziedznieku valsts datubāze, un prasītājs tika informēts par viņa iekļaušanu tajā. ECT uzskatīja, ka uz notiesāta dzimumnoziedznieka iekļaušanu valsts tiesu datubāzē attiecas ECTK 8. pants. Tomēr, ņemot vērā to, ka bija ieviesti pietiekami datu aizsardzības pasākumi, piemēram, datu subjekta tiesības pieprasīt datu dzēšanu, ierobežots datu glabāšanas ilgums un ierobežota piekļuve šādiem datiem, bija panākts taisnīgs līdzsvars starp konkurējošām apskatāmajām privātām un sabiedrības interesēm. Tiesa atzina, ka šajā lietā nav pārkāpts ECTK 8. pants.

Piemērs. Lietā *S. un Marper pret Apvienoto Karalisti*[734] abiem prasītājiem bija izvirzītas apsūdzības par noziedzīgiem nodarījumiem, taču viņi par tiem netika notiesāti. Tomēr policija paturēja un uzglabāja viņu pirkstu nospiedumus, šūnu paraugus un DNS profilus. Tiesību akti atļāva neierobežotu iepriekš minēto biometrisko datu saglabāšanu gadījumos, kad persona tika turēta aizdomās par noziedzīgu nodarījumu, pat ja aizdomās turētais vēlāk tika attaisnots vai atbrīvots. ECT sprieda, ka vispārīga un nekritiska personas datu glabāšana, nepiemērojot laika ierobežojumu, un kurā attaisnotajām personām bija tikai ierobežotas iespējas pieprasīt datu dzēšanu, bija nesamērīga iejaukšanās prasītāju tiesībās uz privātās dzīves neaizskaramību. Tiesa secināja, ka ir pārkāpts ECTK 8. pants.

732 Skatīt, piemēram, ECT 1987. gada 26. marta spriedumu lietā *Leander pret Zviedriju*, Nr. 9248/81, ECT 2012. gada 13. novembra spriedumu lietā *M.M. pret Apvienoto Karalisti*, Nr. 24029/07, ECT 2013. gada 18. aprīļa spriedumu lietā *M.K. pret Franciju*, Nr. 19522/09, vai ECT 2017. gada 22. jūnija spriedumu lietā *Aycaguer pret Franciju*, Nr. 8806/12.

733 ECT 2009. gada 17. decembra spriedums lietā *B.B. pret Franciju*, Nr. 5335/06.

734 ECT 2008. gada 4. decembra spriedums lietā *S. un Marper pret Apvienoto Karalisti* [GC], Nr. 30562/04 un Nr. 30566/04, 119. un 125. punkts.

Izšķirošs jautājums elektronisko komunikāciju kontekstā ir valsts iestāžu iejaukšanās privātuma un datu aizsardzības tiesībās. Novērošanas vai sakaru pārtveršanas līdzekļi, piemēram, klausīšanās vai noklausīšanās ierīces, ir pieļaujami tikai tad, ja to paredz likums un ja tas ir nepieciešams pasākums demokrātiskā sabiedrībā, ņemot vērā šādus aspektus:

- valsts drošības aizsardzību;
- sabiedrības drošību;
- valsts monetārās intereses;
- cīņu ar noziedzību; vai
- datu subjekta aizsardzību vai citu personu tiesību un brīvību aizsardzību.

Daudzos citos ECT spriedumos aplūkots, kā tiek pamatota iejaukšanās tiesībās uz privātumu, veicot novērošanu.

Piemērs. Lietā *Allan pret Apvienoto Karalisti*[735] iestādes slepeni ierakstīja privātas sarunas starp ieslodzīto un draugu cietuma apmeklētāju zonā, kā arī ar līdzapsūdzēto cietuma kamerā. ECT uzskatīja, ka audio un videoierakstīšanas ierīču izmantošana prasītāja kamerā, cietuma apmeklējumu zonā un, piestiprinot ieraksta ierīces otram ieslodzītajam, ir uzskatāma par iejaukšanos prasītāja tiesībās uz privāto dzīvi. Tā kā attiecīgajā laikā nebija likumā noteiktas sistēmas, kas reglamentētu slēptu ierakstīšanas ierīču izmantošanu policijā, šāda iejaukšanās neatbilda likumam. Tāpēc tiesa atzina, ka šajā lietā ir pārkāpts ECTK 8. pants.

Piemērs. Lietā *Roman Zakharov pret Krieviju*[736] prasītājs uzsāka tiesvedību pret trim mobilo sakaru tīkla operatoriem. Viņš apgalvoja, ka ir pārkāptas viņa tiesības uz telefona sakaru privātumu, jo operatori bija uzstādījuši iekārtas, kas Federālajam drošības dienestam ļāva pārtvert viņa telefona sakarus bez iepriekšējas tiesas atļaujas. ECT uzskatīja, ka valsts tiesību normas, kas regulē sakaru pārtveršanu, nenodrošināja atbilstošas un efektīvas garantijas pret patvaļu un ļaunprātīgas izmantošanas risku. Īpaši valsts likumos nebija

735 ECT 2002. gada 5. novembra spriedums lietā *Allan pret Apvienoto Karalisti*, Nr. 48539/99.

736 ECT 2015. gada 4. decembra spriedums lietā *Roman Zakharov pret Krieviju* [GC], Nr. 47143/06.

paredzēts pienākums dzēst saglabātos datus pēc tam, kad bija sasniegts glabāšanas mērķis. Turklāt, kaut arī bija nepieciešama tiesas atļauja, tiesas pārbaudi veica ierobežotā apmērā.

Piemērs. Lietā *Szabó un Vissy pret Ungāriju*[737] prasītāji apgalvoja, ka Ungārijas tiesību akti pārkāpj ECTK 8. pantu, jo tie nebija pietiekami detalizēti izstrādāti vai precīzi. Turklāt tika apgalvots, ka tiesību aktos nav nodrošinātas pietiekamas garantijas pret ļaunprātīgu izmantošanu un patvaļu. ECT konstatēja, ka Ungārijas tiesību aktos nav noteikts, ka novērošanai ir nepieciešama tiesas atļauja. Tomēr tiesa atzīmēja, ka, lai gan novērošanai bija nepieciešams tieslietu ministra apstiprinājums, tā bija acīmredzami politiska un nespēja nodrošināt obligāto "absolūtas nepieciešamības" novērtējumu. Turklāt valsts tiesību aktos nebija paredzēta tiesas kontrole, ņemot vērā, ka subjekti netika informēti. Tiesa secināja, ka ir pārkāpts ECTK 8. pants.

Tā kā policijas iestāžu veiktā datu apstrāde var būtiski ietekmēt skartās personas, šajā jomā īpaši nepieciešami precīzi izstrādāti datu aizsardzības noteikumi personas datu apstrādei. EP Policijas ieteikumā ir mēģināts risināt šo jautājumu, sniedzot norādījumus par to, kā personas dati ir jāapkopo policijas darbā; kā šajā jomā ir jāglabā datu faili; kam būtu jāļauj piekļūt šiem failiem, tostarp sniedzot nosacījumus personas datu nosūtīšanai ārvalstu policijas iestādēm; kādām vajadzētu būt datu subjektu iespējām īstenot to datu aizsardzības tiesības; un kādā veidā jāīsteno neatkarīgu iestāžu veiktā kontrole. Tika apsvērts arī pienākums nodrošināt atbilstošu datu drošību.

Ieteikumā nav paredzēta iespēja policijas iestādēm vākt personas datus bez atlases un nekritiski. Saskaņā ar šo ieteikumu policijas iestāžu veikto personas datu vākšana pieļaujama tikai apjomā, kas nepieciešams reālu draudu novēršanai vai kriminālvajāšanai par konkrētu noziedzīgu nodarījumu. Jebkurai papildu datu vākšanai būtu jābūt balstītai konkrētos valsts tiesību aktos. Sensitīvu datu apstrāde ir jāveic tikai tādā apjomā, kas absolūti nepieciešams konkrētas izmeklēšanas kontekstā.

Ja personas dati tiek vākti bez datu subjektu ziņas, datu subjekts jāinformē par datu vākšanu, tiklīdz šāda izpaušana vairs neierobežo izmeklēšanu. Datu vākšanai, izmantojot tehnisko uzraudzību vai citus automatizētus līdzekļus, jābūt īpašam juridiskam pamatam.

737 ECT 2016. gada 12. janvāra spriedums lietā *Szabó un Vissy pret Ungāriju*, Nr. 37138/14.

Piemērs. Lietā *Versini-Campinchi un Crasnianski pret Franciju*[738] prasītājai, kura bija advokāte, bija telefona saruna ar klientu, kura telefona līnija tika pārtverta pēc izmeklēšanas tiesneša pieprasījuma. Sarunas stenogramma parādīja, ka viņa ir izpaudusi informāciju, uz ko attiecas profesionālās konfidencialitātes pienākums. Prokurors šo informāciju nosūtīja advokātu kolēģijai, kas prasītājai piemēroja sodu. ECT atzina, ka ir notikusi iejaukšanās tiesībās uz privātās dzīves un korespondences neaizskaramību ne tikai personai, kuras tālruņa sarunas tika noklausītas, bet arī prasītājai, kuras saziņa tika pārtverta un transkribēta. Iejaukšanās notika saskaņā ar likumu un tai bija likumīgs mērķis – novērst nelikumības. Prasītāja bija saņēmusi telefona sarunu ierakstu stenogrammas iesniegšanas likumības pārbaudi saistībā ar disciplinārlietu, kas tika ierosināta pret viņu. Kaut arī viņai nebija iespējas lūgt anulēt telefona sarunas stenogrammu, ECT uzskatīja, ka ir bijusi efektīva pārbaude, kas varēja ierobežot iejaukšanos, kas bija sūdzības priekšmets, tādā apjomā, kāds nepieciešams demokrātiskā sabiedrībā. ECT nosprieda, ka arguments, ka kriminālprocesa uzsākšanas iespējai pret advokāti, balstoties uz stenogrammu, varētu būt atturošs efekts uz advokātes un viņas klientu savstarpējās saziņas brīvību, tātad arī uz klienta aizstāvības tiesībām, nebija ticams, ja pašas advokātes izpaustā informācija varēja tikt uzskatīta par prettiesisku rīcību no viņas puses. Līdz ar to 8. panta pārkāpums netika konstatēts.

EP Policijas ieteikumā paredzēts, ka, glabājot personas datus, ir skaidri jānošķir administratīvie un policijas dati, dažādu veidu datu subjektu, piemēram, aizdomās turamo, notiesāto, cietušo un liecinieku, personas dati, un dati, kas tiek uzskatīti par reāliem faktiem, un tādi, kas balstīti uz aizdomām vai spekulācijām.

Stingri jāierobežo mērķis, kādam policijas datus var izmantot. Tas ietekmē policijas datu izpaušanu trešām personām – šādu datu nosūtīšanu vai izpaušanu policijas darbā ir jāregulē atkarībā no tā, vai ir leģitīmas intereses dalīties ar informāciju. Šādu datu nosūtīšana vai izpaušana ārpus policijas darba ir jāatļauj tikai tad, ja ir skaidri noteikti juridiski pienākumi vai atļauja.

Piemērs. Lietā *Karabeyoğlu pret Turciju*[739] prasītāja, kurš bija tiesnesis, telefona līnijas tika uzraudzītas kriminālizmeklēšanas ietvaros, jo viņš tika turēts aizdomās par saistību vai palīdzības un atbalsta sniegšanu nelikumīgai

738 ECT 2016. gada 16. jūnija spriedums lietā *Versini-Campinchi un Crasnianski pret Franciju*, Nr. 49176/11.

739 ECT 2016. gada 7. jūnija spriedums lietā *Karabeyoğlu pret Turciju*, Nr. 30083/10.

organizācijai. Kad tika pieņemts lēmums nesākt kriminālvajāšanu, par krimināLizmeklēšanu atbildīgais prokurors iznīcināja attiecīgos ierakstus. Tomēr kopijas palika pie tiesu izmeklētājiem, kuri pēc tam attiecīgos materiālus izmantoja disciplinārās izmeklēšanas laikā pret prasītāju. ECT uzskatīja, ka attiecīgie tiesību akti bija pārkāpti, jo informācija tika izmantota citiem mērķiem, nevis tiem, kuriem tā tika vākta, un tā nebija iznīcināta likumā noteiktajā termiņā. Iejaukšanās prasītāja tiesībās uz viņa privātās dzīves neaizskaramību nebija saskaņā ar likumu, ciktāl tas attiecās uz disciplinārlietu, kas tika ierosināta pret viņu.

Starptautiska datu nosūtīšana vai izpaušana ir jāattiecina tikai uz ārvalstu policijas iestādēm, un tām būtu jābalstās uz īpašām tiesību normām, iespējams, starptautiskiem nolīgumiem, ja vien tas nav nepieciešams nopietnu un tūlītēju briesmu novēršanai.

Policijas veiktajai datu apstrādei jāpiemēro neatkarīga uzraudzība, lai nodrošinātu atbilstību vietējiem datu aizsardzības likumiem. Datu subjektiem jābūt visām modernizētajā Konvencijā Nr. 108 ietvertajām piekļuves tiesībām. Ja datu subjektu piekļuves tiesības ir ierobežotas saskaņā ar Konvencijas Nr. 108 9. pantu efektīvas policijas izmeklēšanas un kriminālsodu izpildes interesēs, datu subjektam saskaņā ar valsts tiesību aktiem ir jābūt tiesībām vērsties valsts datu aizsardzības uzraudzības iestādē vai citā neatkarīgā iestādē.

8.1.2. Budapeštas konvencija par kibernoziegumiem

Tā kā arvien vairāk tiek izmantotas noziedzīgas darbības un tās ietekmē elektroniskās datu apstrādes sistēmas, šīs problēmas risināšanai ir nepieciešamas jaunas krimināltiesību normas. Tāpēc EP pieņēma starptautisku tiesību instrumentu – Konvenciju par kibernoziegumiem, kas pazīstama arī kā Budapeštas konvencija, kuras mērķis ir risināt ar noziegumiem, kas izdarīti pret elektroniskajiem tīkliem un izmantojot tos, saistītos jautājumus[740]. Šai konvencijai var pievienoties arī valstis, kas nav EP dalībvalstis. Konvencijas līgumslēdzējas puses 2018. gada sākumā bija 14 valstis ārpus EP[741], un vēl septiņas citas valstis, kas nav tās dalībnieces, bija uzaicinātas pievienoties.

740 Eiropas Padomes Ministru komiteja (2001), Konvencija par kibernoziegumiem, *CETS* Nr. 185, Budapešta, 2001. gada 23. novembris, stājās spēkā 2004. gada 1. jūlijā.

741 Amerikas Savienotās Valstis, Austrālija, Čīle, Dominikānas Republika, Izraēla, Japāna, Kanāda, Kolumbija, Maurīcija, Panama, Senegāla, Šrilanka, Tonga un Tunisija. Skatīt Pārskatu par 185. līguma parakstīšanu un ratifikāciju 2017. gada jūlijā.

Konvencija par kibernoziegumiem joprojām ir visietekmīgākais starptautiskais līgums, kas skar likumu pārkāpumus internetā vai citos informācijas tīklos. Tajā ir prasība pusēm atjaunināt un saskaņot savus krimināllikumus pret uzlaušanas un citiem drošības pārkāpumiem, tostarp autortiesību pārkāpumiem, datorizētu krāpšanu, bērnu pornogrāfiju un citām nelikumīgām darbībām kibervidē. Konvencijā paredzētas arī procesuālas pilnvaras attiecībā uz datortīklu meklēšanu un sakaru pārtveršanu kibernoziedzības apkarošanas kontekstā. Visbeidzot, tā dara iespējamu efektīvu starptautisko sadarbību. Konvencijas papildu protokols attiecas uz rasistiska un ksenofobiska rakstura propagandas datortīklos kriminalizēšanu.

Lai arī konvencija nav instruments ar mērķi veicināt datu aizsardzību, tajā noteikts, ka darbības, kas, iespējams, pārkāpj datu subjekta tiesības uz datu aizsardzību, ir krimināli sodāmas. Turklāt tajā tiek prasīts līgumslēdzējām pusēm pieņemt likumdošanas pasākumus, kas valstu iestādēm ļautu pārtvert datu plūsmas un satura datus[742]. Līgumslēdzējām pusēm, īstenojot konvenciju, ir pienākums paredzēt pienācīgu cilvēktiesību un brīvību aizsardzību, tostarp ECTK garantētās tiesības, piemēram, tiesības uz datu aizsardzību[743]. Līgumslēdzējām pusēm nav pienākuma pievienoties arī Konvencijai Nr. 108, lai pievienotos Budapeštas konvencijai par kibernoziegumiem.

8.2. ES tiesību akti par datu aizsardzību policijas un krimināltiesību jautājumos

Svarīgākie aspekti

- ES datu aizsardzība policijas un krimināltiesību jomā ir reglamentēta gan valsts līmeņa, gan pārrobežu apstrādes, ko veic dalībvalstu policijas un krimināltiesību iestādes, kā arī ES dalībnieki, kontekstā.
- Dalībvalstu mērogā valstu tiesību aktos ir jāiekļauj Datu aizsardzības direktīva policijas un krimināltiesību jomā.
- Konkrēti tiesību instrumenti reglamentē datu aizsardzību policijas un tiesībaizsardzības iestāžu pārrobežu sadarbībā, jo īpaši terorisma un pārrobežu noziedzības apkarošanā.

742 Eiropas Padomes Ministru komiteja (2001), Konvencija par kibernoziegumiem, *CETS* Nr. 185, Budapešta, 2001. gada 23. novembris, 20. un 21. pants.

743 Turpat, 15. panta 1. punkts.

- Pastāv īpaši datu aizsardzības noteikumi Eiropas Policijas birojam (Eiropolam), ES Tiesu sadarbības vienībai (*Eurojust*) un jaunizveidotajai Eiropas Prokuratūrai – ES struktūras, kuras palīdz un veicina pārrobežu tiesībaizsardzību.
- Tāpat īpaši datu aizsardzības noteikumi pastāv arī kopīgajām informācijas sistēmām, kuras ir izveidotas ES mērogā pārrobežu informācijas apmaiņai starp kompetentajām policijas un tiesu iestādēm. Svarīgi piemēri ir Šengenas informācijas sistēma II (*SIS II*), Vīzu informācijas sistēma (VIS) un *Eurodac* – centralizēta sistēma, kas satur trešo valstu valstspiederīgo un bezvalstnieku, kuri piesakās uz patvērumu kādā no ES dalībvalstīm, pirkstu nospiedumu datus.
- ES pašlaik atjauno iepriekš izklāstītos datu aizsardzības noteikumus, lai tie atbilstu Datu aizsardzības direktīvai policijas un krimināltiesību jomā.

8.2.1. Datu aizsardzības direktīva policijas un krimināltiesību jomā

Direktīvas (ES) 2016/680 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus, sauktu pie atbildības par tiem vai izpildītu krimināLsodus, un par šādu datu brīvu apriti (Datu aizsardzības direktīva policijas un krimināltiesību jomā)[744] mērķis ir aizsargāt personas datus, kas vākti un apstrādāti krimināltiesību nolūkos, tostarp:

- noziedzīgu nodarījumu novēršanai, izmeklēšanai, atklāšanai un saukšanai pie atbildības par tiem vai krimināLsodu izpildei, tostarp aizsardzībai pret sabiedriskās drošības apdraudējumiem un to novēršanai;
- krimināLsoda izpildei; un
- gadījumos, kad policija vai citas tiesībaizsardzības iestādes rīkojas, lai nodrošinātu likuma ievērošanu un aizsargātu un novērstu draudus sabiedrības drošībai un sabiedrības pamattiesībām, kas varētu būt noziedzīgs nodarījums.

Datu aizsardzības direktīva policijas un krimināltiesību jomā aizsargā dažādu kriminālprocesā iesaistīto personu kategoriju, piemēram, liecinieku, informatoru, cietušo,

744 Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Direktīva (ES) 2016/680 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināLsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI, OV 2016 L 119, 89. lpp. (Datu aizsardzības direktīva policijas un krimināltiesību jomā).

aizdomās turēto un līdzdalībnieku, personas datus. Policijas un krimināltiesību iestādēm ir pienākums ievērot direktīvas noteikumus, katru reizi apstrādājot šādus personas datus tiesībaizsardzības nolūkos, ievērojot gan personisko, gan materiālo direktīvas piemērošanas jomu[745].

Tomēr noteiktos apstākļos ir atļauta arī datu izmantošana citam nolūkam. Datu apstrāde citam tiesībaizsardzības nolūkam, nevis tiem, kuriem tie tika vākti, ir atļauta tikai tad, ja tas ir likumīgi, nepieciešami un samērīgi saskaņā ar valstu vai ES tiesību aktiem[746]. Citiem nolūkiem piemēro Vispārīgās datu aizsardzības regulas noteikumus. Datu koplietošanas reģistrēšana un dokumentēšana ir viens no kompetento iestāžu īpašajiem pienākumiem, palīdzot precizēt no sūdzībām izrietošo atbildību.

Kompetentās iestādes, kas darbojas policijas un krimināltiesību jomā, ir publiskas iestādes vai iestādes, kurām dalībvalsts tiesību aktos uzticēts īstenot publisku varu un publiskas pilnvaras[747], piemēram, privāti pārvaldīti cietumi[748]. Direktīvas piemērojamība attiecas gan uz datu apstrādi valsts teritorijā, gan uz pārrobežu apstrādi starp dalībvalstu policijas un tiesu iestādēm, kā arī uz kompetento iestāžu starptautisku datu nosūtīšanu trešām valstīm un starptautiskām organizācijām[749]. Tā neskar valsts drošību vai personas datu apstrādi, ko veic ES iestādes, struktūras, biroji un aģentūras[750].

Šī direktīva lielā mērā balstīta uz Vispārīgajā datu aizsardzības regulā ietvertajiem principiem un definīcijām, ņemot vērā policijas un krimināltiesību jomu īpašo raksturu. Uzraudzību var veikt tās pašas dalībvalsts iestādes, kas to īsteno arī saskaņā ar Vispārīgo datu aizsardzības regulu. Direktīvā kā jauni pienākumi policijas un krimināltiesību iestādēm ieviesta datu aizsardzības speciālistu iecelšana un datu aizsardzības ietekmes novērtējumu veikšana[751]. Lai arī šos jēdzienus iedvesmojusi

745 Datu aizsardzības direktīva policijas un krimināltiesību jomā, 2. panta 1. punkts.

746 Turpat, 4. panta 2. punkts.

747 Turpat, 3. panta 7. punkts.

748 Eiropas Komisija (2016), Komisijas paziņojums Eiropas Parlamentam, ko izstrādā atbilstoši Līguma par Eiropas Savienības darbību 294. panta 6. punktam, par Padomes nostāju attiecībā uz Eiropas Parlamenta un Padomes direktīvas pieņemšanu par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus, sauktu pie atbildības par tiem vai izpildītu krimināl sodus, un par šādu datu brīvu apriti, un ar ko atceļ Padomes Pamatlēmumu 2008/977/TI, COM(2016) 213 *final*, Brisele, 2016. gada 11. aprīlis.

749 Datu aizsardzības direktīva policijas un krimināltiesību jomā, V nodaļa.

750 Turpat, 2. panta 3. punkts.

751 Turpat, attiecīgi 32. un 27. pants.

Vispārīgā datu aizsardzības regula, direktīva pievēršas policijas un krimināltiesību iestāžu īpašajam raksturam. Salīdzinājumā ar datu apstrādi komerciālos nolūkos, ko reglamentē regula, ar drošību saistītai apstrādei var būt nepieciešama zināma elastība. Piemēram, ja datu subjektiem tiek nodrošināts tāds pats aizsardzības līmenis attiecībā uz tiesībām uz informāciju, piekļuvi viņu personas datiem un datu dzēšanu, kā noteikts Vispārīgajā datu aizsardzības regulā, tas var nozīmēt, ka jebkura novērošanas darbība, kas tiek veikta tiesībaizsardzības nolūkos, tiesībaizsardzības kontekstā kļūs neefektīva. Tādēļ direktīvā nav ietverts pārredzamības princips. Tāpat ar drošību saistītas apstrādes jomā elastīgi jāpiemēro arī datu minimizācijas un nolūka ierobežojuma principi, kas pieprasa ierobežot personas datus tikai līdz tam, kas nepieciešams saistībā ar apstrādes nolūkiem, un veikt apstrādi konkrētiem un skaidriem nolūkiem. Kompetento iestāžu apkopotā un glabātā informācija par konkrēto lietu var izrādīties ārkārtīgi noderīga turpmāko lietu risināšanā.

Ar apstrādi saistītie principi

Datu aizsardzības direktīvā policijas un krimināltiesību jomā noteikti daži galvenie aizsardzības pasākumi attiecībā uz personas datu izmantošanu. Tajā arī izklāstīti šo datu apstrādes principi. Dalībvalstīm jānodrošina, ka personas dati:

- tiek apstrādāti likumīgi un godprātīgi;
- tiek vākti konkrētos, skaidros un leģitīmos nolūkos, un tie netiek apstrādāti ar minētajiem nolūkiem nesaderīgā veidā;
- ir atbilstoši, būtiski un nav pārmērīgi, ņemot vērā nolūkus, kādos tos apstrādā;
- ir precīzi un, ja vajadzīgs, tiek atjaunināti; jāveic visi saprātīgi pasākumi, lai nodrošinātu, ka neprecīzi personas dati, ņemot vērā nolūkus, kādos tie tiek apstrādāti, bez kavēšanās tiktu dzēsti vai laboti;
- tiek glabāti veidā, kas pieļauj datu subjektu identifikāciju, ne ilgāk, kā tas ir nepieciešams tajos nolūkos, kādos tos apstrādā;
- tiek apstrādāti tā, lai tiktu nodrošināta atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu,

iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus[752].

Saskaņā ar šo direktīvu apstrāde ir likumīga tikai tad, ja tā ir nepieciešama attiecīgā uzdevuma izpildei. Turklāt tas ir jādara kompetentai iestādei, lai sasniegtu direktīvā noteiktos mērķus, un apstrādei vajadzētu būt balstītai ES vai valsts tiesību aktos[753]. Datus nedrīkst glabāt ilgāk, nekā tas ir nepieciešams, tie noteiktā termiņā ir jādzēš vai periodiski jāpārskata. Tos drīkst izmantot tikai kompetenta iestāde un nolūkam, kuram dati tika vākti, nosūtīti vai darīti pieejami.

Datu subjekta tiesības

Direktīvā arī izklāstītas datu subjekta tiesības. Tās ietver:

- tiesības saņemt informāciju. Dalībvalstīm ir jānosaka pienākums datu pārzinim darīt pieejamu datu subjektam šādu informāciju: 1) pārziņa identitāte un kontaktinformācija; 2) datu aizsardzības speciālista kontaktinformācija; 3) paredzētās apstrādes nolūki; 4) tiesības iesniegt sūdzību uzraudzības iestādei un tās kontaktinformācija; un 5) tiesības piekļūt personas datiem, tos labot vai dzēst, kā arī ierobežot datu apstrādi[754]. Papildus šīm vispārīgajām informācijas sniegšanas prasībām direktīvā paredzēts, ka īpašos gadījumos un lai ļautu īstenot datu subjektu tiesības, pārziņiem jāsniedz informācija datu subjektiem par apstrādes juridisko pamatu un par to, cik ilgi dati tiks glabāti. Ja personas datus paredzēts nosūtīt citiem saņēmējiem, tostarp trešās valstīs vai starptautiskās organizācijās, datu subjekti jāinformē par šādu saņēmēju kategorijām. Visbeidzot, pārziņiem ir jāsniedz visa papildu informācija, ņemot vērā īpašos apstākļus, kādos dati tiek apstrādāti, piemēram, ja personas dati vākti slēptas novērošanas ietvaros, t. i., bez datu subjekta ziņas. Tādējādi tiek garantēta godprātīga datu subjekta apstrāde[755].

- tiesības piekļūt personas datiem. Dalībvalstīm ir jānodrošina datu subjekta tiesības zināt, vai viņa personas dati tiek apstrādāti. Ja apstrāde tiek veikta, datu subjektam vajadzētu būt piekļuvei noteiktai informācijai, piemēram, apstrādājamo

752 Turpat, 4. panta 1. punkts.

753 Turpat, 8. pants.

754 Turpat, 13. panta 1. punkts.

755 Turpat, 13. panta 2. punkts.

datu kategorijām[756]. Tomēr šīs tiesības var tikt ierobežotas, piemēram, lai novērstu, ka tiek traucēta izmeklēšana vai tiek kaitēts nozieguma kriminālvajāšanai, vai lai aizsargātu sabiedrisko drošību un citu personu tiesības un brīvības[757].

- tiesības labot personas datus. Dalībvalstīm ir pienākums nodrošināt datu subjektam iespēju bez nepamatotas kavēšanās labot nepareizus personas datus. Turklāt datu subjektam ir arī tiesības uz nepilnīgu personas datu papildināšanu[758].

- tiesības dzēst personas datus un ierobežot apstrādi. Noteiktos gadījumos pārzinim ir jādzēš personas dati. Turklāt datu subjekts var panākt savu personas datu dzēšanu, bet tikai tad, ja tie tiek nelikumīgi apstrādāti[759]. Noteiktās situācijās personas datu apstrādi var ierobežot, nevis dzēst datus. Tas var notikt gadījumos, kad 1) tiek apstrīdēta personas datu precizitāte, bet to precizitāti nevar noteikt; vai 2) ja personas dati ir jāsaglabā pierādījumu nolūkā[760].

Ja pārzinis atsakās labot vai dzēst personas datus vai ierobežot datu apstrādi, datu subjekts par to jāinformē rakstiski. Dalībvalstis var ierobežot šīs tiesības uz informāciju, lai cita starpā aizsargātu sabiedrisko drošību vai citu personu tiesības un brīvības tādu pašu iemeslu dēļ, ar ko ierobežo piekļuves tiesības[761].

Datu subjektam parasti ir tiesības uz informāciju par viņa personas datu apstrādi, un viņam ir tiesības piekļūt datiem, labot, dzēst datus vai ierobežot to apstrādi, kuras viņš var īstenot tieši pie pārziņa. Kā atkāpšanās iespēja arī saskaņā ar Datu aizsardzības direktīvu policijas un krimināltiesību jomā var būt datu subjekta tiesību netieša īstenošana, izmantojot datu aizsardzības uzraudzības iestādi, un tā stājas spēkā, ja pārzinis ierobežo datu subjekta tiesības[762]. Direktīvas 17. pantā noteikts, ka dalībvalstīm jāīsteno pasākumi, kas nodrošina, ka datu subjektu tiesības var īstenot arī ar to uzraudzības iestādes starpniecību. Tādēļ datu pārzinim jāinformē datu subjekts par netiešas piekļuves iespējām.

756 Turpat, 14. pants.
757 Turpat, 15. pants.
758 Turpat, 16. panta 1. punkts.
759 Turpat, 16. panta 2. punkts.
760 Turpat, 16. panta 3. punkts.
761 Turpat, 16. panta 4. punkts.
762 Turpat, 17. pants.

Pārziņa un apstrādātāja pienākumi

Datu aizsardzības direktīvas policijas un krimināltiesību jomā kontekstā personas datu pārziņi ir kompetentas publiskas iestādes vai citas struktūras ar attiecīgām publiskām pilnvarām un publisku varu, kas nosaka personas datu apstrādes nolūkus un līdzekļus. Direktīvā ir noteikti vairāki pienākumi datu pārziņiem, lai nodrošinātu augsta līmeņa aizsardzību personas datiem, ko apstrādā tiesībaizsardzības nolūkos.

Kompetentām iestādēm ir jāuztur reģistri par apstrādes darbībām, ko tās veic automatizētās apstrādes sistēmās. Reģistri jāuztur vismaz attiecībā uz personas datu vākšanu, pārveidošanu, piekļuvi, izpaušanu, tostarp nosūtīšanu, kombinēšanu un dzēšanu[763]. Direktīva paredz, ka aplūkošanas un izpaušanas reģistriem jābūt tādiem, lai varētu noteikt operāciju veikšanas datumu un laiku, to pamatojumu un, ciktāl iespējams, veikt personas, kura ir izmantojusi sistēmu vai izpaudusi personas datus, identifikāciju, kā arī noteikt attiecīgo personas datu saņēmējus. Reģistrus izmanto tikai nolūkā pārbaudīt apstrādes likumību, veikt pašuzraudzību, nodrošināt personas datu integritāti un drošību, kā arī kriminālprocesa nolūkā[764]. Pēc uzraudzības iestādes pieprasījuma pārzinim un apstrādātājam jādara pieejami šie ieraksti.

Konkrēti, pārziņiem ir vispārējs pienākums ieviest atbilstošus tehniskos un organizatoriskos pasākumus, lai nodrošinātu, ka apstrāde tiek veikta saskaņā ar direktīvu, un lai varētu pierādīt šādas apstrādes likumību[765]. Izstrādājot šos pasākumus, jāņem vērā apstrādes raksturs, tvērums, konteksts un, kas ir svarīgi, jebkādi iespējamie riski personu tiesībām un brīvībām. Pārziņiem ir jāpieņem iekšējā politika un jāīsteno pasākumi, kas veicina datu aizsardzības principu ievērošanu, jo īpaši integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma principu[766]. Ja pastāv iespēja, ka apstrāde rada lielu risku personu tiesībām, piemēram, jaunu tehnoloģiju izmantošanas dēļ, pārziņiem pirms apstrādes uzsākšanas jāveic datu aizsardzības ietekmes novērtējums[767]. Direktīvā uzskaitīti arī pasākumi, kas pārzinim jāievieš, lai nodrošinātu apstrādes drošību. Tie ietver pasākumus nolūkā novērst neatļautu piekļuvi apstrādātajiem personas datiem, nodrošināt, ka pilnvarotajām personām ir piekļuve tikai tiem personas datiem, kādiem viņiem ir piekļuves atļauja, nodrošināt apstrādes sistēmas funkcijas pareizu darbību un ka saglabātos personas datus nevar sabojāt sistēmas nepareizas darbības rezultātā[768]. Ja noticis personas datu aizsardzības

763 Turpat, 25. panta 1. punkts.

764 Turpat, 25. panta 2. punkts.

765 Turpat, 19. pants.

766 Turpat, 20. pants.

767 Turpat, 27. pants.

768 Turpat, 29. pants.

pārkāpums, pārziņiem trīs dienu laikā jāinformē uzraudzības iestāde, aprakstot pārkāpuma veidu, tā iespējamās sekas, skarto personas datu kategorijas un attiecīgo skarto datu subjektu aptuveno skaitu. Par personas datu aizsardzības pārkāpumu "bez nepamatotas kavēšanās" jāinformē arī datu subjekts, ja pārkāpums, iespējams, rada lielu risku viņa tiesībām un brīvībām[769].

Direktīvā ietverts pārskatatbildības princips, uzliekot pārzinim pienākumu īstenot pasākumus, lai nodrošinātu šā principa ievērošanu. Pārziņiem jāveic visu to apstrādes darbību kategoriju uzskaite, par kurām viņi ir atbildīgi. Detalizēts šādu ierakstu saturs ir noteikts direktīvas 24. pantā. Ierakstiem pēc pieprasījuma jābūt pieejamiem uzraudzības iestādei, lai tā varētu uzraudzīt pārziņa apstrādes darbības. Vēl viens svarīgs pasākums pārskatatbildības uzlabošanai ir datu aizsardzības speciālista (DAS) iecelšana. Pārziņiem ir pienākums iecelt DAS, lai gan direktīva ļauj dalībvalstīm no šā pienākuma atbrīvot tiesas un citas neatkarīgas tiesu iestādes[770]. DAS pienākumi ir līdzīgi Vispārīgajā datu aizsardzības regulā noteiktajiem. Viņš vai viņa uzrauga atbilstību direktīvai, sniedz informāciju un konsultē darbiniekus, kuri veic datu apstrādi, par viņu pienākumiem saskaņā ar datu aizsardzības tiesību aktiem. DAS arī sniedz ieteikumus par nepieciešamību veikt datu aizsardzības ietekmes novērtējumu un darbojas kā uzraudzības iestādes kontaktpersona.

Datu nosūtīšana trešām valstīm vai starptautiskām organizācijām

Līdzīgi kā Vispārīgajā datu aizsardzības regulā, direktīvā paredzēti nosacījumi personas datu nosūtīšanai trešām valstīm vai starptautiskām organizācijām. Ja personas dati tiktu brīvi nosūtīti ārpus ES jurisdikcijas, ES tiesību aktos paredzētie aizsardzības pasākumi un stingrā aizsardzība varētu tikt apdraudēti. Tomēr paši nosacījumi izteikti atšķiras no Vispārīgajā datu aizsardzības regulā paredzētajiem. Personas datu nosūtīšana trešām valstīm vai starptautiskām organizācijām ir atļauta šādos gadījumos[771]:

- Nosūtīšana ir nepieciešama direktīvas mērķiem.

- Personas dati tiek nosūtīti trešās valsts vai starptautiskas organizācijas iestādei, kas ir kompetenta šīs direktīvas izpratnē, lai arī atsevišķos un īpašos gadījumos no šā noteikuma ir iespējama atkāpe[772].

769 Turpat, 30. un 31. pants.

770 Turpat, 32. pants.

771 Turpat, 35. pants.

772 Turpat, 39. pants.

- Personas datu, kas saņemti pārrobežu sadarbības gaitā, nosūtīšanai trešām valstīm vai starptautiskām organizācijām ir nepieciešama datu izcelsmes dalībvalsts atļauja, lai gan steidzamos gadījumos piemērojami atbrīvojumi.

- Eiropas Komisija ir pieņēmusi lēmumu par aizsardzības līmeņa pietiekamību, ir ieviesti attiecīgi aizsardzības pasākumi vai ir piemērojama atkāpe datu nosūtīšanai īpašās situācijās.

- Personas datu tālākai nosūtīšanai uz citu trešo valsti vai starptautisku organizāciju ir nepieciešama iepriekšēja kompetentās iestādes atļauja, kura cita starpā ņems vērā pārkāpuma smagumu un datu aizsardzības līmeni otrās starptautiskās datu nosūtīšanas galamērķa valstī[773].

Saskaņā ar direktīvu personas datu nosūtīšana var notikt, ja ir izpildīts viens no trim nosacījumiem. Pirmkārt, ja Eiropas Komisija saskaņā ar direktīvu ir pieņēmusi lēmumu par aizsardzības līmeņa pietiekamību. Lēmumu var attiecināt uz visu trešās valsts teritoriju, uz konkrētām trešās valsts nozarēm vai uz starptautisku organizāciju. Tomēr to var izdarīt tikai tad, ja ir nodrošināts atbilstošs aizsardzības līmenis un izpildīti direktīvā noteiktie nosacījumi[774]. Šādos gadījumos personas datu nosūtīšanai nav nepieciešama dalībvalsts atļauja[775]. Eiropas Komisijai jāuzrauga tendences, kas varētu ietekmēt lēmumu par aizsardzības līmeņa pietiekamību. Turklāt lēmumā jābūt iekļautam periodiskas pārskatīšanas mehānismam. Komisija var arī atcelt, grozīt vai apturēt lēmumu, ja pieejamā informācija norāda, ka apstākļi trešā valstī vai starptautiskā organizācijā vairs nenodrošina pienācīgu aizsardzības līmeni. Tādā gadījumā Komisijai jāuzsāk apspriešanās ar trešo valsti vai starptautisko organizāciju nolūkā labot situāciju.

Ja nav lēmuma par aizsardzības līmeņa pietiekamību, datu nosūtīšanu var pamatot ar attiecīgiem aizsardzības pasākumiem. Tos var noteikt juridiski saistošā dokumentā, vai arī pārzinis var veikt apstākļu, kas saistīti ar personas datu nosūtīšanu, pašnovērtējumu un konstatēt, ka pastāv attiecīgi aizsardzības pasākumi. Pašnovērtējumā ir jāņem vērā iespējamie sadarbības nolīgumi, kas noslēgti starp Eiropolu vai *Eurojust* un trešo valsti vai starptautisko organizāciju, konfidencialitātes pienākuma esamība un nolūka ierobežojums, kā arī garantijas, ņemot vērā, ka dati netiks

773 Turpat, 35. panta 1. punkts.

774 Turpat, 36. pants.

775 Turpat, 36. panta 1. punkts.

izmantoti, lai īstenotu cietsirdīgu un necilvēcīgu soda veidu, tostarp nāvessodu[776]. Pēdējā gadījumā pārzinim jāinformē kompetentā uzraudzības iestāde par šīs kategorijas ietvaros veiktās nosūtīšanas kategorijām[777].

Ja nav pieņemts lēmums par aizsardzības līmeņa pietiekamību vai nav ieviesti attiecīgi aizsardzības pasākumi, īpašās direktīvā aprakstītās situācijās nosūtīšanu joprojām var atļaut. Tās cita starpā ietver datu subjekta vai citas personas būtisko interešu aizsardzību un tūlītēju un nopietnu draudu novēršanu attiecībā uz dalībvalsts vai trešās valsts sabiedrisko drošību[778].

Atsevišķos un īpašos gadījumos kompetento iestāžu veikta nosūtīšana saņēmējiem, kas reģistrēti trešās valstīs un kas nav kompetentās iestādes, var tikt īstenota, ja papildus vienam no trim iepriekš aprakstītajiem nosacījumiem ir izpildīti papildu nosacījumi, kuri noteikti direktīvas 39. pantā. Konkrēti: nosūtīšanai ir jābūt absolūti nepieciešamai, lai izpildītu tās nosūtošās kompetentās iestādes uzdevumus, kuras atbildība ir arī noteikt, vai personu pamattiesības vai brīvības nav svarīgākas par sabiedrības interesēm, kas ir nosūtīšanas pamatā. Šāda nosūtīšana ir jādokumentē, un kompetentajai nosūtošajai iestādei ir jāinformē kompetentā uzraudzības iestāde[779].

Visbeidzot, attiecībā uz trešām valstīm un starptautiskām organizācijām direktīva pieprasa arī izstrādāt starptautiskas sadarbības mehānismu, lai atvieglotu tiesību aktu efektīvu izpildi un tādējādi datu aizsardzības uzraudzības iestādēm palīdzētu sadarboties ar ārvalstu kolēģiem[780].

Neatkarīga uzraudzība un datu subjekta tiesiskās aizsardzības līdzekļi

Katrai dalībvalstij ir jānodrošina, ka viena vai vairākas neatkarīgas valsts uzraudzības iestādes atbild par konsultācijām un saskaņā ar šo direktīvu pieņemto noteikumu piemērošanas uzraudzību[781]. Uzraudzības iestāde, kas izveidota šīs direktīvas nolūkiem, var būt tā pati, kas izveidota saskaņā ar Vispārīgo datu aizsardzības regulu, bet dalībvalstis var brīvi izraudzīties citu iestādi ar nosacījumu, ka tā atbilst neatkarības

776 Turpat, 71. apsvērums
777 Turpat, 37. panta 1. punkts.
778 Turpat, 38. panta 1. punkts.
779 Turpat, 37. panta 3. punkts.
780 Turpat, 40. pants.
781 Turpat, 41. pants.

kritērijiem. Uzraudzības iestādes izskata arī jebkuras personas iesniegtās sūdzības par viņu tiesību un brīvību aizsardzību attiecībā uz kompetento iestāžu veiktu personas datu apstrādi.

Ja datu subjekta tiesību īstenošana ir atteikta pārliecinošu iemeslu dēļ, datu subjektam jābūt tiesībām to pārsūdzēt kompetentajā valsts uzraudzības iestādē un/vai tiesā. Ja personai ir nodarīts kaitējums valsts tiesību aktu, ar kuriem īsteno šo direktīvu, pārkāpuma rezultātā, tai ir tiesības uz kompensāciju no pārziņa vai jebkuras citas iestādes, kas ir kompetenta saskaņā ar dalībvalsts tiesību aktiem[782]. Parasti datu subjektiem jābūt piekļuvei tiesiskās aizsardzības līdzekļiem attiecībā uz valsts tiesību aktos, ar kuriem īsteno šo direktīvu, noteikto viņu tiesību pārkāpumiem[783].

8.3. Citi īpaši tiesību instrumenti datu aizsardzībai tiesībaizsardzības jautājumos

Papildus Datu aizsardzības direktīvai policijas un krimināltiesību jomā dalībvalstu rīcībā esošās informācijas apmaiņu īpašās jomās regulē vairāki tiesību instrumenti, piemēram, Padomes Pamatlēmums 2009/315/TI par organizatoriskiem pasākumiem un saturu no sodāmības reģistra iegūtas informācijas apmaiņai starp dalībvalstīm, Padomes Lēmums 2000/642/TI par sadarbības pasākumiem starp dalībvalstu finanšu ziņu vākšanas vienībām attiecībā uz informācijas apmaiņu un Padomes 2006. gada 18. decembra Pamatlēmums 2006/960/TI par Eiropas Savienības dalībvalstu tiesībaizsardzības iestāžu informācijas un izlūkdatu apmaiņas vienkāršošanu[784].

Svarīgi ir tas, ka kompetento iestāžu savstarpējā pārrobežu sadarbība[785] aizvien vairāk ietver imigrācijas datu apmaiņu. Neuzskata, ka šī tiesību joma ietilpst policijas un krimināltiesību jautājumos, taču daudzējādā ziņā ir būtiska policijas un tiesu iestāžu

782 Turpat, 56. pants.

783 Turpat, 54. pants.

784 Eiropas Savienības Padome (2009), Padomes 2009. gada 26. februāra Pamatlēmums 2009/315/TI par organizatoriskiem pasākumiem un saturu no sodāmības reģistra iegūtas informācijas apmaiņai starp dalībvalstīm, OV 2009 L 93; Eiropas Savienības Padome (2000), Padomes 2000. gada 17. oktobra Lēmums 2000/642/TI par sadarbības pasākumiem starp dalībvalstu finanšu ziņu vākšanas vienībām attiecībā uz informācijas apmaiņu, OV 2000 L 271; Padomes 2006. gada 18. decembra Pamatlēmums 2006/960/TI par Eiropas Savienības dalībvalstu tiesībaizsardzības iestāžu informācijas un izlūkdatu apmaiņas vienkāršošanu, OV L 386.

785 Eiropas Komisija (2012), *Komisijas paziņojums Eiropas Parlamentam un Padomei: Tiesībaizsardzības iestāžu sadarbības stiprināšana ES: Eiropas Informācijas apmaiņas modelis (EIXM)*, COM(2012) 735 *final*, Brisele, 2012. gada 7. decembris.

darbam. Tas pats attiecas uz datiem par precēm, ko importē ES vai eksportē no ES. Iekšējo robežu kontroles atcelšana Šengenas zonā ir palielinājusi krāpšanas risku, liekot dalībvalstīm pastiprināt sadarbību, jo īpaši uzlabojot pārrobežu informācijas apmaiņu, lai efektīvāk atklātu valsts un ES muitas likumu pārkāpumus un sauktu pie atbildības par tiem. Turklāt pēdējos gados pasaulē ir novērojams smagas un organizētas noziedzības un terorisma pieaugums, kas var būt saistīts ar starptautiskiem ceļojumiem, un daudzos gadījumos ir radusies nepieciešamība pēc pastiprinātas policijas un tiesībaizsardzības iestāžu pārrobežu sadarbības[786].

Prīmes lēmums

Svarīgs institucionalizētas pārrobežu sadarbības piemērs valstī glabātu datu apmaiņai ir Padomes Lēmums 2008/615/TI kopā ar tā īstenošanas noteikumiem Lēmumā 2008/615/TI par pārrobežu sadarbības pastiprināšanu, jo īpaši apkarojot terorismu un pārrobežu noziedzību (Prīmes lēmums), ar kuru Prīmes līgumu 2008. gadā iekļāva ES tiesību aktos[787]. Prīmes līgums bija starptautisks policijas sadarbības nolīgums, kuru 2005. gadā parakstīja Austrija, Beļģija, Francija, Vācija, Luksemburga, Nīderlande un Spānija[788].

Prīmes lēmuma mērķis ir palīdzēt parakstītājām dalībvalstīm uzlabot informācijas apmaiņu, lai novērstu un apkarotu noziedzību trīs jomās, kas ir terorisms, pārrobežu noziedzība un nelegālā migrācija. Tādēļ lēmumā ir izklāstīti nosacījumi attiecībā uz:

- automatizētu piekļuvi DNS profiliem, pirkstu nospiedumu datiem un noteiktiem valsts transportlīdzekļu reģistrācijas datiem;
- datu piegādi saistībā ar nozīmīgiem pārrobežu notikumiem;
- informācijas sniegšanu teroristu nodarījumu novēršanai;
- citiem pasākumiem pārrobežu policijas sadarbības pastiprināšanai.

786 Skatīt Eiropas Komisija (2011), Priekšlikums Eiropas Parlamenta un Padomes direktīvai par pasažieru datu reģistra datu izmantošanu teroristu nodarījumu un smagu noziegumu novēršanai, atklāšanai, izmeklēšanai un saukšanai pie atbildības par tiem, COM(2011) 32 *final*, Brisele, 2011. gada 2. februāris, 1. lpp.

787 Eiropas Savienības Padome (2008), Padomes 2008. gada 23. jūnija Lēmums 2008/615/TI par pārrobežu sadarbības pastiprināšanu, jo īpaši apkarojot terorismu un pārrobežu noziedzību, OV 2008 L 210.

788 Konvencija, ko noslēgusi Beļģijas Karaliste, Vācijas Federatīvā Republika, Spānijas Karaliste, Francijas Republika, Luksemburgas Lielhercogiste, Nīderlandes Karaliste un Austrijas Republika, kurā ir paredzēts pastiprināti izvērst pārrobežu sadarbību, jo īpaši tādu sadarbību, kas saistīta ar terorisma, pārrobežu noziedzības un nelegālas migrācijas apkarošanu.

Datubāzes, kas ir pieejamas saskaņā ar Prīmes lēmumu, pilnībā reglamentē valstu tiesību akti, bet datu apmaiņu papildus regulē arī lēmums, kura atbilstība Datu aizsardzības direktīvai policijas un krimināltiesību jomā būs jānovērtē. Šādu datu plūsmu uzraudzības kompetentās iestādes ir valstu datu aizsardzības uzraudzības iestādes.

Pamatlēmums 2006/960/TI – Zviedrijas iniciatīva

Pamatlēmums 2006/960/TI (Zviedrijas iniciatīva)[789] ir vēl viens pārrobežu sadarbības piemērs attiecībā uz tādu datu apmaiņu, ko valsts mērogā glabā tiesībaizsardzības iestādes. Zviedrijas iniciatīva ir īpaši vērsta uz izlūkdatu un informācijas apmaiņu, un tās 8. pantā paredzēti īpaši datu aizsardzības noteikumi.

Saskaņā ar šo instrumentu uz apmainītās informācijas un izlūkdatu izmantošanu jāattiecina tās dalībvalsts datu aizsardzības noteikumi, kura saņem informāciju, saskaņā ar tiem pašiem noteikumiem, it kā tie būtu vākti šajā dalībvalstī. Papildus 8. pantā tiek noteikts, ka, sniedzot informāciju un izlūkdatus, kompetentā tiesībaizsardzības iestāde var noteikt nosacījumus, kas atbilst tās valsts tiesību aktiem, kā kompetentā tiesībaizsardzības iestāde var tos izmantot. Šie nosacījumi var attiekties arī uz ziņošanu par krimināllizmeklēšanas rezultātiem vai krimināllizlūkošanas operācijām, saistībā ar kurām bijusi nepieciešama informācijas un izlūkdatu apmaiņa. Tomēr, ja valstu tiesību aktos paredzēti izņēmumi izmantošanas ierobežojumiem (piemēram, tiesu iestādēm, likumdošanas struktūrām u. tml.), informāciju un izlūkdatus var izmantot tikai pēc iepriekšējas apspriešanās ar datu devēju dalībvalsti.

Sniegto informāciju un izlūkdatus var izmantot:

- nolūkos, kādos tie sniegti; vai
- lai novērstu tūlītējus un nopietnus draudus sabiedrības drošībai.

Apstrādi citos nolūkos var atļaut, bet tikai ar iepriekšēju datu devējas dalībvalsts atļauju.

Zviedrijas iniciatīvā arī noteikts, ka apstrādātie personas dati ir jāaizsargā saskaņā ar starptautiskiem instrumentiem, piemēram:

789 Eiropas Savienības Padome (2006), Padomes 2006. gada 18. decembra Pamatlēmums 2006/960/TI par Eiropas Savienības dalībvalstu tiesībaizsardzības iestāžu informācijas un izlūkdatu apmaiņas vienkāršošanu, OV L 386/89, 2006. gada 29. decembris.

- Eiropas Padomes Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi[790];

- Šīs Konvencijas 2001. gada 8. novembra papildprotokols par uzraudzības institūcijām un pārrobežu datu plūsmām[791];

- Eiropas Padomes Ieteikums Nr. R(87)15 dalībvalstīm, kas regulē personas datu izmantošanu policijas darbā[792].

ES PDR direktīva

Pasažieru datu reģistra (PDR) dati attiecas uz informāciju par aviopasažieriem, ko vāc un glabā pārvadātāju rezervācijas un izlidošanas kontroles sistēmās pašu komerciāliem nolūkiem. Šie dati satur dažādu vairāku veidu informāciju, piemēram, ceļojuma datumus, ceļojuma maršrutu, biļešu informāciju, kontaktinformāciju, ceļojumu aģentu, ar kura starpniecību lidojums tika rezervēts, izmantotos maksāšanas līdzekļus, sēdvietas numuru un informāciju par bagāžu[793]. PDR datu apstrāde var palīdzēt tiesībaizsardzības iestādēm identificēt zināmos vai potenciālos aizdomās turamos un veikt novērtējumus, pamatojoties uz ceļošanas paradumiem un citiem rādītājiem, ko parasti saista ar noziedzīgām darbībām. PDR datu analīze ļauj retrospektīvi izsekot arī to personu ceļojuma maršrutus un kontaktus, par kurām ir aizdomas, ka tās ir iesaistītas noziedzīgās darbībās, tādējādi dodot iespēju tiesībaizsardzības iestādēm identificēt noziedzīgus tīklus[794]. ES ir noslēgusi dažus nolīgumus ar trešām valstīm par PDR datu apmaiņu, kā paskaidrots 7. iedaļā. Turklāt tā ir ieviesusi PDR datu apstrādi ES ar Direktīvu (ES) 2016/681 par pasažieru datu reģistra (PDR) datu izmantošanu teroristu nodarījumu un smagu noziegumu novēršanai, atklāšanai,

790 Eiropas Padome (1981), Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi, *CETS* Nr. 108.

791 Eiropas Padome (2001), Konvencijas par personu aizsardzību attiecībā uz personu datu automātisko apstrādi Papildu protokols par uzraudzības institūcijām un pārrobežu datu plūsmām, *CETS* Nr. 108.

792 Eiropas Padome (1987), Ministru komitejas Ieteikums Nr. R(87)15 dalībvalstīm, kas regulē personas datu izmantošanu policijas darbā (pieņēma Ministru komiteja 1987. gada 17. septembrī ministru vietnieku 410. sanāksmē).

793 Eiropas Komisija (2011), Priekšlikums Eiropas Parlamenta un Padomes direktīvai par pasažieru datu reģistra datu izmantošanu teroristu nodarījumu un smagu noziegumu novēršanai, atklāšanai, izmeklēšanai un saukšanai pie atbildības par tiem, COM(2011) 32 *final*, Brisele, 2011. gada 2. februāris, 1. lpp.

794 Eiropas Komisija (2015), Faktu lapa "Cīņa ar terorismu ES līmenī: pārskats par Komisijas darbībām, pasākumiem un iniciatīvām", Brisele, 2015. gada 11. janvāris.

izmeklēšanai un saukšanai pie atbildības par tiem (ES PDR direktīva)[795]. Šajā direktīvā ir paredzēts pienākums gaisa pārvadātājiem pārsūtīt PDR datus kompetentajām iestādēm un noteikti stingri datu aizsardzības pasākumi šādu datu apstrādei un vākšanai. ES PDR direktīva attiecas uz starptautiskiem lidojumiem uz un no ES, kā arī uz lidojumiem ES iekšienē, ja kāda dalībvalsts attiecīgi nolemj[796].

Vāktie PDR dati drīkst saturēt tikai ES PDR direktīvā atļauto informāciju. Tie ir jāsaglabā vienā informācijas vienībā, drošā vietā katrā dalībvalstī. PDR dati jāanonimizē sešus mēnešus pēc to nosūtīšanas no gaisa pārvadātāja un jāglabā ne ilgāk kā piecus gadus[797]. PDR datu apmaiņa notiek starp dalībvalstīm, starp dalībvalstīm un Eiropolu, un ar trešām valstīm, bet tikai atsevišķos gadījumos.

PDR datu pārsūtīšanai un apstrādei, kā arī datu subjektu aizsargātajām tiesībām jāatbilst Datu aizsardzības direktīvai policijas un krimināltiesību jomā un jānodrošina augsts privātuma un personas datu aizsardzības līmenis, kā to pieprasa Harta, modernizētā Konvencija Nr. 108 un ECTK.

Neatkarīgās valsts uzraudzības iestādes, kas ir kompetentas saskaņā ar Datu aizsardzības direktīvu policijas un krimināltiesību jomā, atbild arī par konsultāciju sniegšanu un to noteikumu piemērošanas uzraudzību, kurus dalībvalstis pieņēmušas saskaņā ar ES PDR direktīvu.

Telekomunikāciju datu saglabāšana

Datu saglabāšanas direktīva[798], kas 2014. gada 8. aprīlī ar spriedumu lietā *Digital Rights Ireland* tika pasludināta par spēkā neesošu, uzlika sakaru pakalpojumu sniedzējiem pienākumu vismaz sešus, bet ne ilgāk kā 24 mēnešus glabāt pieejamus metadatus konkrētam nolūkam – smagu noziegumu apkarošanai neatkarīgi no tā, vai pakalpojumu sniedzējam šie dati joprojām bija nepieciešami norēķiniem vai pakalpojuma tehniskai nodrošināšanai.

795 Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Direktīva (ES) 2016/681 par pasažieru datu reģistra (PDR) datu izmantošanu teroristu nodarījumu un smagu noziegumu novēršanai, atklāšanai, izmeklēšanai un saukšanai pie atbildības par tiem, OV 2016 L 119, 132. lpp.

796 PDR direktīva, L 119, 132. lpp., 1. panta 1. punkts un 2. panta 1. punkts.

797 Turpat, 12. panta 1. un 2. punkts.

798 Eiropas Parlamenta un Padomes 2006. gada 15. marta Direktīva 2006/24/EK par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK, OV 2006 L 105.

Telekomunikāciju datu saglabāšana nepārprotami ir iejaukšanās tiesībās uz datu aizsardzību[799]. Šīs iejaukšanās pamatotība tikusi apstrīdēta vairākos ES dalībvalstu tiesu procesos[800].

Piemērs. Lietās *Digital Rights Ireland* un *Kärntner Landesregierung un citi*[801] *Digital Rights* grupa un *Seitlinger* kungs cēla prasību attiecīgi Īrijas Augstajā tiesā un Austrijas Konstitucionālajā tiesā, apstrīdot to valsts pasākumu likumību, kas ļauj saglabāt elektronisko telekomunikāciju datus. *Digital Rights* lūdza Īrijas tiesu atzīt par spēkā neesošu Direktīvu 2006/24/EK un valsts krimināltiesību daļu, kas attiecas uz teroristu nodarījumiem. Tāpat *Seitlinger* kungs un vairāk nekā 11 000 citu prasītāju apstrīdēja un lūdza anulēt normu Austrijas tiesību aktā par telekomunikācijām, ar kuru tika transponēta Direktīva 2006/24/EK.

Izskatot šos lūgumus sniegt prejudiciālu nolēmumu, EST pasludināja Datu saglabāšanas direktīvu par spēkā neesošu. Saskaņā ar EST viedokli dati, ko drīkstēja saglabāt saskaņā ar direktīvu, sniedza precīzu informāciju par personām, skatot tos kopumā. Turklāt EST pārbaudīja, cik nopietni ir iejaukšanās pamattiesībās uz privātās dzīves neaizskaramību un personas datu aizsardzību. Tiesa secināja, ka saglabāšana atbilst sabiedrības interešu mērķim, proti, cīņai pret smagu noziegumu un tādējādi arī sabiedriskajai drošībai. Tomēr EST konstatēja, ka ES likumdevējs, pieņemot direktīvu, ir pārkāpis proporcionalitātes principu. Lai arī direktīva var būt piemērota prasītā mērķa sasniegšanai, "direktīvas plašā un īpaši nopietnā iejaukšanās pamattiesībās uz privātuma un personas datu aizsardzību ir nepietiekami reglamentēta, lai nodrošinātu, ka šī iejaukšanās patiešām būtu ierobežota ar absolūti nepieciešamo".

Ja nav īpašu tiesību aktu par datu saglabāšanu, tā ir atļauta kā preventīvs pasākums, kā izņēmums telekomunikāciju datu konfidencialitātes pienākumam saskaņā ar

799 EDAU (2011), *2011. gada 31. maija atzinums par Komisijas izvērtējuma ziņojumu Padomei un Eiropas Parlamentam par Datu saglabāšanas direktīvu (Direktīva 2006/24/EK)*, 2011. gada 31. maijs.

800 Vācija, Federālā konstitucionālā tiesa (*Bundesverfassungsgericht*), 1 BvR 256/08, 2010. gada 2. marts; Rumānija, Federālā konstitucionālā tiesa (*Curtea Constituțională a României*), Nr. 1258, 2009. gada 8. oktobris; Čehijas Republika, Konstitucionālā tiesa (Ústavní soud České republiky), 94/2011 Coll., 2011. gada 22. marts.

801 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C-293/12 un C-594/12 *Digital Rights Ireland Ltd pret Minister for Communications, Marine un Natural Resources un citiem* un *Kärntner Landesregierung un citiem* [GC], 65. punkts.

Direktīvu 2002/58/EK (Direktīva par privāto dzīvi un elektronisko komunikāciju)[802], bet to var darīt tikai smagu noziegumu apkarošanas nolūkā. Šāda saglabāšana jāierobežo līdz absolūti nepieciešamajam attiecībā uz saglabāto datu kategorijām, skartajiem komunikācijas līdzekļiem, skartajām personām un izvēlēto saglabāšanas ilgumu. Valstu iestādēm var būt piekļuve saglabātajiem datiem, piemērojot stingrus nosacījumus, tostarp iepriekšēju neatkarīgas iestādes veiktu pārskatu. Dati ir jāsaglabā ES teritorijā.

Piemērs. Pēc sprieduma lietā *Digital Rights Ireland* un *Kärntner Landesregierung un citi*[803] EST tika ierosinātas vēl divas lietas par Zviedrijā un Apvienotajā Karalistē piemēroto vispārīgo pienākumu elektronisko komunikāciju pakalpojumu sniedzējiem saglabāt telekomunikāciju datus, kā prasīts par spēkā neesošu atzītajā Datu saglabāšanas direktīvā. Apvienotajās lietās *Tele2 Sverige* un *Home Department pret Tom Watson un citiem*[804] EST lēma, ka valsts tiesību akti, kas paredz vispārēju un nekritisku datu saglabāšanu, nepieprasot nekādu saistību starp saglabājamajiem datiem un draudiem sabiedriskajai drošībai, kā arī neprecizējot nevienu nosacījumu, piemēram, saglabāšanas periods, ģeogrāfiskā zona, personu grupa, kas varētu būt iesaistīta smagā noziegumā, pārsniedz absolūti nepieciešamā robežas, un to nevar uzskatīt par pamatotu demokrātiskā sabiedrībā, kā to prasa Direktīva 2002/58/EK, lasot ES Pamattiesību hartas kontekstā.

Perspektīva

Eiropas Komisija 2017. gada janvārī publicēja priekšlikumu regulai par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko komunikāciju nozarē, ar ko paredzēts atcelt un aizstāt Direktīvu 2002/58/EK[805]. Priekšlikumā nav iekļautas

802 Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (Direktīva par privāto dzīvi un elektronisko komunikāciju), OV 2002 L 201.

803 EST 2014. gada 8. aprīļa spriedums apvienotajās lietās C-293/12 un C-594/12 *Digital Rights Ireland Ltd pret Minister for Communications, Marine and Natural Resources un citiem* un Kärntner Landesregierung un citiem [GC].

804 EST 2016. gada 21. decembra spriedums apvienotajās lietās C-203/15 un C-698/15 *Tele2 Sverige AB pret Post-och telestyrelsen* un *Secretary of State for the Home Department pret Tom Watson un citiem* [GC].

805 Eiropas Komisija (2017), Priekšlikums Eiropas Parlamenta un Padomes regulai par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko komunikāciju nozarē un ar ko atceļ Direktīvu 2002/58/EK (Regula par privāto dzīvi un elektronisko komunikāciju), COM(2017) 10 *final*, Brisele, 2017. gada 10. janvāris.

īpašas normas par datu saglabāšanu. Tomēr tajā paredzēts, ka dalībvalstis var ierobežot noteiktus tiesību aktos paredzētos pienākumus un tiesības, ja šāds ierobežojums ir nepieciešams un samērīgs pasākums, lai aizsargātu noteiktas sabiedrības intereses, tostarp valsts drošību, aizsardzību, sabiedrisko drošību un noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu, saukšanu pie atbildības par tiem vai kriminālsodu izpildi[806]. Tāpēc dalībvalstis varētu glabāt vai izveidot valsts datu saglabāšanas sistēmas, kurās paredz mērķtiecīgus saglabāšanas pasākumus, ciktāl šādas sistēmas atbilst Savienības tiesību aktiem, ņemot vērā EST judikatūru par E-privātuma direktīvas interpretāciju un ES Pamattiesību hartu[807]. Rokasgrāmatas izstrādes laikā joprojām norisinājās diskusijas par regulas pieņemšanu.

ES un ASV "jumta" nolīgums par to personas datu aizsardzību, ar kuriem apmainās tiesībaizsardzības nolūkos

ES un ASV jumta nolīgums par personas datu apstrādi noziedzīgu nodarījumu novēršanai, izmeklēšanai, atklāšanai un saukšanai pie atbildības par tiem ar ASV stājās spēkā 2017. gada 1. februārī[808]. ES un ASV jumta nolīguma mērķis ir nodrošināt augsta līmeņa datu aizsardzību ES pilsoņiem, vienlaikus uzlabojot ES un ASV tiesībaizsardzības iestāžu sadarbību. Tas papildina spēkā esošos ES un ASV un dalībvalstu un ASV nolīgumus starp tiesībaizsardzības iestādēm, turklāt palīdzot ieviest skaidrus un saskaņotus datu aizsardzības noteikumus turpmākiem nolīgumiem šajā jomā. Šajā sakarībā nolīguma mērķis ir izveidot ilgtermiņa tiesisko regulējumu, lai atvieglotu informācijas apmaiņu.

Nolīgums pats par sevi nenodrošina piemērotu juridisko pamatu personas datu apmaiņai, bet tā vietā piedāvā atbilstošas datu aizsardzības garantijas skartajām personām. Tas aptver visu personas datu apstrādi, kas nepieciešama noziedzīgu nodarījumu, tostarp terorisma, novēršanai, izmeklēšanai, atklāšanai un saukšanai pie atbildības par tiem[809].

806 Turpat, 26. apsvērums.

807 Skatīt Priekšlikuma regulai par privāto dzīvi un elektronisko komunikāciju paskaidrojuma rakstu (COM(2017) 10 *final*, 1.3. punkts.

808 Skatīt ES Padome (2016), *"Uzlabotas ES pilsoņu datu aizsardzības tiesības sadarbībā tiesībaizsardzības jomā: ES un ASV paraksta jumta nolīgumu"*, preses relīze 305/16, 2016. gada 2. jūnijs.

809 Nolīgums starp Amerikas Savienotajām Valstīm un Eiropas Savienību par personas datu aizsardzību saistībā ar noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu un saukšanu pie atbildības par tiem, 2016. gada 18. maijs, (OR.en) 8557/16, 3. panta 1. punkts. Skatīt arī Komisijas paziņojumu par ES un ASV 2010. gada 26. maija sarunām par datu aizsardzības nolīgumu, MEMO/10/216 un ES Komisijas paziņojumu presei (2010) par augstiem privātuma standartiem ES un ASV 2010. gada 26. maijā noslēgtajā datu aizsardzības nolīgumā, IP/10/609.

Nolīgumā noteikti vairāki aizsardzības pasākumi, lai nodrošinātu personas datu izmantošanu tikai nolīgumā paredzētajiem mērķiem. Jo īpaši ar to nodrošina šādu aizsardzību ES pilsoņiem:

- datu izmantošanas ierobežojumi: personas datus drīkst izmantot tikai noziedzīgu nodarījumu novēršanai, izmeklēšanai, atklāšanai vai saukšanai pie atbildības par tiem;
- aizsardzība pret patvaļīgu un neattaisnojamu diskrimināciju;
- tālāknosūtīšana: jebkurai nosūtīšanai valstij, kas nav ASV vai ES valsts, vai starptautiskai organizācijai, ir nepieciešama iepriekšēja piekrišana no tās valsts kompetentās iestādes, kura sākotnēji nosūtīja datus;
- datu kvalitāte: personas dati ir jāsaglabā, ņemot vērā to precizitāti, atbilstību, savlaicīgumu un pilnīgumu;
- apstrādes drošība, tostarp paziņošana par personas datu pārkāpumiem;
- sensitīvu datu apstrāde ir atļauta tikai, piemērojot attiecīgus aizsardzības pasākumus saskaņā ar likumu;
- glabāšanas termiņi: personas datus nedrīkst saglabāt ilgāk nekā tie nepieciešami vai atbilstoši;
- piekļuves un labošanas tiesības: jebkurai personai ir tiesības piekļūt saviem personas datiem, piemērojot noteiktus nosacījumus, un pieprasīt labot datus, ja tie ir nepareizi;
- automatizētiem lēmumiem nepieciešami attiecīgi aizsardzības pasākumi, tostarp iespēja panākt cilvēka līdzdalību;
- efektīva uzraudzība, tostarp sadarbība starp ES un ASV uzraudzības iestādēm; un
- tiesiskās aizsardzības līdzekļi un izpildes panākšana. ES pilsoņiem ir tiesības[810] lūgt tiesisko aizsardzību ASV tiesā, ja ASV varas iestādes liedz piekļuvi vai veikt labojumus, vai nelikumīgi izpauž viņu personas datus.

810 ASV Likumu par tiesisko aizsardzību izsludināja prezidents *Obama* 2016. gada 24. februārī.

"Jumta nolīguma" ietvaros ir izveidota arī sistēma, lai vajadzības gadījumā informētu skarto personu kompetento uzraudzības iestādi dalībvalstī par visiem datu aizsardzības pārkāpumiem. Nolīgumā paredzētās juridiskās garantijas nodrošina vienlīdzīgu attieksmi pret ES pilsoņiem ASV, kur notiek privātuma pārkāpums[811].

8.3.1. Datu aizsardzība ES tiesu un tiesībaizsardzības iestādēs

Eiropols

ES tiesībaizsardzības aģentūras Eiropols galvenā mītne atrodas Hāgā, un katrā dalībvalstī ir Eiropola nacionālās vienības (*ENU*). Eiropols tika izveidots 1998. gadā. Aģentūras kā ES iestādes pašreizējais juridiskais statuss balstīts regulā par Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (Eiropola regula)[812]. Eiropola mērķis ir palīdzēt novērst un izmeklēt organizēto noziedzību, terorismu un citus smagu noziegumu veidus, kas uzskaitīti Eiropola regulas I pielikumā un skar divas vai vairākas dalībvalstis. To īsteno, veicot informācijas apmaiņu un darbojoties kā ES informācijas centram, kā arī nodrošinot izlūkdatu analīzes un draudu novērtējumus.

Lai sasniegtu savus mērķus, Eiropols ir izveidojis Eiropola informācijas sistēmu, kas nodrošina datubāzi, kurā dalībvalstis apmainās ar kriminālizlūkošanu un informāciju, izmantojot savas *ENU*. Eiropola informācijas sistēmu var izmantot, lai padarītu pieejamus datus, kas attiecas uz: personām, kuras tiek turētas aizdomās vai ir notiesātas par Eiropola kompetencē esošu noziedzīgu nodarījumu; vai personām, par kurām ir faktiskas norādes, ka tās izdarīs šādus pārkāpumus. Eiropols un *ENU* var ievadīt datus tieši Eiropola informācijas sistēmā un iegūt datus no tās. Datus modificēt, labot vai dzēst var tikai persona, kura ievadījusi datus sistēmā. ES struktūras, trešās valstis un starptautiskās organizācijas arī var sniegt informāciju Eiropolam.

811 Eiropas Datu aizsardzības uzraudzītājs izdeva atzinumu par ES un ASV nolīgumu, cita starpā iesakot šādas korekcijas: 1) pantu, kas skar datu saglabāšanu ne ilgāk kā nepieciešami un atbilstoši, papildināt ar frāzi "konkrētiem mērķiem, kuriem tie tika pārsūtīti", un 2) izslēgt sensitīvu datu masveida nosūtīšanu, kas varētu būt iespējama. Skatīt Eiropas Datu aizsardzības uzraudzītāja Atzinumu 1/2016, *Sākotnējais atzinums attiecībā uz Amerikas Savienoto Valstu un Eiropas Savienības nolīgumu par personas datu aizsardzību saistībā ar noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu un saukšanu pie atbildības par tiem*, 35. punkts.

812 Eiropas Parlamenta un Padomes 2016. gada 11. maija Regula (ES) 2016/794 par Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (Eiropolu) un ar kuru aizstāj un atceļ Padomes Lēmumus 2009/371/TI, 2009/934/TI, 2009/935/TI, 2009/936/TI un 2009/968/TI, OV 2016 L 135, 53. lpp.

Informāciju, tostarp personas datus, Eiropols var iegūt arī no publiski pieejamiem avotiem, piemēram, internetā. Personas datu nosūtīšana ES struktūrām ir atļauta tikai tad, ja tas ir nepieciešams Eiropola vai saņēmējas ES struktūras uzdevuma izpildei. Personas datu nosūtīšana trešām valstīm vai starptautiskām organizācijām ir atļauta tikai tad, ja Eiropas Komisija nolemj, ka attiecīgā valsts vai starptautiskā organizācija nodrošina pietiekamu datu aizsardzības līmeni ("lēmums par aizsardzības līmeņa pietiekamību") vai arī ir noslēgts starptautisks vai sadarbības nolīgums. Eiropols var saņemt un apstrādāt personas datus no privātām pusēm un privātpersonām, piemērojot stingrus nosacījumus, ka šos datus nosūta *ENU* saskaņā ar tās valsts tiesību aktiem, kontaktpunkts trešā valstī vai starptautiska organizācija, ar kuru ir izveidota sadarbība, noslēdzot sadarbības nolīgumu, vai ar trešās valsts iestādes vai starptautiskas organizācijas starpniecību, uz kuru attiecas lēmums par aizsardzības līmeņa pietiekamību vai ar kuru ES ir noslēgusi starptautisku nolīgumu. Visa informācijas apmaiņa notiek, izmantojot drošas informācijas apmaiņas tīkla lietojumprogrammu (*SIENA*).

Reaģējot uz jaunākajām tendencēm, Eiropolā ir izveidoti specializēti centri. Eiropas Kibernoziedzības apkarošanas centrs Eiropolā tika izveidots 2013. gadā[813]. Šis centrs darbojas kā ES informācijas centrs kibernoziedzības jautājumos, ļaujot ātrāk reaģēt tiešsaistes noziegumu gadījumā, attīstot un izmantojot digitālās kriminālistikas iespējas un nodrošinot paraugpraksi kibernoziegumu izmeklēšanā. Centrs galvenokārt pievēršas kibernoziegumiem:

- ko izdara organizētas grupas nolūkā gūt lielu peļņu no noziedzīgiem nodarījumiem, piemēram, tiešsaistes krāpniecība;
- kas cietušajam nodara nopietnu kaitējumu, piemēram, bērnu seksuāla izmantošana tiešsaistē;
- kas skar kritisko infrastruktūru vai informācijas sistēmas ES iekšienē.

Eiropas Terorisma apkarošanas centrs (*ECTC*) tika izveidots 2016. gada janvārī ar mērķi sniegt operatīvu atbalstu dalībvalstīm izmeklēšanā, kas saistīta ar teroristu nodarījumiem. Tas salīdzina reālā laika operatīvos datus ar Eiropola rīcībā esošajiem

813 Skatīt arī EDAU (2012) *Atzinumu attiecībā uz Eiropas Komisijas paziņojumu Padomei un Eiropas Parlamentam par Eiropas Kibernoziedzības apkarošanas centra izveidi*, Brisele, 2012. gada 29. jūnijs.

datiem, ātri atklājot finanšu pavedienus, un analizē visu pieejamo izmeklēšanas informāciju, lai palīdzētu izveidot strukturētu teroristu tīkla ainu[814].

Eiropas Migrantu kontrabandas apkarošanas centrs (EMKAC) tika izveidots 2016. gada februārī pēc Padomes sanāksmes, kas noturēta 2015. gada novembrī nolūkā atbalstīt dalībvalstis, mērķējot uz un iznīcinot noziedzīgos tīklus, kas iesaistīti nelegālā migrantu kontrabandā. Tas darbojas kā informācijas centrs, sniedzot atbalstu ES reģionālajiem darba grupu birojiem Katānijā (Itālija) un Pirejā (Grieķija), kas palīdz valstu pārvaldes iestādēm vairākās jomās, tostarp izlūkdatu apmaiņā, kriminālizmeklēšanā un kriminālvajāšanā pret cilvēku kontrabandas tīkliem[815].

Datu aizsardzības režīms, kas regulē Eiropola darbības, ir ticis uzlabots un balstās uz ES iestāžu datu aizsardzības regulas[816] principiem, kā arī atbilst Datu aizsardzības direktīvai policijas un krimināltiesību jomā, modernizētajai Konvencijai Nr. 108 un Policijas ieteikumam.

Personas datus attiecībā uz noziedzīgos nodarījumos cietušām personām, lieciniekiem vai citām personām, kuras var sniegt informāciju par noziedzīgiem nodarījumiem, vai personām, kuras ir jaunākas par 18 gadiem, ir atļauts apstrādāt, ja tas ir noteikti nepieciešams un samērīgs pasākums, lai novērstu vai apkarotu noziedzību, uz kuru attiecas Eiropola mērķi[817]. Sensitīvu personas datu apstrāde ir aizliegta, ja vien tas nav absolūti nepieciešami un samērīgi tādu noziedzīgu nodarījumu novēršanai vai apkarošanai, kas atbilst Eiropola mērķiem, un ja šie dati papildina citus Eiropola apstrādātos personas datus[818]. Abos gadījumos tikai Eiropolam ir piekļuve attiecīgajiem datiem[819].

Datu saglabāšana ir atļauta tikai nepieciešamā un samērīgā termiņā, un tās turpināšana tiek pārskatīta ik pēc trim gadiem. Bez šādas pārskatīšanas dati tiek automātiski dzēsti[820].

814 Skatīt Eiropola *tīmekļa vietni par ECTC*.

815 Skatīt Eiropola tīmekļa vietni par EMKAC.

816 Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti, OV 2001 L 8.

817 Eiropola regula, 30. panta 1. punkts.

818 Turpat, 30. panta 2. punkts.

819 Turpat, 30. panta 3. punkts.

820 Turpat, 31. pants.

Ievērojot zināmus nosacījumus, Eiropols drīkst nosūtīt personas datus tieši ES struktūrai vai trešās valsts iestādei, vai starptautiskai organizācijai[821]. Par datu pārkāpumiem, ja tie varētu nopietni un nelabvēlīgi ietekmēt attiecīgo datu subjektu tiesības un brīvības, jāpaziņo bez nepamatotas kavēšanās[822]. Dalībvalstu līmenī Eiropola veiktās personas datu apstrādes uzraudzībai tiek nozīmēta valsts uzraudzības iestāde[823].

EDAU pienākums ir uzraudzīt un nodrošināt fizisko personu pamattiesību un brīvību aizsardzību Eiropola veiktās personas datu apstrādes jomā, kā arī konsultēt Eiropolu un datu subjektus visos ar personas datu apstrādi saistītajos jautājumos. Šajā nolūkā EDAU darbojas kā izmeklēšanas un sūdzību izskatīšanas struktūra un ciešā sadarbībā ar valstu uzraudzības iestādēm[824]. EDAU un valstu uzraudzības iestādes vismaz divas reizes gadā tiksies Sadarbības padomē, kurai ir padomdevēja funkcija[825]. Dalībvalstīm ar likumu ir jāizveido uzraudzības iestāde, kas ir kompetenta uzraudzīt, vai personas datu nosūtīšana no valsts līmeņa Eiropolam un personas datu iegūšana ir pieļaujama, kā arī jebkādu saziņu ar Eiropolu no dalībvalsts puses[826]. Dalībvalstīm arī tiek prasīts nodrošināt valsts uzraudzības iestādes darbības pilnīgu neatkarību, pildot savus uzdevumus un pienākumus saskaņā ar Eiropola regulu[827]. Lai pārbaudītu datu apstrādes likumību, pašuzraudzītu savas aktivitātes un nodrošinātu datu integritāti un drošību, Eiropols uztur datu apstrādes darbību reģistrus vai dokumentāciju. Šajos reģistros ir informācija par apstrādes darbībām automatizētās apstrādes sistēmās, kas saistītas ar datu vākšanu, pārveidošanu, piekļuvi, izpaušanu, kombinēšanu vai dzēšanu[828].

EDAU lēmumu var pārsūdzēt EST[829]. Ikvienai personai, kurai nodarīts kaitējums nelikumīgas datu apstrādes darbības rezultātā, ir tiesības saņemt kompensāciju par nodarīto kaitējumu vai nu no Eiropola, vai no atbildīgās dalībvalsts, pirmajā gadījumā iesniedzot prasību EST vai otrajā gadījumā – kompetentajā valsts tiesā[830]. Turklāt

821 Turpat, attiecīgi 24. un 25. pants.
822 Turpat, 35. pants.
823 Eiropola regula, 42. pants.
824 Turpat, 43. un 44. pants.
825 Turpat, 45. pants.
826 Turpat, 42. panta 1. punkts.
827 Turpat, 42. panta 1. punkts.
828 Turpat, 40. pants.
829 Turpat, 48. pants.
830 Turpat, 50. pants.

valstu parlamentu un Eiropas Parlamenta specializētā Kopējā parlamentārās pārraudzības grupa var veikt Eiropola darbību pārbaudi[831]. Ikvienam indivīdam ir tiesības piekļūt visiem saviem personas datiem, kas ir Eiropola rīcībā, papildus tiesībām pieprasīt veikt šo personas datu pārbaudi, labojumus vai dzēšanu. Uz šīm tiesībām var attiekties atbrīvojumi un ierobežojumi.

Eurojust

Eurojust ir 2002. gadā izveidota ES struktūra, kuras galvenā mītne atrodas Hāgā. Tā veicina tiesu iestāžu sadarbību izmeklēšanā un kriminālvajāšanā saistībā ar smagiem noziegumiem, kas skar vismaz divas dalībvalstis[832]. *Eurojust* kompetences jomas ir šādas:

- stimulēt un uzlabot izmeklēšanas un kriminālvajāšanas koordinēšanu starp dažādu dalībvalstu kompetentajām iestādēm;

- atvieglot pieprasījumu un lēmumu izpildi saistībā ar tiesu iestāžu sadarbību.

Eurojust funkcijas pilda valstu pārstāvji. Katra dalībvalsts deleģē *Eurojust* vienu tiesnesi vai prokuroru, kura statuss ir noteikts valsts tiesību aktos un kuram ir vajadzīgās pilnvaras, lai pildītu tiesu iestāžu sadarbības stimulēšanai un uzlabošanai nepieciešamos uzdevumus. Turklāt valstu pārstāvji, pildot īpašus *Eurojust* uzdevumus, kopīgi darbojas kā kolēģija.

Eurojust drīkst apstrādāt personas datus, ciktāl tas nepieciešams tās mērķu sasniegšanai. Tomēr tas attiecas tikai uz konkrētu informāciju par personām, kuras tiek turētas aizdomās par noziedzīga nodarījuma izdarīšanu, dalību tajos vai ir tikušas notiesātas par šādiem noziedzīgiem nodarījumiem, kas ir *Eurojust* kompetencē. *Eurojust* drīkst arī apstrādāt noteiktu informāciju par noziedzīgu nodarījumu, kas ir *Eurojust* kompetencē, lieciniekiem vai cietušajiem[833]. Izņēmuma gadījumos *Eurojust* ierobe-

831 Turpat, 51. pants.

832 Eiropas Savienības Padome (2002), Padomes 2002. gada 28. februāra Lēmums 2002/187/TI, ar ko izveido *Eurojust*, lai pastiprinātu cīņu pret smagiem noziegumiem, OV 2002 L 63; Eiropas Savienības Padome (2003), Padomes 2003. gada 18. jūnija Lēmums 2003/659/TI, ar kuru groza Lēmumu 2002/187/TI, ar ko izveido *Eurojust*, lai pastiprinātu cīņu pret smagiem noziegumiem, OV 2003 L 44; Eiropas Savienības Padome (2009), Padomes 2008. gada 16. decembra Lēmums 2009/426/TI par *Eurojust* stiprināšanu un ar kuru groza Lēmumu 2002/187/TI, ar ko izveido *Eurojust*, lai pastiprinātu cīņu pret smagiem noziegumiem, OV 2009 L 138 (*Eurojust* lēmums).

833 Padomes lēmuma 2002/187/TI, ko groza ar Padomes lēmumu 2003/659/TI un Padomes lēmumu 2009/426/TI konsolidētā versija, 15. panta 2. punkts.

žotā laika periodā var apstrādāt plašākus personas datus, kas attiecas uz nodarījuma apstākļiem, ja šie dati ir tieši saistīti ar noziedzīgu izmeklēšanu. *Eurojust* savas kompetences ietvaros var sadarboties ar citām ES iestādēm, struktūrām un aģentūrām, kā arī apmainīties ar tām ar personas datiem. *Eurojust* drīkst arī sadarboties un apmainīties ar personas datiem ar trešām valstīm un organizācijām.

Datu aizsardzības jomā *Eurojust* ir pienākums garantēt aizsardzības līmeni, kas ir vismaz līdzvērtīgs modernizētās Konvencijas Nr. 108 un tās turpmāko grozījumu principiem. Veicot datu apmaiņu, ir jāievēro īpaši noteikumi un ierobežojumi, kas tiek ieviesti vai nu sadarbības līgumā, vai darba kārtībā saskaņā ar *Eurojust* Padomes lēmumiem un *Eurojust* datu aizsardzības noteikumiem[834].

Eurojust ir izveidota neatkarīga Apvienotā uzraudzības iestāde (AUI), kuras uzdevums ir uzraudzīt *Eurojust* veikto personas datu apstrādi. Ja personas neapmierina *Eurojust* lēmums par piekļuvi personas datiem, to labošanu, bloķēšanu vai dzēšanu, to var pārsūdzēt AUI. Ja *Eurojust* personas datus apstrādā nelikumīgi, *Eurojust* saskaņā ar tās dalībvalsts, kurā atrodas tās galvenā mītne, proti, Nīderlandes tiesību aktiem atbild par datu subjektam nodarītajiem zaudējumiem.

Perspektīva

Eiropas Komisija 2013. gada jūlijā iesniedza priekšlikumu regulai par *Eurojust* reformu. Šim priekšlikumam tika pievienots priekšlikums izveidot Eiropas Prokuratūru (skatīt zemāk). Šīs regulas mērķis ir pilnveidot funkcijas un struktūru atbilstoši Lisabonas līgumam. Turklāt reformas mērķis ir skaidri nodalīt *Eurojust* operatīvos uzdevumus, ko veic *Eurojust* kolēģija, un tās administratīvos uzdevumus. Tas arī ļauj dalībvalstīm vairāk pievērsties operatīvajiem uzdevumiem. Tiks izveidota jauna Valde, kas palīdzēs kolēģijai pildīt administratīvos uzdevumus[835].

Eiropas Prokuratūra

Dalībvalstīm ir ekskluzīva kompetence veikt kriminālvajāšanu par noziedzīgiem nodarījumiem saistībā ar krāpšanu un nepareizu ES budžeta izmantošanu, kam var būt arī pārrobežu sekas. Šādu pārkāpumu izdarītāju izmeklēšanas, kriminālvajāšanas un saukšanas pie atbildības nozīme ir pieaugusi, īpaši ņemot vērā pašreizējo

834 *Eurojust* iekšējie noteikumi par personas datu apstrādi un aizsardzību, OV 2005, C 68/01, 2005. gada 19. marts, 1. lpp.

835 Skatīt Eiropas Komisijas *Eurojust* tīmekļa vietni.

ekonomisko krīzi[836]. Eiropas Komisija ir iesniegusi priekšlikumu regulai par neatkarīgas Eiropas Prokuratūras (*EPPO*[837]) izveidi ar mērķi apkarot noziedzīgus nodarījumus, kas skar ES finanšu intereses. *EPPO* tiks izveidota, izmantojot ciešākas sadarbības procedūru, kas ļauj vismaz deviņām dalībvalstīm izveidot pastiprinātu sadarbību ES struktūru jomā, neiesaistot citas ES valstis[838]. Ciešākajai sadarbībai ir pievienojušās Beļģija, Bulgārija, Čehijas Republika, Francija, Grieķija, Horvātija, Igaunija, Kipra, Latvija, Lietuva, Luksemburga, Portugāle, Rumānija, Slovākija, Slovēnija, Somija, Spānija un Vācija. Austrija un Itālija ir izteikušas nodomu pievienoties[839].

EPPO būs kompetenta izmeklēt un ierosināt ES kriminālvajāšanu par krāpšanu un citiem noziegumiem, kas ietekmē ES finanšu intereses, ar mērķi efektīvi koordinēt izmeklēšanu un kriminālvajāšanu dažādās valstu tiesību sistēmās, kā arī uzlabot resursu izmantošanu un informācijas apmaiņu Eiropas mērogā[840].

EPPO vadīs Eiropas prokurors, un katrā dalībvalstī tiks deleģēts vismaz viens Eiropas prokurors, kurš būs atbildīgs par izmeklēšanu un kriminālvajāšanu šajā dalībvalstī.

Priekšlikumā ir noteikti stingri aizsardzības pasākumi *EPPO* izmeklēšanā iesaistīto personu tiesību garantēšanai, kā noteikts valstu, ES tiesību aktos un ES Pamattiesību hartā. Izmeklēšanas pasākumiem, kas galvenokārt attiecas uz pamattiesībām, būs nepieciešama iepriekšēja valsts tiesas atļauja[841]. *EPPO* izmeklēšanu pārskatīs valstu tiesas[842].

Uz *EPPO* veikto administratīvo personas datu apstrādi attieksies ES iestāžu datu aizsardzības regula[843]. Tādu personas datu apstrādei, kas saistīti ar operatīvajiem jau-

836 Skatīt Eiropas Komisijas (2013) Priekšlikumu Padomes Regulai par Eiropas Prokuratūras izveidi, COM(2013) 534 *final*, Brisele, 2013. gada 17. jūlijs, 1. lpp., un Komisijas tīmekļa vietni par *EPPO*.

837 Eiropas Komisija (2013), Priekšlikums Padomes Regulai par Eiropas Prokuratūras izveidi, COM(2013) 534 *final*, Brisele, 2013. gada 17. jūlijs

838 Līgums par Eiropas Savienības darbību, 86. panta 1. punkts un 329. panta 1. punkts.

839 Skatīt Eiropas Savienības Padome (2017), "20 dalībvalstis vienojas par Eiropas Prokuratūras (EPPO) izveides detaļām", paziņojums presei, 2017. gada 8. jūnijs.

840 Eiropas Komisija (2013), Priekšlikums Padomes Regulai par Eiropas Prokuratūras izveidi, COM(2013) 534 *final*, Brisele, 2013. gada 17. jūlijs, 1. lpp. un 51. lpp. Skatīt arī Eiropas Komisijas tīmekļa vietni par *EPPO*.

841 Eiropas Komisija (2013), Priekšlikums Padomes Regulai par Eiropas Prokuratūras izveidi, COM(2013) 534 *final*, Brisele, 2013. gada 17. jūlijs, 26. panta 4. punkts.

842 Turpat, 36. pants.

843 Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti, OV 2001 L 8.

tājumiem, piemēram, Eiropolu, *EPPO* būs atsevišķs datu aizsardzības režīms, līdzīgs tam, ko piemēro Eiropola un *Eurojust* darbībām, ņemot vērā, ka *EPPO* funkciju īstenošana ietvers personas datu apstrādi sadarbībā ar tiesībaizsardzības un krimināltvajāšanas iestādēm dalībvalstu mērogā. Tāpēc *EPPO* datu aizsardzības noteikumi ir gandrīz identiski Datu aizsardzības direktīvā policijas un krimināltiesību jomā ietvertajiem noteikumiem. Saskaņā ar priekšlikumu par *EPPO* izveidi personas datu apstrādei ir jāatbilst likumības un godprātības, nolūka ierobežojuma, datu minimizēšanas, precizitātes, integritātes un konfidencialitātes principiem. *EPPO* pēc iespējas skaidri jānošķir dažāda veida datu subjektu piemēram, personu, kuras notiesātas par noziedzīgu nodarījumu, personu, kuras ir tikai aizdomās turamās, cietušo un liecinieku, personas dati. Tai jācenšas arī pārbaudīt apstrādāto personas datu kvalitāti un pēc iespējas nošķirt faktos balstītus personas datus no personas datiem, kas balstīti uz personīgiem novērtējumiem.

Priekšlikumā ir ietverti noteikumi par datu subjektu tiesībām, jo īpaši tiesībām uz informāciju, piekļuvi saviem personas datiem, to labošanu, dzēšanu un apstrādes ierobežošanu, un paredzēts, ka šādas tiesības var izmantot arī netieši, ar EDAU starpniecību. Tajā ietverti arī apstrādes drošības un pārskatatbildības principi, pieprasot *EPPO* ieviest attiecīgus tehniskos un organizatoriskos pasākumus, lai nodrošinātu apstrādes radītajiem riskiem atbilstošu drošības līmeni, reģistrēt visas apstrādes darbības un veikt datu aizsardzības ietekmes novērtējumu pirms apstrādes, ja apstrādes veids (piemēram, apstrāde, izmantojot jaunas tehnoloģijas), iespējams, rada lielu risku personu tiesībām. Visbeidzot, priekšlikumā paredzēts, ka kolēģija ieceļ datu aizsardzības speciālistu, kurš ir pienācīgi jāiesaista visos jautājumos, kas saistīti ar personas datu aizsardzību, un kuram jānodrošina *EPPO* atbilstība piemērojamiem datu aizsardzības tiesību aktiem.

8.3.2. Datu aizsardzība ES mēroga apvienotajās informācijas sistēmās

Papildus datu apmaiņai starp dalībvalstīm un specializētu ES iestāžu, piemēram, Eiropola, *Eurojust* un *EPPO*, izveidei cīņai ar pārrobežu noziedzību ES mērogā ir izveidotas vairākas kopīgas informācijas sistēmas, kas veicina un atvieglo sadarbību un datu apmaiņu starp kompetentajām valstu un ES iestādēm noteiktiem nolūkiem robežu aizsardzības, imigrācijas, patvēruma un muitas jomā. Tā kā Šengenas zona vispirms tika izveidota, noslēdzot starptautisku nolīgumu, kas darbojas neatkarīgi no ES tiesību aktiem, Šengenas informācijas sistēmu (*SIS*) izstrādāja, pamatojoties uz daudzpusējiem nolīgumiem, un vēlāk iekļāva ES tiesību aktos. Vīzu informācijas sistēma

(VIS), *Eurodac*, *Eurosur* un Muitas informācijas sistēma (MIS) tika izveidotas kā instrumenti, ko reglamentē ES tiesību akti.

Šo sistēmu uzraudzību kopīgi veic valstu uzraudzības iestādes un EDAU. Lai nodrošinātu augstu aizsardzības līmeni, šīs iestādes sadarbojas uzraudzības koordinācijas grupās (*SCG*), kas attiecas uz šādām lielapjoma IT sistēmām: 1) *Eurodac*; 2) Vīzu informācijas sistēma; 3) Šengenas informācijas sistēma; 4) Muitas informācijas sistēma un 5) Iekšējā tirgus informācijas sistēma[844]. *SCG* parasti tiekas divreiz gadā vēlēta priekšsēdētāja vadībā un pieņem pamatnostādnes, apspriež pārrobežu gadījumus vai pieņem kopējus regulējumus pārbaudēm.

Eiropas Savienības Aģentūra lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*)[845], kas izveidota 2012. gadā, atbild par otrās paaudzes Šengenas informācijas sistēmas (*SIS II*), Vīzu informācijas sistēmas (VIS) un *Eurodac* sistēmas darbības pārvaldību. *Eu-LISA* galvenais uzdevums ir nodrošināt efektīvu, drošu un nepārtrauktu informācijas tehnoloģiju sistēmu darbību. Tā arī atbild par nepieciešamo pasākumu pieņemšanu, lai nodrošinātu sistēmu un datu drošību.

Šengenas informācijas sistēma

Vairākas bijušās Eiropas Kopienas dalībvalstis 1985. gadā noslēdza Nolīgumu starp Beniluksa Ekonomikas savienību, Vāciju un Franciju par pakāpenisku kontroles atcelšanu pie kopīgām robežām (Šengenas nolīgums), lai izveidotu brīvas personu pārvietošanās zonu bez robežkontroles Šengenas teritorijā[846]. Lai līdzsvarotu draudus sabiedriskajai drošībai, ko varētu radīt atvērtās robežas, tika pastiprināta robežkontrole uz Šengenas zonas ārējām robežām, kā arī izveidota cieša sadarbība starp valstu policijas un tieslietu iestādēm.

Papildu valstīm pievienojoties Šengenas nolīgumam, ar Amsterdamas līgumu Šengenas sistēma beidzot tika integrēta ES tiesiskajā regulējumā[847]. Šis lēmums tika

844 Skatīt Eiropas Datu aizsardzības uzraudzītāja tīmekļa vietni par pārraudzības koordinēšanu.

845 Eiropas Parlamenta un Padomes 2011. gada 25. oktobra Regula (ES) Nr. 1077/2011 par Eiropas Savienības Aģentūru lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā, OV 2011 L 286.

846 Nolīgums starp Beniluksa Ekonomikas savienības valstu valdībām, Vācijas Federatīvās Republikas valdību un Francijas Republikas valdību par pakāpenisku kontroles atcelšanu pie kopīgām robežām, OV 2000 L 239.

847 Eiropas Kopienas (1997), Amsterdamas Līgums, ar ko groza Līgumu par Eiropas Savienību, Eiropas Kopienu dibināšanas līgumus un dažus ar tiem saistītus aktus, OV 1997 C 340.

īstenots 1999. gadā. Šengenas informācijas sistēmas jaunākā versija, tā sauktā *SIS II*, savu darbību sāka 2013. gada 9. aprīlī. Šobrīd to izmanto lielākā daļa ES dalībvalstu[848], kā arī Islande, Lihtenšteina, Norvēģija un Šveice[849]. Arī Eiropolam un *Eurojust* ir piekļuve *SIS II*.

SIS II sastāv no centrālās sistēmas (*C-SIS*), valsts sistēmas (*N-SIS*) katrā dalībvalstī un sakaru infrastruktūras starp centrālo sistēmu un valstu sistēmām. *C-SIS* satur noteiktus datus, kurus dalībvalstis ievadījušas par personām un objektiem. Valstu robežkontroles punkti, policijas, muitas, vīzu un tiesu iestādes visā Šengenas zonā izmanto *SIS*. Katra dalībvalsts izmanto *C-SIS* nacionālo kopiju, kas zināma kā Valsts Šengenas informācijas sistēmas (*N-SIS*), kuru pastāvīgi atjaunina, tādējādi atjauninot *C-SIS*. *SIS* satur dažādus brīdinājumu veidus:

- personai nav tiesību ieceļot vai uzturēties Šengenas teritorijā; vai
- persona vai objekts ir tiesu vai tiesībaizsardzības iestādes meklēšanā (piemēram, Eiropas apcietināšanas orderi, lūgumi veikt diskrētas pārbaudes); vai
- persona ir izsludināta par pazudušu; vai
- iesniegts paziņojums, ka mantas, piemēram, banknotes, automašīnas, furgoni, šaujamieroči un personu apliecinoši dokumenti, ir nozagtas vai pazaudētas.

Ja ir brīdinājums, jāveic papildu darbības ar *SIRENE* biroju starpniecību. *SIS II* ir jaunas funkcijas, piemēram, iespēja ievadīt: biometriskos datus, piemēram, pirkstu nospiedumus un fotogrāfijas; vai jaunas brīdinājumu kategorijas, piemēram, nozagtas laivas, lidmašīnas, konteinerus vai maksāšanas līdzekļus; uzlabotus brīdinājumus par personām un objektiem; un Eiropas apcietināšanas ordera (EAO) kopijas attiecībā uz meklēšanā esošām personām, lai tās apcietinātu, nodotu vai izdotu.

848 Horvātija, Īrija un Kipra veic sagatavošanās darbus integrācijai *SIS II*, taču vēl tajā nepiedalās. Vairāk informācijas par Šengenas informācijas sistēmu skatīt Eiropas Komisijas Migrācijas un iekšlietu ģenerāldirektorāta tīmekļa vietnē.

849 Eiropas Parlamenta un Padomes 2006. gada 20. decembra Regula (EK) Nr. 1987/2006 par otrās paaudzes Šengenas Informācijas sistēmas (*SIS II*) izveidi, darbību un izmantošanu, OV 2006 L 381 (*SIS II*), un Eiropas Savienības Padome (2007), Padomes 2007. gada 12. jūnija Lēmums 2007/533/TI par otrās paaudzes Šengenas Informācijas sistēmas (*SIS II*) izveidi, darbību un izmantošanu, (*SIS II*), OV 2007 L 205.

SIS II balstās divos tiesību aktos, kas papildina viens otru: *SIS II* lēmums[850] un *SIS II* regula[851]. ES likumdevējs lēmuma un regulas pieņemšanai izmantoja atšķirīgu juridisko pamatu. Lēmums regulē *SIS II* izmantošanu nolūkos, uz kuriem attiecas policijas un tiesu iestāžu sadarbība krimināllietās (agrākais ES trešais pīlārs). Regulu piemēro brīdināšanas procedūrām, kas attiecas uz vīzu, patvēruma, imigrācijas un citām politikām, kas skar personu brīvu pārvietošanos (agrākais pirmais pīlārs). Brīdināšanas procedūras attiecībā uz katru pīlāru bija jāreglamentē atsevišķos tiesību aktos, ņemot vērā, ka abi tiesību akti tika pieņemti pirms Lisabonas līguma un pīlāru struktūras atcelšanas.

Abi tiesību akti satur noteikumus par datu aizsardzību. *SIS II* lēmums aizliedz apstrādāt sensitīvus datus[852]. Personas datu apstrāde ietilpst modernizētās Konvencijas Nr. 108 piemērošanas jomā[853]. Turklāt personām ir tiesības piekļūt ar viņu saistītajiem *SIS II* ievadītajiem personas datiem[854].

SIS II regula reglamentē nosacījumus un procedūras brīdinājumu ievadīšanai un apstrādei attiecībā uz trešo valstu pilsoņu ieceļošanas vai uzturēšanās atteikumiem. Tajā arī paredzēti noteikumi apmaiņai ar papildinformāciju ieceļošanas vai uzturēšanās dalībvalstī nolūkos[855]. Regula satur arī noteikumus par datu aizsardzību. Nav atļauts apstrādāt Vispārīgās datu aizsardzības regulas 9. panta 1. punktā minētās sensitīvu personas datu kategorijas[856]. *SIS II* regulā ir ietvertas arī šādas noteiktas datu subjekta tiesības:

- tiesības piekļūt personas datiem, kas attiecas uz datu subjektu[857];
- tiesības labot datus, kuros ir faktu kļūda[858];

850 Padomes 2007. gada 12. jūnija Lēmums 2007/533/TI par otrās paaudzes Šengenas Informācijas sistēmas (*SIS II*) izveidi, darbību un izmantošanu, OV L 205, 2007. gada 7. augusts.

851 Eiropas Parlamenta un Padomes 2006. gada 20. decembra Regula (EK) Nr. 1987/2006 par otrās paaudzes Šengenas Informācijas sistēmas (*SIS II*) izveidi, darbību un izmantošanu, OV L 381, 2006. gada 28. decembris.

852 *SIS II* lēmums, 56. pants; *SIS II* regula, 40. pants.

853 *SIS II* lēmums, 57. pants.

854 *SIS II* lēmums, 58. pants; *SIS II* regula, 41. pants.

855 *SIS II* regula, 2. pants.

856 Turpat, 40. pants.

857 Turpat, 41. panta 1. punkts.

858 Turpat, 41. panta 5. punkts.

- tiesības dzēst nelikumīgi saglabātus datus[859]; un

- tiesības tikt informētam, ja par datu subjektu ir izdots brīdinājums. Informāciju sniedz rakstiski, pievienojot lēmuma kopiju vai atsauci uz lēmumu par brīdinājuma izdošanu[860].

Tiesības tikt informētam nenodrošina, ja 1) personas dati nav iegūti no datu subjekta un informācijas sniegšana nav iespējama, vai tā ir saistīta ar nesamērīgu piepūli; 2) ja datu subjektam jau ir šī informācija; vai 3) ja valsts tiesību aktos ir atļauti ierobežojumi tiesībām, cita starpā nolūkā aizsargāt valsts drošību vai novērst noziedzīgus nodarījumus[861].

Gan attiecībā uz *SIS II* lēmumu, gan uz *SIS II* regulu var izmantot indivīdu piekļuves tiesības *SIS II* jebkurā dalībvalstī, un tās tiek īstenotas saskaņā ar šīs dalībvalsts tiesību aktiem[862].

Piemērs. Lietā *Dalea pret Franciju*[863] prasītājam tika atteikta vīza Francijas apmeklējumam, jo Francijas iestādes bija ievietojušas paziņojumu Šengenas informācijas sistēmā, ka šai personai ieceļošana ir jāatsaka. Prasītājs nesekmīgi lūdza nodrošināt piekļuvi datiem un to labošanu vai dzēšanu vispirms Francijas Datu aizsardzības komisijā un, visbeidzot, Valsts padomē. ECT uzskatīja, ka ziņojumi par prasītāju Šengenas informācijas sistēmā bija saskaņā ar likumu un šādi tika īstenots leģitīmais mērķis aizsargāt valsts drošību. Tā kā prasītājs nespēja pierādīt, kā viņš faktiski ir cietis sakarā ar atteikumu ieceļot Šengenas zonā, un tā kā tika veikti pietiekami pasākumi, lai viņu pasargātu no patvaļīgu lēmumu pieņemšanas, iejaukšanās viņa tiesībās uz privātās dzīves neaizskaramību bija samērīga. Tādējādi prasītāja sūdzība saskaņā ar 8. pantu tika atzīta par nepieņemamu.

Katras dalībvalsts kompetentā valsts uzraudzības iestāde pārrauga vietējās *N-SIS*. Valsts uzraudzības iestādei ir jānodrošina, ka datu apstrādes darbību revīzija vietējā *N-SIS* tiek veikta vismaz reizi četros gados[864]. Valstu uzraudzības iestādes un EDAU

859 Turpat, 41. panta 5. punkts.

860 Turpat, 42. panta 1. punkts.

861 Turpat, 42. panta 2. punkts.

862 *SIS II* regula, 41. panta 1. punkts un *SIS II* lēmums, 58. pants.

863 ECT 2010. gada 2. februāra spriedums lietā *Dalea pret Franciju*, Nr. 964/07.

864 *SIS II* regula, 60. panta 2. punkts.

sadarbojas un nodrošina *N-SIS* koordinētu pārraudzību, savukārt EDAU ir atbildīgs par *C-SIS* pārraudzību. Pārredzamības nolūkos reizi divos gados Eiropas Parlamentam, Padomei un *eu-LISA* tiek nosūtīts kopīgs darbības pārskats. *SIS II* uzraudzības koordinācijas grupa (*SCG*) ir izveidota, lai nodrošinātu *SIS* pārraudzības koordināciju, un tā sanāk kopā līdz divām reizēm gadā. Šajā grupā ietilpst EDAU un uzraudzības iestāžu pārstāvji no dalībvalstīm, kuras ir ieviesušas *SIS II*, kā arī Islandes, Lihtenšteinas, Norvēģijas un Šveices, jo *SIS* attiecas arī uz tām, ņemot vērā, ka šīs valstis ir Šengenas dalībnieces[865]. Horvātija, Īrija un Kipra vēl nav iekļautas *SIS II*, un tāpēc tās piedalās *SCG* tikai novērotāju statusā. *SCG* kontekstā EDAU un valstu uzraudzības iestādes aktīvi sadarbojas, apmainoties ar informāciju, palīdzot cita citai veikt revīzijas un pārbaudes, izstrādājot saskaņotus priekšlikumus iespējamo problēmu kopīgiem risinājumiem, kā arī veicinot izpratni par datu aizsardzības tiesībām[866]. *SIS II SCG* arī pieņem pamatnostādnes, lai palīdzētu datu subjektiem. Viens piemērs ir rokasgrāmata, kas palīdz datu subjektiem īstenot savas piekļuves tiesības[867].

Perspektīva

Eiropas Komisija 2016. gadā veica *SIS* novērtējumu[868], parādot, ka ir ieviesti valstu mehānismi, ļaujot datu subjektiem piekļūt *SIS II*, labot un dzēst viņu personas datus vai saņemt kompensāciju saistībā ar kļūdainiem datiem. Lai uzlabotu *SIS II* efektivitāti un lietderību, Eiropas Komisija iesniedza trīs regulas priekšlikumus:

- regula par *SIS* izveidi, darbību un izmantošanu robežkontroles jomā, ar kuru atcelt *SIS II* regulu;
- regula par *SIS* izveidi, darbību un izmantošanu policijas un tiesu iestāžu sadarbības krimināllietās jomā, ar kuru, cita starpā, atcelt *SIS II* lēmumu; un
- regula par *SIS* izmantošanu to trešo valstu valstspiederīgo atgriešanai, kuri dalībvalstīs uzturas nelikumīgi.

865 Skatīt Eiropas Datu aizsardzības uzraudzītāja tīmekļa vietni par Šengenas informācijas sistēmu.

866 *SIS II* regula, 46. pants un *SIS II* lēmums, 62. pants.

867 Skatīt *SIS II SCG*, Šengenas informācijas sistēma. Rokasgrāmata piekļuves tiesību īstenošanai, pieejama EDAU tīmekļa vietnē.

868 Eiropas Komisija (2016), Komisijas ziņojums Eiropas Parlamentam un Padomei par otrās paaudzes Šengenas Informācijas sistēmas (*SIS II*) novērtējumu saskaņā ar Regulas (EK) Nr. 1987/2006 24. panta 5. punktu, 43. panta 3. punktu un 50. panta 5. punktu un Lēmuma 2007/533/TI 59. panta 3. punktu un 66. panta 5. punktu, COM(2016) 880 *final*, Brisele, 2016. gada 21. decembris.

Svarīgi, ka priekšlikumi ļauj apstrādāt arī citas biometrisko datu kategorijas papildus fotogrāfijām un pirkstu nospiedumiem, kas jau ietilpst pašreizējā *SIS II* režīmā. Arī sejas attēli, plaukstu nospiedumi un DNS profili tiks saglabāti *SIS* datubāzē. Turklāt, kaut arī ar *SIS II* regulu un *SIS II* lēmumu paredzēja iespēju veikt meklēšanu, izmantojot pirkstu nospiedumus, lai identificētu personu, priekšlikumi šo meklēšanu padara obligātu, ja personas identitāti nevar noskaidrot citā veidā. Sejas attēli, fotoattēli un plaukstu nospiedumi tiks izmantoti, lai sistēmā meklētu un identificētu cilvēkus, ja tas ir tehniski iespējams. Jaunie noteikumi par biometriskajiem raksturlielumiem rada īpašus draudus privātpersonu tiesībām. Savā atzinumā par Komisijas priekšlikumiem[869] EDAU atzīmēja, ka biometriskie dati ir ļoti jutīgi un to ievadīšanai tik liela mēroga datubāzē ir jābalstās uz pierādījumiem pamatotu novērtējumu par nepieciešamību tos iekļaut *SIS*. Citiem vārdiem, ir jāparāda jauno raksturlielumu apstrādes nepieciešamība. EDAU arī uzskatīja, ka ir jāprecizē, kāda veida informāciju var iekļaut DNS profilā. Tā kā DNS profilā var iekļaut sensitīvu informāciju (būtiskākais piemērs varētu būt informācija, kas atklāj veselības problēmas), *SIS* glabātajos DNS profilos jāietver: "tikai tā minimālā informācija, kas ir absolūti nepieciešama pazudušo personu identificēšanai un skaidri izslēdz informāciju par veselības stāvokli, rasi un jebkādu citu sensitīvu informāciju"[870]. Priekšlikumos tomēr ir noteikti papildu aizsardzības pasākumi, lai ierobežotu datu vākšanu un turpmāku apstrādi līdz tādam apjomam, kas ir absolūti nepieciešams un vajadzīgs darbības nodrošināšanai, un piekļuve ir atļauta tikai personām, kurām operatīvos nolūkos ir jāapstrādā personas dati[871]. Priekšlikumos arī *eu-LISA* tiek pilnvarota noteiktos intervālos sagatavot datu kvalitātes ziņojumus dalībvalstīm, lai regulāri pārskatītu brīdinājumus datu kvalitātes nodrošināšanas nolūkā[872].

869 EDAU (2017), EDAU Atzinums par Šengenas informācijas sistēmas jauno juridisko pamatu, Atzinums 7/2017, 2017. gada 2. maijs.

870 Turpat, 22. punkts.

871 Eiropas Komisija (2016), Priekšlikums Eiropas Parlamenta un Padomes Regulai par Šengenas Informācijas sistēmas (*SIS*) izveidi, darbību un izmantošanu policijas sadarbības un tiesu iestāžu sadarbības krimināllietās jomā, ar ko groza Regulu (ES) Nr. 515/2014 un atceļ Regulu (EK) Nr. 1986/2006, Padomes Lēmumu 2007/533/TI un Komisijas Lēmumu 2010/261/ES, COM(2016) 883 *final*, Brisele, 2016. gada 21. decembris.

872 Turpat, 15. lpp.

Vīzu informācijas sistēma

Vīzu informācijas sistēma (VIS), kuras darbību arī pārvalda *eu-LISA*, tika izstrādāta, lai atbalstītu kopējas ES vīzu politikas ieviešanu[873]. VIS ļauj Šengenas valstīm apmainīties ar datiem par personām, kuras iesniedz vīzu pieteikumus, izmantojot pilnībā centralizētu sistēmu, kas savieno Šengenas valstu konsulātus un vēstniecības trešās valstīs ar visu Šengenas valstu ārējiem robežšķērsošanas punktiem. VIS apstrādā datus par īstermiņa vīzu pieteikumiem, lai apmeklētu Šengenas zonu vai šķērsotu to tranzītā. VIS ļauj robežkontroles iestādēm, izmantojot biometriskos raksturlielumus, jo īpaši pirkstu nospiedumus, pārbaudīt, vai persona, kura uzrāda vīzu, ir tās likumīgais turētājs, un identificēt personas, kurām nav dokumentu vai ir viltoti dokumenti.

Eiropas Parlamenta un Padomes Regula (EK) Nr. 767/2008 par Vīzu informācijas sistēmu (VIS) un datu apmaiņu starp dalībvalstīm saistībā ar īstermiņa vīzām (VIS regula) reglamentē personas datu nosūtīšanas saistībā ar pieteikumiem īstermiņa vīzām nosacījumus un procedūras. Tā arī pārrauga attiecībā uz pieteikumiem pieņemtos lēmumus, tostarp lēmumus par vīzu anulēšanu, atsaukšanu vai pagarināšanu[874]. VIS regula galvenokārt attiecas uz datiem par pieteikuma iesniedzēju, viņa vai viņas vīzām, fotogrāfijām, pirkstu nospiedumiem, saitēm ar iepriekšējiem pieteikumiem un personu, kuras viņu pavada, pieteikuma datnēm vai datiem par personu uzaicināšanu[875]. Piekļuve VIS datu ievadīšanai, labošanai vai dzēšanai ir atļauta tikai vīzu iestādēm, turpretim piekļuve datiem to aplūkošanai tiek nodrošināta vīzu iestādēm un iestādēm, kuru kompetencē ir veikt pārbaudes ārējos robežšķērsošanas punktos, imigrācijas pārbaudes un patvēruma piešķiršanu.

Izpildot noteiktus nosacījumus, kompetentās valstu policijas iestādes un Eiropols var pieprasīt piekļuvi VIS ievadītajiem datiem, lai novērstu, atklātu vai izmeklētu

873 Eiropas Savienības Padome (2004), Padomes 2004. gada 8. jūnija Lēmums 2004/512/EK, ar ko izveido Vīzu informācijas sistēmu (VIS), OV 2004 L 213; Eiropas Parlamenta un Padomes 2008. gada 9. jūlija Regula (EK) Nr. 767/2008 par Vīzu informācijas sistēmu (VIS) un datu apmaiņu starp dalībvalstīm saistībā ar īstermiņa vīzām, OV 2008 L 218 (VIS regula), Eiropas Savienības Padome (2008), Padomes 2008. gada 23. jūnija Lēmums 2008/633/TI par izraudzīto dalībvalstu iestāžu un Eiropola piekļuvi Vīzu informācijas sistēmai (VIS) konsultāciju nolūkos, lai novērstu, atklātu un izmeklētu teroristu nodarījumus un citus smagus noziedzīgus nodarījumus, OV 2008 L 218.

874 VIS regula, 1. pants.

875 Eiropas Parlamenta un Padomes 2008. gada 9. jūlija Regula (EK) Nr. 767/2008 par Vīzu informācijas sistēmu (VIS) un datu apmaiņu starp dalībvalstīm saistībā ar īstermiņa vīzām (VIS regula), OV 2008 L 218, 5. pants.

teroristu un noziedzīgus nodarījumus[876]. Tā kā VIS ir izstrādāta kā instruments, lai atbalstītu kopējās vīzu politikas īstenošanu, nolūka ierobežošanas princips, saskaņā ar kuru, kā paskaidrots 3.2. iedaļā, personas datus drīkst apstrādāt tikai attiecībā uz konkrētām, skaidri noteiktām un likumīgām personām un datiem jābūt adekvātiem, atbilstošiem un ne pārmērīgiem attiecībā uz nolūkiem, kādiem dati tiek apstrādāti, tiktu pārkāpts, ja VIS pārtaptu par tiesībaizsardzības instrumentu. Šā iemesla dēļ valstu tiesībaizsardzības iestādēm un Eiropolam nav regulāras piekļuves VIS datubāzei. Piekļuvi var piešķirt tikai katrā gadījumā atsevišķi, un tai var piemērot stingrus aizsardzības pasākumus. Nosacījumi un aizsardzības pasākumi, saskaņā ar kuriem šīm iestādēm tiek piešķirta piekļuve VIS un nodrošināta tajā esošo datu apskate, ir noteikti Padomes Lēmumā 2008/633/TI[877].

Turklāt VIS regulā ir paredzētas datu subjektu tiesības. Tās ir šādas:

- Tiesības saņemt informāciju no atbildīgās dalībvalsts par datu pārziņa, kas atbild par personas datu apstrādi šajā dalībvalstī, identitāti un kontaktinformāciju, nolūkiem, kādos viņu personas dati VIS tiks apstrādāti, personām, kurām datus var pārsūtīt (saņēmējiem), un datu saglabāšanas periodu. Turklāt vīzu pieteikumu iesniedzējiem jābūt informētiem par to, ka viņu personas datu vākšana VIS ietvaros ir obligāta, lai izskatītu viņu pieteikumu, savukārt dalībvalstīm datu subjekti jāinformē arī par tiesībām piekļūt saviem datiem, pieprasīt to labošanu vai dzēšanu, kā arī par procedūrām šo tiesību īstenošanai[878].

- Tiesības piekļūt ar viņiem saistītajiem VIS ierakstītajiem personas datiem[879].

- Tiesības labot kļūdainus datus[880].

- Tiesības dzēst nelikumīgi saglabātus datus[881].

876 Eiropas Savienības Padome (2008), Padomes 2008. gada 23. jūnija Lēmums 2008/633/TI par izraudzīto dalībvalstu iestāžu un Eiropola piekļuvi Vīzu informācijas sistēmai (VIS) konsultāciju nolūkos, lai novērstu, atklātu un izmeklētu teroristu nodarījumus un citus smagus noziedzīgus nodarījumus, OV 2008 L 218.

877 Turpat.

878 VIS regula, 37. pants.

879 Turpat, 38. panta 1. punkts.

880 Turpat, 38. panta 2. punkts.

881 Turpat, 38. panta 2. punkts.

Lai nodrošinātu VIS pārraudzību, tika izveidota VIS *SCG*. To veido EDAU un valstu uzraudzības iestāžu pārstāvji, kuri tiekas divreiz gadā. Šajā grupā ir ES 28 dalībvalstu, kā arī Islandes, Lihtenšteinas, Norvēģijas un Šveices pārstāvji.

Eurodac

Eurodac apzīmē Eiropas daktiloskopiju[882]. Tā ir centralizēta sistēma, kas satur pirkstu nospiedumu datus par trešo valstu valstspiederīgajiem un bezvalstniekiem, kuri lūdz patvērumu kādā no ES dalībvalstīm[883]. Sistēma darbojas kopš 2003. gada janvāra pēc Padomes Regulas (EK) Nr. 2725/2000 pieņemšanas. Pārstrādāto versiju sāka piemērot 2015. gadā. Tās mērķis galvenokārt ir palīdzēt noteikt, kurai dalībvalstij jābūt atbildīgai par konkrēta patvēruma pieteikuma izskatīšanu saskaņā ar Regulu (EK) Nr. 604/2013. Šajā regulā paredzēti kritēriji un mehānismi, lai noteiktu dalībvalsti, kura ir atbildīga par trešās valsts valstspiederīgā vai bezvalstnieka starptautiskās aizsardzības pieteikuma izskatīšanu, kas iesniegts kādā no dalībvalstīm (Dublinas III regula)[884]. Personas dati *Eurodac* galvenokārt kalpo tam, lai atvieglotu Dublinas III regulas piemērošanu[885].

Valstu tiesībaizsardzības iestādēm un Eiropolam ir atļauts salīdzināt ar kriminālizmeklēšanu saistītos pirkstu nospiedumus ar pirkstu nospiedumiem, kurus satur *Eurodac*, bet tikai nolūkā novērst, atklāt vai izmeklēt teroristu vai citus smagus noziedzīgus nodarījumus. Tā kā *Eurodac* ir paredzēts kā instruments ES patvēruma politikas īstenošanas atbalstam, nevis kā tiesībaizsardzības rīks, tiesībaizsardzības iestādēm ir piekļuve datubāzei tikai noteiktos gadījumos, noteiktos apstākļos, stingri

882 Skatīt Eiropas Datu aizsardzības uzraudzītāja *tīmekļa vietni par Eurodac*.

883 Padomes 2000. gada 11. decembra Regula (EK) Nr. 2725/2000 par pirkstu nospiedumu salīdzināšanas sistēmas *Eurodac* izveidi, lai efektīvi piemērotu Dublinas Konvenciju, OV 2000 L 316; Padomes 2002. gada 28. februāra Regula (EK) Nr. 407/2002, ar ko paredz dažus īstenošanas noteikumus Regulai (EK) Nr. 2725/2000 par pirkstu nospiedumu salīdzināšanas sistēmas *Eurodac* izveidi, lai efektīvi piemērotu Dublinas Konvenciju, OV 2002 L 62 (*Eurodac* regulas), Eiropas Parlamenta un Padomes 2013. gada 26. jūnija Regula (ES) Nr. 603/2013 par pirkstu nospiedumu salīdzināšanas sistēmas *Eurodac* izveidi, lai efektīvi piemērotu Regulu (ES) Nr. 604/2013, ar ko paredz kritērijus un mehānismus, lai noteiktu dalībvalsti, kura ir atbildīga par trešās valsts valstspiederīgā vai bezvalstnieka starptautiskās aizsardzības pieteikuma izskatīšanu, kas iesniegts kādā no dalībvalstīm, un par dalībvalstu tiesībaizsardzības iestāžu un Eiropola pieprasījumiem veikt salīdzināšanu ar *Eurodac* datiem tiesībaizsardzības nolūkos, un ar kuru groza Regulu (ES) Nr. 1077/2011, ar ko izveido Eiropas Aģentūru lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā, OV 2013 L 180, 1. lpp. (*Eurodac* pārstrādātā regula).

884 Eiropas Parlamenta un Padomes 2013. gada 26. jūnija Regula (ES) Nr. 604/2013, ar ko paredz kritērijus un mehānismus, lai noteiktu dalībvalsti, kura ir atbildīga par trešās valsts valstspiederīgā vai bezvalstnieka starptautiskās aizsardzības pieteikuma izskatīšanu, kas iesniegts kādā no dalībvalstīm, OV 2013 L 180 (Dublinas III regula).

885 *Eurodac* pārstrādātā regula, OV 2013 L 180, 1. lpp., 1. panta 1. punkts.

ievērojot nosacījumus[886]. Turpmākai datu izmantošanai tiesībaizsardzības nolūkos tiek piemērota Datu aizsardzības direktīva policijas un krimināltiesību jomā, turpretī datus, ko galvenokārt izmanto Dublinas III regulas piemērošanas atvieglošanai, aizsargā Vispārīgā datu aizsardzības regula. Personas datu, ko saskaņā ar *Eurodac* pārstrādāto regulu ieguvusi dalībvalsts vai Eiropols, tālāka nosūtīšana jebkurai trešai valstij, starptautiskai organizācijai vai privātai organizācijai, kas reģistrēta ES vai ārpus tās, ir aizliegta[887].

Eurodac sastāv no *eu-LISA* pārvaldītas centrālās vienības pirkstu nospiedumu glabāšanai un salīdzināšanai, kā arī sistēmas elektroniskai datu pārsūtīšanai starp dalībvalstīm un centrālo datubāzi. Dalībvalstis noņem un pārsūta ikvienas vismaz 14 gadus vecas personas, kura lūdz patvērumu tās teritorijā, un visu vismaz 14 gadus vecu trešo valstu pilsoņu vai bezvalstnieku, kas aizturēti par neatļautu to ārējās robežas šķērsošanu, pirkstu nospiedumus. Dalībvalstis var arī noņemt un pārsūtīt trešo valstu valstspiederīgo vai bezvalstnieku pirkstu nospiedumus, ja konstatē, ka viņi šo dalībvalstu teritorijā uzturas neatļauti.

Kaut arī ikviena dalībvalsts var ielūkoties *Eurodac* un pieprasīt salīdzinājumus ar pirkstu nospiedumu datiem, tikai dalībvalstij, kas ir savākusi pirkstu nospiedumus un nosūtījusi tos centrālajai vienībai, ir tiesības grozīt datus, tos labojot, papildinot vai izdzēšot[888]. *Eu-LISA* reģistrē visu datu apstrādi, lai uzraudzītu datu aizsardzību un nodrošinātu datu drošību[889]. Valstu uzraudzības iestādes palīdz un konsultē datu subjektus par viņu tiesību īstenošanu[890]. Pirkstu nospiedumu datu vākšanu un pārsūtīšanu var pārskatīt valstu tiesas[891]. ES iestāžu datu aizsardzības regula[892] un EDAU uzraudzība attiecas uz apstrādes darbībām centrālajā sistēmā, kuru pārvalda *eu-LISA* attiecībā uz *Eurodac*[893]. Ja kādai personai ir nodarīts kaitējums nelikumīgas apstrādes darbības vai kādas darbības, kas nav saderīga ar *Eurodac* regulu, šai personai ir tiesības uz kompensāciju no dalībvalsts, kas ir atbildīga par kaitējumu[894]. Tomēr jāuz-

886 Turpat, 1. panta 2. punkts.

887 Turpat, 35. pants.

888 Turpat, 27. pants.

889 Turpat, 28. pants.

890 Turpat, 29. pants.

891 Turpat, 29. pants.

892 Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti, OV 2001 L 8.

893 *Eurodac* pārstrādātā regula, OV 2013 L 180, 1. lpp., 31. pants.

894 Turpat, 37. pants.

sver, ka patvēruma meklētāji ir īpaši neaizsargāta cilvēku grupa, kas nereti devušies ilgā un riskantā ceļā. Viņu neaizsargātības un nedrošās situācijas dēļ, kādā viņi bieži atrodas, kamēr tiek izskatīts patvēruma pieteikums, praksē var izrādīties sarežģīti īstenot viņu tiesības, tostarp tiesības uz kompensāciju.

Lai *Eurodac* izmantotu tiesībaizsardzības nolūkos, dalībvalstīm ir jānozīmē iestādes, kurām būs tiesības pieprasīt piekļuvi, kā arī iestādes, kas pārbaudīs salīdzināšanas pieprasījumu likumību[895]. Valstu iestāžu un Eiropola piekļuvei *Eurodac* pirkstu nospiedumu datiem piemēro ļoti stingrus nosacījumus. Pieprasītājai iestādei jāiesniedz pamatots elektronisks pieprasījums tikai pēc datu salīdzināšanas citās pieejamās informācijas sistēmās, piemēram, valstu pirkstu nospiedumu datubāzēs un VIS, ietvertajiem datiem. Lai salīdzinājumu atzītu par samērīgu, jābūt sevišķi svarīgiem sabiedriskās drošības jautājumiem. Salīdzinājumam ir jābūt patiesi nepieciešamam, tam jābūt saistītam ar konkrētu lietu, un ir jābūt pamatotam iemeslam uzskatīt, ka salīdzinājums ievērojami veicinās attiecīgā noziedzīgā nodarījuma novēršanu, atklāšanu vai izmeklēšanu, jo īpaši, ja ir pamatotas aizdomas, ka par teroristu nodarījuma vai cita smaga noziedzīga nodarījuma izdarīšanu aizdomās turētais, vainīgais vai cietušais ietilpst kategorijā, uz kuru attiecas pirkstu nospiedumu vākšana *Eurodac* sistēmā. Salīdzinājums jāveic tikai, izmantojot pirkstu nospiedumu datus. Eiropolam arī jāsaņem atļauja no tās dalībvalsts, kura vākusi pirkstu nospiedumu datus.

Eurodac glabātie personas dati, kas attiecas uz patvēruma meklētājiem, tiek saglabāti 10 gadus no datuma, kad noņemti pirkstu nospiedumi, izņemot gadījumus, kad datu subjekts saņem ES dalībvalsts pilsonību. Šajā gadījumā dati ir nekavējoties jādzēš. Dati par ārvalstu pilsoņiem, kuri aizturēti par ārējās robežas neatļautu šķērsošanu, tiek saglabāti 18 mēnešus. Šie dati nekavējoties jādzēš, ja datu subjekts saņem uzturēšanās atļauju, atstāj ES teritoriju vai iegūst kādas dalībvalsts pilsonību. To personu dati, kurām piešķirts patvērums, trīs gadu periodā pieejami salīdzināšanai saistībā ar teroristu un citu smagu noziedzīgu nodarījumu novēršanu, atklāšanu un izmeklēšanu.

Papildus visām ES dalībvalstīm, Islande, Norvēģija, Lihtenšteina un Šveice arī piemēro *Eurodac*, pamatojoties uz starptautiskiem nolīgumiem.

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. sēj., Nr. 2, 108.–129. lpp.

Eurodac SCG ir izveidota, lai nodrošinātu *Eurodac* uzraudzību. Tajā ir EDAU un valstu uzraudzības iestāžu pārstāvji, kuri tiekas divreiz gadā. Šajā grupā ir ES 28 dalībvalstu, kā arī Islandes, Lihtenšteinas, Norvēģijas un Šveices pārstāvji[896].

Perspektīva

Lai uzlabotu kopējās Eiropas patvēruma sistēmas (KEPS) darbību, Komisija 2016. gada maijā iesniedza reformu priekšlikumu jaunai pārstrādātai *Eurodac* regulai[897]. Ierosinātā pārstrādāšana ir svarīga, jo ievērojami paplašinās sākotnējās *Eurodac* datubāzes darbības jomu. Sākotnēji *Eurodac* tika izveidota, lai atbalstītu KEPS ieviešanu, nodrošinot pirkstu nospiedumu pierādījumus un ļaujot noteikt, kura dalībvalsts ir atbildīga par ES iesniegtā patvēruma pieteikuma izskatīšanu. Ierosinātā pārstrādāšana paplašinās datubāzes darbības jomu, lai atvieglotu nelegālo migrantu atgriešanu[898]. Valstu iestādes varēs izmantot datubāzi, lai identificētu trešo valstu valstspiederīgos, kuri ES uzturas nelikumīgi vai kuri ieceļojuši ES nelikumīgi, iegūstot pierādījumus, kas palīdzētu dalībvalstīm atgriezt šīs personas. Turklāt, lai arī pašreiz spēkā esošajā tiesiskajā regulējumā ir paredzēta tikai pirkstu nospiedumu vākšana un glabāšana, ar priekšlikumu tiek ieviesta personu sejas attēlu vākšana[899], kas ir vēl viens biometrisko datu veids. Priekšlikums arī pazemināt bērnu minimālo vecumu, no kura var ņemt biometriskos datus, līdz sešiem gadiem[900], nevis 14 gadiem, kas ir minimālais vecums saskaņā ar 2013. gada regulu. Priekšlikuma paplašinātā darbības joma nozīmē iejaukšanos vairāk privātpersonu, kuras var tikt iekļautas datubāzē, tiesībās uz privātumu un datu aizsardzību. Lai līdzsvarotu šo iejaukšanos, priekšlikuma un Eiropas Parlamenta Pilsoņu brīvību, tieslietu un iekšlietu komiteja

896 Skatīt Eiropas Datu aizsardzības uzraudzītāja tīmekļa vietni par *Eurodac*.

897 Eiropas Komisija, Priekšlikums Eiropas Parlamenta un Padomes regulai par pirkstu nospiedumu salīdzināšanas sistēmas *Eurodac* izveidi, lai efektīvi piemērotu [Regulu (ES) Nr. 604/2013, ar ko paredz kritērijus un mehānismus, lai noteiktu dalībvalsti, kura ir atbildīga par trešās valsts valstspiederīgā vai bezvalstnieka starptautiskās aizsardzības pieteikuma izskatīšanu, kas iesniegts kādā no dalībvalstīm], lai identificētu trešās valsts valstspiederīgo vai bezvalstnieku, kurš uzturas nelikumīgi, un par dalībvalstu tiesībaizsardzības iestāžu un Eiropola pieprasījumiem veikt salīdzināšanu ar *Eurodac* datiem tiesībaizsardzības nolūkos (pārstrādāta redakcija), COM(2016) 272 *final*, 2016. gada 4. maijs.

898 Skatīt priekšlikuma paskaidrojuma rakstu, 3. lpp.

899 Eiropas Komisija, Priekšlikums Eiropas Parlamenta un Padomes regulai par pirkstu nospiedumu salīdzināšanas sistēmas *Eurodac* izveidi, lai efektīvi piemērotu [Regulu (ES) Nr. 604/2013, ar ko paredz kritērijus un mehānismus, lai noteiktu dalībvalsti, kura ir atbildīga par trešās valsts valstspiederīgā vai bezvalstnieka starptautiskās aizsardzības pieteikuma izskatīšanu, kas iesniegts kādā no dalībvalstīm], lai identificētu trešās valsts valstspiederīgo vai bezvalstnieku, kurš uzturas nelikumīgi, un par dalībvalstu tiesībaizsardzības iestāžu un Eiropola pieprasījumiem veikt salīdzināšanu ar *Eurodac* datiem tiesībaizsardzības nolūkos (pārstrādāta redakcija), COM(2016) 272 *final*, 2016. gada 4. maijs, 2. panta 1. punkts.

900 Turpat, 2. panta 2. punkts.

komitejas[901] ierosināto grozījumu mērķis ir pastiprināt datu aizsardzības prasības. Rokasgrāmatas izstrādes laikā Parlamentā un Padomē joprojām norisinājās diskusijas par priekšlikumu.

Eurosur

Eiropas Robežu uzraudzības sistēmas (*Eurosur*)[902] mērķis ir uzlabot Šengenas ārējo robežu kontroli, atklājot, novēršot un apkarojot nelegālo imigrāciju un pārrobežu noziedzību. Tā kalpo, lai uzlabotu informācijas apmaiņu un operatīvo sadarbību starp valstu koordinācijas centriem un *Frontex* – ES aģentūru, kuras pārziņā ir jaunās integrētās robežu pārvaldības koncepcijas izstrāde un piemērošana[903]. Tās vispārīgie mērķi ir šādi:

- samazināt nelikumīgi iebraukušo migrantu skaitu, kuri nepamanīti ieceļo ES;
- samazināt nelegālo migrantu nāves gadījumu skaitu, glābjot vairāk cilvēku dzīvības jūrā;
- palielināt ES iekšējo drošību kopumā, uzlabojot pārrobežu noziedzības novēršanu[904].

Eurosur uzsāka darbību 2013. gada 2. decembrī visās dalībvalstīs ar ārējām robežām, bet pārējās – 2014. gada 1. decembrī. Regula attiecas uz dalībvalstu ārējo sauszemes, jūras un gaisa robežu uzraudzību. *Eurosur* apmainās ar personas datiem un tos

901 Eiropas Parlaments, *Ziņojums par priekšlikumu Eiropas Parlamenta un Padomes regulai par pirkstu nospiedumu salīdzināšanas sistēmas* Eurodac *izveidi, lai efektīvi piemērotu [Regulu (ES) Nr. 604/2013, ar ko paredz kritērijus un mehānismus, lai noteiktu dalībvalsti, kura ir atbildīga par trešās valsts valstspiederīgā vai bezvalstnieka starptautiskās aizsardzības pieteikuma izskatīšanu, kas iesniegts kādā no dalībvalstīm], lai identificētu trešās valsts valstspiederīgo vai bezvalstnieku, kurš uzturas nelikumīgi, un par dalībvalstu tiesībaizsardzības iestāžu un Eiropola pieprasījumiem veikt salīdzināšanu ar* Eurodac *datiem tiesībaizsardzības nolūkos (pārstrādāta redakcija)*, PE 597.620v03-00, 2017. gada 9. jūnijs.

902 Eiropas Parlamenta un Padomes 2013. gada 22. oktobra Regula (ES) Nr. 1052/2013, ar ko izveido Eiropas Robežu uzraudzības sistēmu (*Eurosur*), OV 2013 L 295.

903 Eiropas Parlamenta un Padomes 2016. gada 14. septembra Regula (ES) 2016/1624 par Eiropas Robežu un krasta apsardzi un ar ko groza Eiropas Parlamenta un Padomes Regulu (ES) 2016/399 un ar ko atceļ Eiropas Parlamenta un Padomes Regulu (EK) Nr. 863/2007, Padomes Regulu (EK) Nr. 2007/2004 un Padomes Lēmumu 2005/267/EK, OV L 251.

904 Skatīt arī: Eiropas Komisija (2008), Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai: *Eiropas Robežu uzraudzības sistēmas (*Eurosur*) izveidošanas izpēte*, COM(2008) 68 *final*, Brisele, 2008. gada 13. februāris; Eiropas Komisija (2011), *Ietekmes novērtējums, kas pievienots priekšlikumam Eiropas Parlamenta un Padomes regulai, ar ko izveido Eiropas Robežu uzraudzības sistēmu* (Eurosur), darba dokuments, SEC(2011) 1536 *final*, Brisele, 2011. gada 12. decembris, 18. lpp.

apstrādā ļoti ierobežotā apjomā, jo dalībvalstīm un *Frontex* ir tiesības apmainīties tikai ar kuģu identifikācijas numuriem. *Eurosur* apmainās ar operatīvo informāciju, piemēram, par patruļu atrašanās vietu un incidentu norises vietu, un parasti apmainītajā informācijā nevar iekļaut personas datus[905]. Izņēmuma gadījumos, kad personas datu apmaiņa notiek *Eurosur* ietvaros, regulā paredzēts, ka pilnībā piemēro vispārējo ES datu aizsardzības tiesisko regulējumu[906].

Tādējādi *Eurosur* nodrošina tiesības uz datu aizsardzību, proti, nosakot, ka personas datu apmaiņai jāatbilst kritērijiem un aizsardzības pasākumiem, kas noteikti Datu aizsardzības direktīvā policijas un krimināltiesību jomā un Vispārīgajā datu aizsardzības regulā[907].

Muitas informācijas sistēma

Vēl viena svarīga ES mērogā izveidota informācijas sistēma ir Muitas informācijas sistēma (MIS)[908]. Iekšējā tirgus izveides gaitā tika atceltas visas pārbaudes un formalitātes attiecībā uz preču pārvietošanu ES teritorijā, kas izraisīja paaugstinātu krāpšanas risku. Šo risku atsvēra intensīvāka sadarbība starp dalībvalstu muitas administrācijām. MIS mērķis ir palīdzēt dalībvalstīm novērst, izmeklēt un saukt pie atbildības par nopietniem valsts un ES muitas un lauksaimniecības likumu pārkāpumiem. MIS ir izveidota, balstoties uz diviem tiesību aktiem, kas pieņemti uz atšķirīgiem juridiskiem pamatiem: Padomes Regula (EK) Nr. 515/97 attiecas uz sadarbību starp dažādām valstu administratīvajām iestādēm krāpšanas apkarošanā muitas savienības un kopējās lauksaimniecības politikas kontekstā, savukārt Padomes Lēmuma 2009/917/TI mērķis ir palīdzēt novērst, izmeklēt un saukt par atbildību par smagiem muitas likumu pārkāpumiem. Tas nozīmē, ka MIS skar ne tikai tiesībaizsardzības jomu.

MIS ietvertajā informācijā ietilpst personas dati, kas saistīti ar mantām, transportlīdzekļiem, uzņēmumiem, personām, aizturētām, atsavinātām vai konfiscētām

905 Eiropas Komisija, EUROSUR: Šengenas ārējo robežu aizsardzība – migrantu dzīvju nosargāšana. Īsumā par EUROSUR, 2013. gada 29. novembris.

906 Regula 1052/2013, 13. apsvērums un 13. pants.

907 Turpat, 13. apsvērums un 13. pants.

908 Eiropas Savienības Padome (1995), Padomes 1995. gada 26. jūlija Akts, ar ko izstrādā Konvenciju par informācijas tehnoloģiju izmantošanu muitas vajadzībām, OV 1995 C 316, ko groza ar Eiropas Savienības Padomes (2009) 1997. gada 13. marta Regulu Nr. 515/97 par dalībvalstu pārvaldes iestāžu savstarpēju palīdzību un šo iestāžu un Komisijas sadarbību, lai nodrošinātu muitas un lauksaimniecības tiesību aktu pareizu piemērošanu, Padomes 2009. gada 30. novembra Lēmums 2009/917/TI par informācijas tehnoloģiju izmantošanu muitas vajadzībām, OV 2009 L 323 (MIS Lēmums).

precēm un skaidru naudu. Apstrādājamo datu kategorijas ir skaidri definētas, un tajās ietilpst attiecīgo personu vārdi, nacionalitāte, dzimums, dzimšanas vieta un datums, iemesls viņu datu iekļaušanai sistēmā, kā arī transportlīdzekļa reģistrācijas numurs[909]. Šo informāciju var izmantot vienīgi novērošanai, ziņošanai vai īpašu pārbaužu veikšanai, vai stratēģiskai vai operatīvai analīzei attiecībā uz personām, par kurām ir aizdomas, ka tās pārkāpj muitas noteikumus.

Piekļuve MIS tiek piešķirta valstu muitas, nodokļu, lauksaimniecības, sabiedrības veselības un policijas iestādēm, kā arī Eiropolam un *Eurojust*.

Personas datu apstrādei ir jāatbilst īpašajiem noteikumiem, kas noteikti Regulā (EK) Nr. 515/97 un Padomes Lēmumā 2009/917/TI, kā arī Vispārīgās datu aizsardzības regulas, ES iestāžu datu aizsardzības regulas, modernizētās Konvencijas Nr. 108 un Policijas ieteikuma noteikumiem. EDAU pārziņā ir MIS atbilstības Regulai (EK) Nr. 45/2001 uzraudzība. Vismaz reizi gadā tas sasauc sanāksmi ar visām valstu datu aizsardzības uzraudzības iestādēm, kuru kompetencē ir ar MIS saistīti uzraudzības jautājumi.

ES informācijas sistēmu sadarbspēja

Migrācijas pārvaldība, integrēta ES ārējo robežu pārvaldība un cīņa pret terorismu un pārrobežu noziedzību rada nopietnas problēmas, kas globalizētajā pasaulē kļūst arvien sarežģītākas. Pēdējos gados ES strādā pie jaunas visaptverošas pieejas drošības aizsargāšanai un uzturēšanai, neapdraudot ES vērtības un pamatbrīvības. Šajos centienos galvenā nozīme ir efektīvai informācijas apmaiņai starp valstu tiesībaizsardzības iestādēm un starp dalībvalstīm un attiecīgajām ES aģentūrām[910]. Pašreizējām ES robežu pārvaldības un iekšējās drošības informācijas sistēmām ir savi attiecīgie mērķi, institucionālā struktūra, datu subjekti un lietotāji. ES strādā pie trūkumu novēršanas sadrumstalotās ES datu pārvaldības funkcionalitātē starp dažādām informācijas sistēmām, piemēram, *SIS II*, VIS un *Eurodac*, pētot sadarbspējas

909 Skatīt MIS lēmuma 24., 25. un 28. pantu.

910 Eiropas Komisija (2016), Komisijas paziņojums Eiropas Parlamentam un Padomei: Spēcīgākas un viedākas robežu un drošības informācijas sistēmas, COM(2016) 205 *final*, Brisele, 2016. gada 6. aprīlis, Eiropas Komisija (2016), Komisijas paziņojums Eiropas Parlamentam, Eiropas Padomei un Padomei: Drošības stiprināšana pasaulē, ko raksturo mobilitāte: informācijas apmaiņas uzlabojumi cīņā pret terorismu un ārējo robežu stiprināšana, COM(2016) 602 *final*, Brisele, 2016. gada 14. septembris, Eiropas Komisija (2016), Priekšlikums Eiropas Parlamenta un Padomes Regulai par Šengenas informācijas sistēmas izmantošanu to trešo valstu valstspiederīgo atgriešanai, kuri dalībvalstīs uzturas nelikumīgi. Skatīt arī Komisijas paziņojumu Eiropas Parlamentam, Eiropadomei, Padomei: Septītais progresa ziņojums virzībā uz efektīvu un patiesu drošības savienību, COM(2017) 261 *final*, Brisele, 2017. gada 16. maijs.

potenciālu[911]. Galvenais mērķis ir nodrošināt, lai kompetentajām policijas, muitas un tiesu iestādēm būtu sistemātiski pieejama informācija, kas nepieciešama to pienākumu izpildei, saglabājot līdzsvaru attiecībā uz tiesībām uz privātumu, datu aizsardzību un citām pamattiesībām.

Sadarbspēja ir "informācijas sistēmu spēja apmainīties ar datiem un nodrošināt informācijas apmaiņu"[912]. Šī apmaiņa nedrīkst apdraudēt nepieciešami stingros piekļuves un lietošanas noteikumus, ko garantē Vispārīgā datu aizsardzības regula, Datu aizsardzības direktīva policijas un krimināltiesību jomā, ES Pamattiesību harta un visi citi attiecīgie noteikumi. Neviens integrēts datu pārvaldības risinājums nedrīkst ietekmēt nolūka ierobežojuma, integrētas datu aizsardzības vai datu aizsardzības pēc noklusējuma principus[913].

Papildus trīs galveno informācijas sistēmu – *SIS II*, VIS un *Eurodac* – funkcionalitātes uzlabošanai Komisija ir ierosinājusi izveidot ceturto centralizēto robežu pārvaldības sistēmu, kas paredzēta trešo valstu pilsoņiem: ieceļošanas/izceļošanas sistēmu (IIS)[914], kuru paredzēts ieviest līdz 2020. gadam[915]. Komisija ir arī sniegusi priekšlikumu par Eiropas ceļošanas informācijas un atļauju sistēmas (*ETIAS*) izveidi[916]. Šajā sistēmā tiks apkopota informācija par personām, kuras ieceļo ES bez vīzām, lai varētu veikt iepriekšējas nelikumīgas migrācijas un drošības pārbaudes.

911 Eiropas Savienības Padome (2005), Hāgas programma brīvības, drošības un tiesiskuma stiprināšanai Eiropas Savienībā, OV 2005 C 53, Eiropas Komisija (2010), Komisijas paziņojums Eiropas Parlamentam un Padomei: Pārskats par informācijas pārvaldību brīvības, drošības un tiesiskuma jomā, COM(2010) 385 *final*, Eiropas Komisija (2016), Komisijas paziņojums Eiropas Parlamentam un Padomei: Spēcīgākas un viedākas robežu un drošības informācijas sistēmas, COM(2016) 205 *final*, Brisele, 2016. gada 6. aprīlis, Eiropas Komisija (2016), Komisijas 2016. gada 17. jūnija Lēmums, ar ko izveido augsta līmeņa ekspertu grupu informācijas sistēmu un sadarbspējas jautājumos, OV 2016 C 257.

912 Eiropas Komisija (2016), Komisijas paziņojums Eiropas Parlamentam un Padomei: Spēcīgākas un viedākas robežu un drošības informācijas sistēmas, COM(2016) 205 *final*, Brisele, 2016. gada 6. aprīlis, 14. lpp.

913 Turpat, 4.–5. lpp.

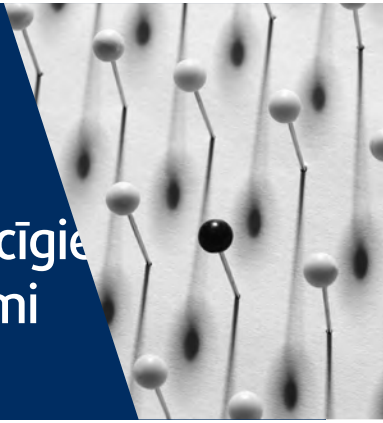
914 Eiropas Komisija (2016), Priekšlikums Eiropas Parlamenta un Padomes regulai, ar ko izveido ieceļošanas/izceļošanas sistēmu (IIS), lai reģistrētu to trešo valstu valstspiederīgo ieceļošanas un izceļošanas datus un ieceļošanas atteikumus, kuri šķērso Eiropas Savienības dalībvalstu ārējās robežas, un ar ko paredz nosacījumus piekļuvei IIS tiesībaizsardzības nolūkos un groza Regulu (EK) Nr. 767/2008 un Regulu (ES) Nr. 1077/2011, COM(2016) 194 *final*, Brisele, 2016. gada 6. aprīlis.

915 Eiropas Komisija (2016), Komisijas paziņojums Eiropas Parlamentam un Padomei: Spēcīgākas un viedākas robežu un drošības informācijas sistēmas, COM(2016) 205 *final*, Brisele, 2016. gada 6. aprīlis, 5. lpp.

916 Eiropas Komisija (2016), Priekšlikums Eiropas Parlamenta un Padomes Regulai, ar ko izveido Eiropas Ceļošanas informācijas un atļauju sistēmu (*ETIAS*) un groza Regulas (ES) Nr. 515/2014, (ES) 2016/399, (ES) 2016/794 un (ES) 2016/1624, COM(2016) 731 *final*, 2016. gada 16. novembris.

9

Īpaši datu veidi un to attiecīgie datu aizsardzības noteikumi



ES	Aptvertie jautājumi	EP
Vispārīgā datu aizsardzības regula Direktīva par privāto dzīvi un elektronisko komunikāciju	**Elektroniskā komunikācija**	Modernizētā Konvencija Nr. 108 Telekomunikāciju pakalpojumu ieteikums
Vispārīgā datu aizsardzības regula, 88. pants	**Nodarbinātības attiecības**	Modernizētā Konvencija Nr. 108 Nodarbinātības politikas ieteikums ECT lieta *Copland pret Apvienoto Karalisti*, Nr. 62617/00, 2007
Vispārīgā datu aizsardzības regula, 9. panta 2. punkta h) un i) apakšpunkts.	**Medicīniskie dati**	Modernizētā Konvencija Nr. 108 Medicīnisko datu ieteikums ECT lieta *Z. pret Somiju*, Nr. 22009/93, 1997
Klīnisko izmēģinājumu regula	**Klīniskie izmēģinājumi**	
Vispārīgā datu aizsardzības regula, 6. panta 4. punkts un 89. pants	**Statistika**	Modernizētā Konvencija Nr. 108 Statistikas datu ieteikums
Regula (EK) Nr. 223/2009 par Eiropas statistiku EST lieta C-524/06 *Huber pret Vācijas Federatīvo Republiku* [GC], 2008	**Oficiālie statistikas dati**	Modernizētā Konvencija Nr. 108 Statistikas datu ieteikums

ES	Aptvertie jautājumi	EP
Direktīva 2014/65/ES par finanšu instrumentu tirgiem Regula (ES) Nr. 648/2012 par ārpusbiržas atvasinātajiem instrumentiem, centrālajiem darījumu un darījumu reģistriem Regula (EK) Nr. 1060/2009 par kredītreitingu aģentūrām Direktīva 2007/64/EK par maksājumu pakalpojumiem iekšējā tirgū	**Finanšu dati**	Modernizētā Konvencija Nr. 108 Ieteikums 90(19), ko izmanto maksājumiem un citām saistītām darbībām ECT lieta *Michaud pret Franciju*, Nr. 12323/11, 2012

Vairākos gadījumos Eiropas mērogā ir pieņemti īpaši tiesību instrumenti, lai detalizētāk piemērotu modernizētās Konvencijas Nr. 108 vai Vispārīgās datu aizsardzības regulas īpašos noteikumus konkrētām situācijām.

9.1. Elektroniskā komunikācija

Svarīgākie aspekti

- Īpašie noteikumi par datu aizsardzību telekomunikāciju jomā, īpaši atsaucoties uz telefona pakalpojumiem, ir ietverti Eiropas Padomes 1995. gada ieteikumā.
- Personas datu apstrāde saistībā ar komunikāciju pakalpojumu piegādi ES mērogā ir reglamentēta Direktīvā par privāto dzīvi un elektronisko komunikāciju.
- Elektroniskās komunikācijas konfidencialitāte attiecas ne tikai uz komunikācijas saturu, bet arī uz metadatiem, piemēram, informāciju par to, kas ar ko ir sazinājies, kad un cik ilgi, kā arī atrašanās vietas datiem, piemēram, no kurienes dati nosūtīti.

Komunikāciju tīkliem ir paaugstināts nepamatotas iejaukšanās potenciāls lietotāju personīgajā sfērā, jo tie nodrošina jaudīgas tehniskās iespējas noklausīties un pārraudzīt komunikāciju, kas tiek veikta šādos tīklos. Līdz ar to uzskatīja, ka nepieciešams ieviest īpašus datu aizsardzības noteikumus, lai novērstu konkrētus riskus komunikāciju pakalpojumu lietotājiem.

EP 1995. gadā izdeva ieteikumu datu aizsardzībai telekomunikāciju jomā, īpaši attiecībā uz telefona pakalpojumiem[917]. Saskaņā ar šo ieteikumu personas datu vākšanas un apstrādes nolūkiem telekomunikāciju kontekstā vajadzētu skart tikai lietotāja pieslēgšanu tīklam, konkrētā telekomunikāciju pakalpojuma pieejamības nodrošināšanu, rēķinu sagatavošanu, verificēšanu, optimālas tehniskās darbības nodrošināšanu, kā arī tīkla attīstību un apkalpošanu.

Īpaša uzmanība tika pievērsta arī komunikāciju tīklu izmantošanai tiešās tirgvedības ziņojumu sūtīšanai. Parasti tiešās tirgvedības ziņojumus nedrīkst adresēt abonentiem, kuri ir nepārprotami atteikušies tos saņemt. Automātiskas zvana ierīces iepriekš ierakstītu reklāmas ziņojumu pārraidīšanai var tikt izmantotas tikai tad, ja abonents ir devis nepārprotamu piekrišanu. Valsts tiesību aktos jāparedz detalizēti izstrādāti noteikumi šajā jomā.

Pēc pirmā mēģinājuma 1997. gadā **ES tiesiskajā regulējumā** 2002. gadā tika pieņemta Direktīva par privāto dzīvi un elektronisko komunikāciju un grozīta 2009. gadā. Tas tika darīts, lai papildinātu un pielāgotu iepriekšējās Datu aizsardzības direktīvas noteikumus telekomunikāciju nozarei[918].

Direktīvu par privāto dzīvi un elektronisko komunikāciju piemēro tikai komunikāciju pakalpojumiem publiskajos elektroniskajos tīklos.

Direktīvā par privāto dzīvi un elektronisko komunikāciju ir izdalītas trīs galvenās datu kategorijas, kas rodas komunikācijas laikā:

- dati, kas veido komunikācijas laikā nosūtīto ziņojumu saturu – šie dati ir stingri konfidenciāli;

917 Eiropas Padomes Ministru komiteja (1995), Ieteikums Nr. Rec(95)4 dalībvalstīm par personas datu aizsardzību telekomunikāciju jomā, ar īpašu atsauci uz telefona pakalpojumiem, 1995. gada 7. februāris.

918 Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē, OV 2002 L 201 (Direktīva par privāto dzīvi un elektronisko komunikāciju), kuru groza ar 2009. gada 25. novembra Direktīvu 2009/136/EK par universālo pakalpojumu un lietotāju tiesībām attiecībā uz elektronisko sakaru tīkliem un pakalpojumiem, ar ko groza Direktīvu 2002/22/EK par universālo pakalpojumu un lietotāju tiesībām attiecībā uz elektronisko sakaru tīkliem un pakalpojumiem, Direktīvu 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē un Regulu (EK) Nr. 2006/2004 par sadarbību starp valstu iestādēm, kas atbildīgas par tiesību aktu īstenošanu patērētāju tiesību aizsardzības jomā, OV 2009 L 337.

- komunikācijas izveidošanai un uzturēšanai nepieciešamie dati – tā sauktie metadati, ko direktīvā dēvē par "informāciju par datu plūsmu", piemēram, informācija par komunikācijas pusēm, komunikācijas laiku un ilgumu;

- metadatos ir dati, kas īpaši attiecas uz sakaru ierīces atrašanās vietu, tā sauktie atrašanās vietas dati – šie dati vienlaikus ir arī dati par sakaru ierīču lietotāju atrašanās vietu, jo īpaši gadījumos, ja skarti mobilo sakaru ierīču lietotāji.

Informāciju par datu plūsmu pakalpojumu sniedzējs var izmantot tikai norēķiniem un pakalpojuma tehniskai nodrošināšanai. Ar datu subjekta piekrišanu šos datus tomēr var izpaust citiem pārziņiem, kuri piedāvā pakalpojumus ar pievienoto vērtību, piemēram, sniedz informāciju par tuvāko metro staciju vai aptieku attiecībā pret lietotāja atrašanās vietu vai laika prognozi šai atrašanās vietai.

Saskaņā ar E-privātuma direktīvas 15. pantu citai piekļuvei datiem par komunikāciju elektroniskajos tīklos ir jāatbilst prasībām par pamatotu iejaukšanos datu aizsardzības tiesībās, kas noteiktas ECTK 8. panta 2. punktā un apstiprinātas ES Pamattiesību hartas 8. un 52. pantā. Šāda pieeja var ietvert piekļuvi noziegumu izmeklēšanai.

Ar 2009. gada grozījumiem Direktīvā par privāto dzīvi un elektronisko komunikāciju[919] ieviesa:

- E-pasta sūtīšanas ierobežojumi tiešas tirgvedības nolūkos tika attiecināti arī uz īsziņu pakalpojumiem, multivides ziņojumapmaiņas pakalpojumiem un citiem līdzīgu lietotņu veidiem; tirgvedības e-pasti ir aizliegti, ja nav saņemta iepriekšēja piekrišana. Bez šādas piekrišanas tirgvedības e-pastus var sūtīt tikai iepriekšējiem klientiem, ja viņi ir uzrādījuši savu e-pasta adresi un neiebilst pret šādu komunikāciju.

- Dalībvalstīm tika noteikts pienākums nodrošināt tiesiskās aizsardzības līdzekļus pret nevēlamas komunikācijas aizlieguma pārkāpumiem[920].

919 Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīva 2009/136/EK, ar ko groza Direktīvu 2002/22/EK par universālo pakalpojumu un lietotāju tiesībām attiecībā uz elektronisko sakaru tīkliem un pakalpojumiem, Direktīvu 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē un Regulu (EK) Nr. 2006/2004 par sadarbību starp valstu iestādēm, kas atbildīgas par tiesību aktu īstenošanu patērētāju tiesību aizsardzības jomā, OV 2009 L 337.

920 Skatīt grozīto direktīvu, 13. pants.

- Sīkdatņu, programmatūru, ar ko uzrauga un reģistrē datora lietotāja darbības, iestatīšana vairs nav atļauta bez datora lietotāja piekrišanas. Valstu likumos ir jānosaka detalizētāks regulējums, kā izteikt un saņemt piekrišanu, lai nodrošinātu pietiekamu aizsardzību[921].

Ja datu pārkāpums notiek neatļautas piekļuves, datu nozaudēšanas vai iznīcināšanas rezultātā, par to nekavējoties jāinformē kompetentā uzraudzības iestāde. Abonenti jāinformē, ja datu pārkāpuma rezultātā tiem var tikt nodarīts kaitējums[922].

Datu saglabāšanas direktīvā[923] komunikāciju pakalpojumu sniedzējiem ir noteikts pienākums saglabāt metadatus. Taču EST šo direktīvu pasludināja par spēkā neesošu (plašāka informācija 8.3. iedaļā).

Perspektīva

Eiropas Komisija 2017. gada janvārī pieņēma jaunu priekšlikumu e-privātuma regulai, ar ko aizstāt veco E-privātuma direktīvu. Mērķis joprojām būtu nodrošināt "fizisku un juridisku personu pamattiesību un pamatbrīvību aizsardzību elektronisko sakaru pakalpojumu sniegšanā un izmantošanā, un īpaši par tiesībām uz privātās dzīves un sakaru neaizskaramību un par fizisku personu aizsardzību saistībā ar personas datu apstrādi". Tajā pašā laikā jaunais priekšlikuma mērķis ir nodrošināt elektronisko komunikāciju datu un elektronisko komunikāciju pakalpojumu brīvu apriti Savienībā[924]. Kaut arī Vispārīgā datu aizsardzības regula galvenokārt attiecas uz ES Pamattiesību hartas 8. pantu, ierosinātās regulas mērķis ir iestrādāt Hartas 7. pantu ES sekundārajos tiesību aktos.

Regulā iepriekšējās direktīvas noteikumi tiktu pielāgoti jaunajām tehnoloģijām un tirgus realitātei, un tā izveidotu visaptverošu un konsekventu regulējumu ar

921 Skatīt turpat, 5. pants; skatīt arī 29. panta darba grupas (2012) *Atzinumu 04/2012 par sīkdatņu atbrīvošanu no prasības par piekrišanu*, WP 194, Brisele, 2012. gada 7. jūnijs.

922 Skatīt arī 29. panta darba grupas (2011) *Darba dokumentu 01/2011 par pašreizējo ES personas datu pārkāpumu regulējumu un ieteikumiem turpmākai politikas attīstībai*, WP 184, Brisele, 2011. gada 5. aprīlis.

923 Eiropas Parlamenta un Padomes 2006. gada 15. marta Direktīva 2006/24/EK par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK, OV 2006 L 105.

924 Priekšlikums Eiropas Parlamenta un Padomes regulai par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko komunikāciju nozarē un ar ko atceļ Direktīvu 2002/58/EK (Regula par privāto dzīvi un elektronisko komunikāciju), COM(2017) 10 *final*, 1. pants.

Vispārīgo datu aizsardzības regulu. Šajā ziņā E-privātuma regula būtu *lex specialis* Vispārīgajai datu aizsardzības regulai, to pielāgojot elektronisko komunikāciju datiem, kas sastāda personas datus. Jaunā regula attiecas uz "elektronisko komunikāciju datu", tostarp elektroniskās komunikācijas satura un metadatu, kas ne vienmēr ir personas dati, apstrādi. Teritoriālā piemērošanas joma ir tikai ES teritorija, ietverot gadījumus, kad ES iegūtie dati tiek apstrādāti ārpus tās, un to piemēro augstākā līmeņa komunikāciju pakalpojumu sniedzējiem. Tie ir pakalpojumu sniedzēji, kas izplata saturu, pakalpojumus vai lietotnes internetā, bez tieša tīkla operatora vai interneta pakalpojumu sniedzēja (IPS) līdzdalības. Šādu pakalpojumu sniedzēju piemēri ir *Skype* (balss un videozvani), *WhatsApp* (ziņojumapmaiņa), *Google* (meklēšana), *Spotify* (mūzika) un *Netflix* (video saturs). Uz jauno regulu attieksies Vispārīgās datu aizsardzības regulas izpildes mehānismi.

E-privātuma regulu paredzēts pieņemt līdz 2018. gada 25. maijam, un līdz tam brīdim Vispārīgā datu aizsardzības regula būs piemērojama visās 28 dalībvalstīs. Tomēr tam nepieciešama Eiropas Parlamenta un Padomes piekrišana[925].

9.2. Nodarbinātības dati

Svarīgākie aspekti

- Īpaši datu aizsardzības noteikumi, kas piemērojami darba attiecībās, izklāstīti Eiropas Padomes Ieteikumā par nodarbinātības datiem.
- Vispārīgajā datu aizsardzības regulā nodarbinātības attiecības īpaši norādītas tikai sensitīvu datu apstrādes kontekstā.
- Piekrišanas, kas bija jāsniedz labprātīgi, spēkā esamība kā juridiskais pamats, apstrādājot datus par darbiniekiem, var būt apšaubāma, ņemot vērā ekonomisko nelīdzsvarotību starp darba devēju un darbiniekiem. Rūpīgi jāizvērtē ar piekrišanas sniegšanu saistītie apstākļi.

925 Vairāk informācijas Eiropas Komisija (2017), "Komisija ierosina visaptverošus privātuma noteikumus attiecībā uz visiem elektroniskajiem sakariem un atjaunina datu aizsardzības noteikumus ES iestādēm", paziņojums presei, 2017. gada 10. janvāris.

Uz datu apstrādi nodarbinātības jomā attiecas vispārējie ES tiesību akti par personas datu aizsardzību. Tomēr viena regula[926] īpaši skar personas datu apstrādes aizsardzību Eiropas iestādēs nodarbinātības kontekstā (cita starpā). Vispārīgajā datu aizsardzības regulā nodarbinātības attiecības ir īpaši norādītas 9. panta 2. punktā, kurā noteikts, ka personas datus var apstrādāt, lai realizētu pārziņa vai datu subjekta pienākumus un īstenotu konkrētas viņu tiesības nodarbinātības jomā.

Saskaņā ar Vispārīgo datu aizsardzības regulu darbiniekam jābūt iespējai skaidri nodalīt datus, kuru apstrādei/saglabāšanai viņš vai viņa labprātīgi piekrīt, un nolūkus, kādiem viņa vai viņas dati tiek glabāti. Pirms piekrišanas saņemšanas darbinieki ir jāinformē arī par viņu tiesībām un datu glabāšanas ilgumu. Ja notiek personas datu pārkāpumi, kas var radīt lielu risku fizisko personu tiesībām un brīvībām, darba devējam par šo pārkāpumu jāinformē darbinieks. Regulas 88. pants ļauj dalībvalstīm paredzēt detalizētāk izstrādātus noteikumus, lai nodrošinātu darbinieku tiesību un brīvību aizsardzību attiecībā uz viņu personas datiem nodarbinātības kontekstā.

Piemērs. Lietā *Worten*[927] datos ietilpa darba laika uzskaite, kurā ietverti ikdienas darba un atpūtas laiki, kas ir personas dati. Valsts tiesību aktos var būt prasība darba devējam darīt darba laika uzskaiti pieejamu tām valsts iestādēm, kuras ir atbildīgas par darba nosacījumu uzraudzību. Tas ļautu nekavējoties piekļūt attiecīgajiem personas datiem. Tomēr piekļuve personas datiem ir nepieciešama, lai valsts iestāde varētu uzraudzīt tiesību aktus par darba nosacījumu ievērošanu[928].

Kas attiecas uz **EP**, Ieteikums par nodarbinātības datiem tika izdots 1989. gadā un pārskatīts 2015. gadā[929]. Ieteikums skar personas datu apstrādi nodarbinātības nolūkos gan privātajā, gan publiskajā sektorā. Apstrādē ir jāievēro noteikti principi un ierobežojumi, piemēram, pārredzamības princips un apspriešanās ar darbinieku pārstāvjiem pirms uzraudzības sistēmu izveides darba vietā. Ieteikumā arī norādīts, ka

926 Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti, OV 2001 L 8.

927 EST 2013. gada 30. maija spriedums lietā C-342/12, *Worten – Equipamentos para o Lar SA pret Autoridade para as Condições de Trabalho (ACT)*, 19. punkts.

928 Turpat, 43. punkts.

929 Eiropas Padome, Ministru komiteja (2015), Ieteikums Nr. Rec(2015)5 dalībvalstīm, kas regulē personas datu izmantošanu nodarbinātības kontekstā, 2015. gada aprīlis.

darba devējiem ir jāievieš preventīvi pasākumi, piemēram, filtri, tā vietā, lai uzraudzītu darbinieku interneta lietojumu.

Pārskats par visbiežāk sastopamajām datu aizsardzības problēmām, kas raksturīgas nodarbinātības jomai, sniegts 29. panta darba grupas darba dokumentā[930]. Darba grupa analizēja piekrišanas kā juridiskā pamata nodarbinātības datu apstrādei nozīmi[931]. Tā konstatēja, ka ekonomiskā nelīdzsvarotība starp darba devēju, kurš lūdz piekrišanu, un darbinieku, kurš sniedz piekrišanu, bieži rada šaubas, vai piekrišana tika sniegta labprātīgi. Tādēļ, novērtējot piekrišanas spēkā esamību nodarbinātības kontekstā, rūpīgi jāapsver apstākļi, kādos piekrišana tiek izmantota kā datu apstrādes juridiskais pamats.

Bieži sastopama datu aizsardzības problēma mūsdienu tipiskajā darba vidē ir darbinieku elektroniskās komunikācijas likumīgas uzraudzības apjoms darba vietā. Bieži apgalvo, ka šo problēmu var viegli atrisināt, aizliedzot izmantot komunikācijas iespējas privātām vajadzībām darba vietā. Šāds vispārējs aizliegums tomēr varētu būt nesamērīgs un neīstenojams. Šajā sakarībā īpaši interesanti ir ECT spriedumi lietās *Copland pret Apvienoto Karalisti* un Bărbulescu pret Rumāniju.

Piemērs. Lietā *Copland pret Apvienoto Karalisti*[932] tika veikta slepena koledžas darbinieces tālruņa, e-pasta un interneta lietojuma uzraudzība, lai pārliecinātos, vai viņa pārmērīgi neizmanto koledžas iespējas personīgos nolūkos. ECT uzskatīja, ka uz telefona zvaniem, kas veikti uzņēmuma telpās, attiecas privātās dzīves un korespondences jēdzieni. Tādēļ šādus zvanus un e-pastus, kas nosūtīti no darba vietas, kā arī informāciju, kas iegūta, pārraugot personīgo interneta lietojumu, aizsargāja ECTK 8. pants. Prasītājas gadījumā nebija noteikumu, kas regulētu apstākļus, kādos darba devēji var uzraudzīt darbinieku tālruņa, e-pasta un interneta izmantojumu. Tādēļ iejaukšanās neatbilda likumiem. Tiesa secināja, ka ir pārkāpts ECTK 8. pants.

930 29. panta darba grupa (2017), *Atzinums 2/2017 par datu apstrādi darbā*, WP 249, Brisele, 2017. gada 8. jūnijs.

931 29. panta darba grupa (2005), *Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta vienotu interpretāciju*, WP 114, Brisele, 2005. gada 25. novembris.

932 ECT 2007. gada 3. aprīļa spriedums lietā *Copland pret Apvienoto Karalisti*, Nr. 62617/00.

Piemērs. Lietā *Bărbulescu pret Rumāniju*[933] prasītājs tika atlaists par interneta izmantošanu darba vietā un laikā, pārkāpjot iekšējos noteikumus. Prasītāja darba devējs uzraudzīja viņa komunikāciju. Valsts iekšējās tiesvedības gaitā tika iesniegti ieraksti, kas satur tīri privāta rakstura ziņojumus. Konstatējot 8. panta piemērojamību, ECT atstāja atklātu jautājumu, vai darba devēja ierobežojošie noteikumi ļāva prasītājam pamatoti cerēt uz privātuma ievērošanu, taču secināja, ka darba devēja norādījumi nevar samazināt privāto sociālo dzīvi darba vietā līdz nullei.

Faktiski līgumslēdzējām valstīm bija jāpiešķir plaša rīcības brīvība, novērtējot nepieciešamību izveidot tiesisko regulējumu, kas reglamentē apstākļus, kādos darba devējs var regulēt savu darbinieku ar darbu nesaistīto elektronisko vai cita veida komunikāciju darba vietā. Tomēr valsts iestādēm bija pienākums nodrošināt, lai darba devēja ieviestie pasākumi, uzraugot korespondenci un citu komunikāciju, neatkarīgi no šādu pasākumu apjoma un ilguma, tiktu papildināti ar atbilstošiem un pietiekamiem aizsardzības pasākumiem pret ļaunprātīgu izmantošanu. Proporcionalitātei un procesuālajām garantijām, kas aizsargā pret patvaļīgu izmantojumu, bija būtiska nozīme, un ECT identificēja vairākus būtiskus faktorus šajos apstākļos. Šādu faktoru vidū cita starpā bija tas, cik lielā mērā darba devējs uzrauga darbiniekus un kāds ir iejaukšanās līmenis darbinieka privātumā, sekas darbiniekam un tas, vai pastāv atbilstoši drošības pasākumi. Turklāt valsts iestādēm bija jānodrošina, ka darbiniekam, kura saziņa tika uzraudzīta, ir iespēja izmantot tiesiskās aizsardzības līdzekļus tiesā, kas ir kompetenta vismaz pēc būtības noteikt, kā šie izklāstītie kritēriji tika ievēroti un vai apstrīdētie pasākumi bija likumīgi.

Šajā gadījumā ECT konstatēja 8. panta pārkāpumu, jo valsts iestādes nebija nodrošinājušas pienācīgu aizsardzību prasītāja tiesībām uz viņa privātās dzīves un korespondences neaizskaramību un attiecīgi nebija panākušas taisnīgu līdzsvaru starp attiecīgajām interesēm.

Saskaņā ar EP Nodarbinātības politikas ieteikumu personas dati, kas savākti nodarbinātības nolūkos, iegūstami tieši no konkrētā darbinieka.

933 ECT 2017. gada 5. septembra spriedums lietā *Bărbulescu pret Rumāniju* [GC], Nr. 61496/08, 121. punkts.

Personas datos, kas savākti darbā pieņemšanas nolūkos, drīkst ietvert tikai informāciju, kas nepieciešama kandidātu piemērotības un viņu karjeras potenciāla novērtēšanai.

Ieteikumā īpaši minēti arī vērtēšanas dati, kas attiecas uz atsevišķu darbinieku sniegumu vai potenciālu. Vērtēšanas datiem jābūt balstītiem uz taisnīgiem un godīgiem vērtējumiem, un tie nedrīkst būt aizvainojoši formulēti. To pieprasa godprātīgas datu apstrādes un datu precizitātes principi.

Īpašs datu aizsardzības tiesību aspekts darba devēja un darbinieka attiecībās ir darbinieku pārstāvju nozīme. Šādi pārstāvji var saņemt darbinieku personas datus tikai tādā apjomā, ciktāl tas ir nepieciešams, lai viņi varētu pārstāvēt darbinieku intereses, vai ja šie dati ir nepieciešami, lai izpildītu vai uzraudzītu koplīgumos noteiktos pienākumus.

Sensitīvus personas datus, kas savākti nodarbinātības nolūkos, drīkst apstrādāt tikai īpašos gadījumos un saskaņā ar valsts tiesību aktos noteiktajiem aizsardzības pasākumiem. Darba devēji var uzdot jautājumus darbiniekiem vai kandidātiem par viņu veselības stāvokli vai veikt medicīnisko pārbaudi tikai tad, ja tas ir nepieciešams. To varētu darīt, lai noteiktu viņu piemērotību darbam, izpildītu profilaktiskās medicīnas prasības, aizsargātu datu subjekta vai citu darbinieku un personu vitālās intereses, ļautu piešķirt sociālos pabalstus vai atbildētu uz tiesas pieprasījumiem. Veselības datus nedrīkst vākt no citiem avotiem, tikai no konkrētā darbinieka, izņemot gadījumus, kad ir saņemta nepārprotama un apzināta piekrišana, vai valsts tiesību aktos paredzētajos gadījumos.

Saskaņā ar Nodarbinātības politikas ieteikumu darbinieki ir jāinformē par viņu personas datu apstrādes nolūku, savākto personas datu veidu, vienībām, kurām dati tiek regulāri izpausti, kā arī par šādas izpaušanas mērķi un juridisko pamatu. Elektroniskai komunikācijai darba vietā var piekļūt tikai drošības vai citu likumīgu iemeslu dēļ, un šāda pieeja ir atļauta tikai pēc tam, kad darbinieki ir informēti, ka darba devējam var būt piekļuve šāda veida komunikācijai.

Darbiniekiem jābūt tiesībām piekļūt saviem nodarbinātības datiem, kā arī tiesībām tos labot vai dzēst. Ja tiek apstrādāti vērtēšanas dati, darbiniekiem jābūt tiesībām vērtējumu apstrīdēt. Iekšējās izmeklēšanas vajadzībām tomēr var uz laiku ierobežot šīs tiesības. Ja darbiniekam tiek liegta pieeja personas nodarbinātības datiem, iespēja tos labot vai dzēst, valsts tiesību aktos jāparedz piemērotas procedūras šāda atteikuma apstrīdēšanai.

9.3. Veselības dati

Svarīgākais aspekts

- Medicīniskie dati ir sensitīvi personas dati, tāpēc tiem piemēro īpašu aizsardzību.

Personas dati par datu subjekta veselību tiek klasificēti kā sensitīvi dati saskaņā ar Vispārīgās datu aizsardzības regulas 9. panta 1. punktu un modernizētās Konvencijas Nr. 108 6. pantu. Līdz ar to uz datiem, kas saistīti ar veselību, attiecas stingrāks datu apstrādes režīms nekā uz datiem, kas nav sensitīvi. Vispārīgā datu aizsardzības regula aizliedz apstrādāt "veselības datus" (saprotami kā "visi dati par datu subjekta veselības stāvokli, kuri atspoguļo informāciju par datu subjekta kādreizējo, tagadējo vai prognozējamo fiziskās vai garīgās veselības stāvokli")[934], kā arī ģenētiskos datus un biometriskos datus, izņemot gadījumus, kad tas ir atļauts saskaņā ar 9. panta 2. punktu. Abi datu veidi ir pievienoti "īpašo kategoriju personas datu" sarakstam[935].

Piemērs. Lietā *Z pret Somiju*[936] prasītājas bijušais vīrs, kurš bija inficēts ar *HIV*, bija izdarījis vairākus dzimumnoziegumus. Pēc tam viņš tika notiesāts par slepkavību, balstoties uz to, ka viņš apzināti bija pakļāvis savus upurus *HIV* infekcijas riskam. Valsts tiesa noteica pilnam spriedumam un lietas dokumentiem konfidenciālas informācijas statusu uz 10 gadiem, ignorējot prasītājas lūgumus noteikt ilgāku konfidencialitātes periodu. Apelācijas tiesa noraidīja šos lūgumus, un tās spriedumā bija norādīti gan prasītājas, gan viņas bijušā vīra vārdi. ECT uzskatīja, ka iejaukšanās nav uzskatāma par nepieciešamu demokrātiskā sabiedrībā, jo medicīnisko datu aizsardzība ir ārkārtīgi svarīga, lai varētu īstenot tiesības uz privātās un ģimenes dzīves neaizskaramību, jo īpaši, ja runa ir par informāciju par *HIV* infekcijām, ņemot vērā aizspriedumus, kādi daudzās sabiedrībās pastāv attiecībā uz šo stāvokli. Tādēļ Tiesa secināja, ka, ļaujot piekļuvi apelācijas tiesas spriedumam, kurā aprakstīta prasītājas identitāte un veselības stāvoklis, 10 gadus pēc sprieduma pasludināšanas tiktu pārkāpts ECTK 8. pants.

934 Vispārīgā datu aizsardzības regula, 35. apsvērums.

935 Turpat, 2. pants.

936 ECT 1997. gada 25. februāra spriedums lietā *Z pret Somiju*, Nr. 22009/93, 94. un 112. punkts; skatīt arī ECT 1997. gada 27. augusta spriedumu lietā *M.S. pret Zviedriju*, Nr. 20837/92; ECT 2006. gada 10. oktobra spriedumu lietā *L.L. pret Franciju*, Nr. 7508/02; ECT 2008. gada 17. jūlija spriedumu lietā *I pret Somiju*, Nr. 20511/03; ECT 2009. gada 28. aprīļa spriedumu lietā *K.H. un citi pret Slovākiju*, Nr. 32881/04; ECT 2009. gada 2. jūnija spriedumu lietā *Szuluk pret Apvienoto Karalisti*, Nr. 36936/05.

Saskaņā ar **ES tiesību aktiem** Vispārīgās datu aizsardzības regulas 9. panta 2. punkta h) apakšpunkts ļauj apstrādāt medicīniskos datus, ja tas ir nepieciešams profilaktiskās medicīnas, medicīniskas diagnozes, aprūpes vai ārstēšanas nodrošināšanas vai veselības aprūpes pakalpojumu pārvaldības nolūkos. Apstrāde tomēr ir pieļaujama tikai tad, ja to veic veselības aprūpes speciālists, uz kuru attiecas pienākums glabāt dienesta noslēpumu, vai cita persona, kurai ir saistoši līdzvērtīgi pienākumi.

Saskaņā ar **EP tiesību aktiem** 1997. gada Medicīnisko datu ieteikumā sīkāk izstrādāti Konvencijas Nr. 108 principi, kas piemērojami datu apstrādei medicīnas jomā[937]. Ierosinātie noteikumi atbilst Vispārīgās datu aizsardzības regulas nosacījumiem attiecībā uz medicīnisko datu apstrādes likumīgajiem mērķiem, obligātajiem dienesta noslēpumu pienākumiem personām, kuras izmanto veselības datus, un datu subjektu tiesībām uz pārredzamību un piekļuvi, labošanu un dzēšanu. Turklāt medicīnas datus, ko likumīgi apstrādā veselības aprūpes speciālisti, nedrīkst nodot tiesībaizsardzības iestādēm, ja nav nodrošināti "pietiekami drošības pasākumi, lai novērstu informācijas izpaušanu, kas ir pretrunā ECTK 8. pantā garantētajai (..) privātās dzīves neaizskaramībai"[938]. Arī valsts tiesību aktiem "jābūt pietiekami precīzi formulētiem, un tiem ir jāsniedz atbilstoša tiesiskā aizsardzība pret patvaļu"[939].

Turklāt Medicīnisko datu ieteikumā ir īpaši noteikumi par nedzimušu bērnu un rīcībnespējīgu personu medicīniskajiem datiem, kā arī par ģenētisko datu apstrādi. Zinātniskā pētniecība ir nepārprotami atzīts iemesls datu saglabāšanai ilgāk nekā tas nepieciešams, lai gan parasti šim nolūkam būs jāveic anonimizācija. Medicīnisko datu ieteikuma 12. punktā ir ierosināti detalizēti izstrādāti noteikumi situācijām, kad pētniekiem nepieciešami personas dati, bet anonimizēti dati nav pietiekami.

Pseidonimizācija var būt piemērots līdzeklis, lai apmierinātu zinātnes vajadzības, vienlaikus aizsargājot skarto pacientu intereses. Pseidonimizācijas jēdziens datu aizsardzības kontekstā plašāk izskaidrots 2.1.1. iedaļā.

937 Eiropas Padome, Ministru komiteja (1997), Ieteikums Rec(97)5 dalībvalstīm par medicīnisko datu aizsardzību, 1997. gada 13. februāris. Vēršam uzmanību, ka šis ieteikums šobrīd tiek pārskatīts.

938 ECT 2013. gada 6. jūnija spriedums lietā *Avilkina un citi pret Krieviju*, Nr. 1585/09, 53. punkts. Skatīt arī ECT 2008. gada 25. novembra spriedumu lietā *Biriuk pret Lietuvu*, Nr. 23373/03.

939 ECT 2014. gada 29. aprīļa spriedums lietā *L.H. pret Latviju*, Nr. 52019/07, 59. punkts.

Eiropas Padomes 2016. gada ieteikums par datiem, kas iegūti ģenētisku testu rezultātā, attiecas arī uz datu apstrādi medicīnas jomā[940]. Šis ieteikums ir ļoti svarīgs e-veselībai, ko medicīniskās aprūpes nodrošināšanas atvieglošanai izmanto IKT. Šāds piemērs ir pacienta paternitātes testa rezultātu nosūtīšana no viena veselības aprūpes sniedzēja citam. Šā ieteikuma mērķis ir aizsargāt to personu tiesības, kuru personas dati tiek apstrādāti apdrošināšanas nolūkos, apdrošinot pret riskiem, kas saistīti ar personas veselību, fizisko stāvokli, vecumu vai nāvi. Apdrošinātājiem jāpamato ar veselību saistīto datu apstrāde, un apstrādei jābūt samērīgai, salīdzinot ar apsvērtā riska raksturu un nozīmīgumu. Šāda veida datu apstrādei ir nepieciešama subjekta piekrišana. Apdrošinātājiem arī ir jāievieš aizsardzības pasākumi ar veselību saistītu datu glabāšanai.

Klīniskajiem pētījumiem, kas ietver jaunu zāļu ietekmes uz pacientiem dokumentētā pētniecības vidē novērtēšanu, ir ievērojama ietekme uz datu aizsardzību. Cilvēkiem paredzētu zāļu klīnisko izpēti reglamentē ar Eiropas Parlamenta un Padomes 2014. gada 16. aprīļa Regulu (ES) Nr. 536/2014 par cilvēkiem paredzētu zāļu klīniskajām pārbaudēm un ar ko atceļ Direktīvu 2001/20/EK (Klīnisko izmēģinājumu regula)[941]. Klīnisko izmēģinājumu regulas galvenie elementi ir šādi:

- racionalizēta pieteikumu iesniegšanas procedūra, izmantojot ES portālu[942];
- klīnisko pētījumu pieteikumu izvērtēšanas termiņi[943];
- ētikas komiteja, kas piedalās izvērtējumā saskaņā ar dalībvalstu tiesību aktiem (un Eiropas tiesību aktiem, kuros noteikti attiecīgie laika periodi)[944]; un
- uzlabota klīnisko pētījumu un to rezultātu pārredzamība[945].

940 Eiropas Padome, Ministru komiteja (2016), Ieteikums Nr. Rec(2016)8 dalībvalstīm par personas ar veselību saistītu datu, tostarp datu, kas iegūti ģenētiskos testos, apstrādi apdrošināšanas vajadzībām, 2016. gada 26. oktobris.

941 Eiropas Parlamenta un Padomes 2014. gada 16. aprīļa Regula (ES) Nr. 536/2014 par cilvēkiem paredzētu zāļu klīniskajām pārbaudēm un ar ko atceļ Direktīvu 2001/20/EK (Klīnisko izmēģinājumu regula), OV 2014 L 158.

942 Klīnisko izmēģinājumu regula, 5. panta 1. punkts.

943 Turpat, 5. panta 2.–5. punkts.

944 Turpat, 2. panta 2. punkta 11. apakšpunkts.

945 Turpat, 9. panta 1. punkts un 67. apsvērums.

Vispārīgajā datu aizsardzības regulā noteikts, ka, sniedzot piekrišanu dalībai zinātniskās pētniecības darbībās klīniskajos pētījumos, piemēro Regulu (ES) Nr. 536/2014[946].

ES mērogā tiek gatavotas vairākas citas likumdošanas un citas iniciatīvas attiecībā uz personas datiem veselības nozarē[947].

Elektroniskās veselības kartes

Elektroniskā veselības karte definēta kā "visaptveroša medicīniskā karte vai līdzīga dokumentācija elektroniskā formā par personas agrāko un tagadējo fiziskās un garīgās veselības stāvokli, kura ļauj viegli piekļūt šiem datiem ārstēšanas un citām cieši saistītām vajadzībām"[948]. Elektroniskās veselības kartes ir pacientu slimības vēstures elektroniskas versijas, un tās var ietvert klīniskos datus attiecībā uz šīm personām, piemēram, iepriekšējo slimības vēsturi, problēmas un apstākļus, medikamentus un ārstēšanu, kā arī izmeklējumu un laboratorijas rezultātus un ziņojumus. Šiem elektroniskajiem dokumentiem, kas var būt gan pilnīga medicīniskā karte, gan izraksti vai kopsavilkumi, var piekļūt ģimenes ārsts, farmaceits un citi veselības aprūpes speciālisti. E-veselības jēdziens attiecas arī uz šīm medicīniskajām kartēm.

> Piemērs. A kungs ir noslēdzis apdrošināšanas polisi ar uzņēmumu B, kas ir apdrošinātājs. Apdrošinātājs no A apkopos noteiktu ar veselību saistītu informāciju, piemēram, par aktuāliem veselības jautājumiem vai slimībām. Apdrošinātājam ir jāuzglabā A ar veselību saistītie personas dati atsevišķi no citiem datiem. Apdrošinātājam arī jāuzglabā ar veselību saistītie personas dati atsevišķi no citiem personas datiem. Tas nozīmē, ka tikai par A lietu atbildīgajam darbiniekam būs piekļuve A veselības datiem.

Tomēr dažas datu aizsardzības problēmas rada elektroniskie veselības dokumenti, piemēram, to pieejamība, pareiza glabāšana un datu subjekta piekļuve.

Papildus elektroniskajām veselības kartēm 2014. gada 10. aprīlī Eiropas Komisija publicēja Zaļo grāmatu par mobilo veselību (m-veselību), uzskatot, ka m-veselība ir

946 Vispārīgā datu aizsardzības regula, 156. un 161. apsvērums.

947 EDAU (2013), *Eiropas Datu aizsardzības uzraudzītāja Atzinums par Komisijas paziņojumu "E-veselības rīcības plāns 2012.–2020. gadam – inovatīva veselības aprūpe 21. gadsimtam", Brisele, 2013. gada 27. marts.*

948 Komisijas 2008. gada 2. jūlija Ieteikums par elektronisko veselības karšu sistēmu pārrobežu sadarbspēju, 3. punkta c) apakšpunkts.

jauna un strauji augoša joma, kas veselības aprūpi var pārveidot, kā arī paaugstināt tās efektivitāti un kvalitāti. Šis termins aptver medicīnisko un sabiedrības veselības praksi, kurā izmanto mobilās ierīces, piemēram, mobilos tālruņus, pacientu uzraudzības ierīces, personālos digitālos asistentus un citas bezvadu ierīces, kā arī lietotnes (piemēram, labsajūtas lietotnes), ko var savienot ar medicīniskām ierīcēm vai sensoriem[949]. Dokumentā ir aprakstīti ar personas datu aizsardzības tiesībām saistītie riski, ko varētu radīt m-veselības attīstība, un noteikts, ka, ņemot vērā veselības datu sensitīvo raksturu, attīstībā ir jāievieš konkrēti un atbilstoši aizsardzības pasākumi pacienta datiem, piemēram, šifrēšana, un piemēroti pacientu autentifikācijas mehānismi, lai mazinātu drošības riskus. Personas datu aizsardzības noteikumu, tostarp pienākuma sniegt informāciju datu subjektam, datu drošības un personas datu likumīgas apstrādes principa ievērošana ir būtiska, lai panāktu uzticēšanos m-veselības risinājumiem[950]. Tāpēc nozare ir izstrādājusi rīcības kodeksu, kura izstrādē piedalījies plašs ieinteresēto personu loks, tostarp pārstāvji, kuri ir kompetenti datu aizsardzībā, pašregulēšanā un kopregulēšanā, IKT un veselības aprūpē[951]. Rokasgrāmatas izstrādes laikā rīcības kodeksa projekts bija iesniegts 29. panta datu aizsardzības darba grupai komentāru sniegšanai, gaidot tā oficiālu apstiprināšanu.

9.4. Datu apstrāde pētniecības un statistikas nolūkos

Svarīgākie aspekti

- Datus, kas vākti statistikas, zinātniskās vai vēstures pētniecības nolūkos, nedrīkst izmantot citos nolūkos.
- Dati, kas likumīgi vākti jebkādam nolūkam, var tikt izmantoti arī statistikas, zinātniskās vai vēstures pētniecības nolūkos, ja ir ieviesti atbilstoši aizsardzības pasākumi. Šim nolūkam anonimizācija vai pseidonimizācija pirms datu pārsūtīšanas trešām personām var būt šādi aizsardzības pasākumi.

ES tiesību akti atļauj apstrādāt datus statistikas un zinātniskās vai vēstures pētniecības nolūkos, ja ir ieviesti attiecīgi datu subjektu tiesību un brīvību aizsardzības

949 Eiropas Komisija (2014), *Zaļā grāmata par mobilo veselību ("m-veselība")*, COM(2014) 219 *final*, Brisele, 2014. gada 10. aprīlis.

950 Turpat, 8. lpp.

951 Rīcības kodeksa par privātumu mobilajās veselības aprūpes lietotnēs projekts, 2016. gada 7. jūnijs.

pasākumi. Tie var ietvert pseidonimizāciju[952]. ES vai valstu tiesību aktos var paredzēt noteiktas atkāpes no datu subjektu tiesībām, ja šīs tiesības, iespējams, padara neiespējamu vai nopietni pasliktina pētījumu likumīgā mērķa sasniegšanu[953]. Var ieviest atkāpes attiecībā uz datu subjekta piekļuves tiesībām, tiesībām veikt labojumus, tiesībām uz apstrādes ierobežošanu un tiesībām iebilst.

Lai gan datus, ko pārzinis likumīgi savācis jebkādam nolūkam, šis pārzinis var atkārtoti izmantot savos statistikas, zinātniskās vai vēstures pētniecības nolūkos, tomēr dati jāanonimizē vai atkarībā no konteksta jāpiemēro tādi pasākumi kā pseidonimizācija pirms to nosūtīšanas trešām personām statistikas, zinātniskas vai vēstures pētniecības nolūkos, izņemot gadījumus, kad datu subjekts tam devis piekrišanu vai ja tas īpaši paredzēts valsts tiesību aktos. Atšķirībā no anonīmiem datiem uz pseidonimizētiem datiem joprojām attiecas Vispārīgā datu aizsardzības regula[954].

Tādējādi ar regulu tiek noteikts īpašs režīms attiecībā uz vispārīgajiem datu aizsardzības noteikumiem, lai neierobežotu pētniecības attīstību un izveidotu Eiropas pētniecības telpu, kā noteikts LESD 179. pantā. Tas nodrošina personas datu apstrādes plašu interpretāciju zinātniskās pētniecības, tostarp tehnoloģiju attīstības un demonstrēšanas, fundamentālo zinātnes pētījumu, lietišķo pētījumu un privāti finansētu pētījumu, nolūkos. Šeit arī atzīta datu apkopošanas reģistros nozīme pētniecības nolūkos un iespējamās grūtības datu vākšanas brīdī pilnībā identificēt personas datu apstrādes nākamo mērķi zinātniskās pētniecības nolūkos[955]. Šā iemesla dēļ regula atļauj apstrādāt datus šajos nolūkos bez datu subjektu piekrišanas, ja ir ieviesti attiecīgie aizsardzības pasākumi.

Svarīgs datu izmantošanas piemērs statistikas nolūkos ir oficiālā statistika, ko iegūst valstu un ES statistikas biroji saskaņā ar valstu un ES tiesību aktiem par oficiālo statistiku. Saskaņā ar šiem tiesību aktiem pilsoņiem un uzņēmumiem parasti ir pienākums izpaust datus attiecīgajām statistikas iestādēm. Ierēdņiem, kuri strādā statistikas birojos, ir saistoši īpaši pienākumi par dienesta noslēpuma glabāšanu, kas pienācīgi jāizpilda, jo tie ir izšķirīgi augsta līmeņa pilsoņu uzticības panākšanai, kāda nepieciešama, kad dati jāpadara pieejami statistikas iestādēm[956].

952 Vispārīgā datu aizsardzības regula, 89. panta 1. punkts.

953 Turpat, 89. panta 2. punkts.

954 Turpat, 26. apsvērums.

955 Turpat 33., 157. un 159. apsvērums.

956 Turpat, 90. pants.

Regula (EK) Nr. 223/2009 par Eiropas statistiku (Eiropas statistikas regula) satur būtiskus datu aizsardzības noteikumus oficiālās statistikas kontekstā, un tāpēc to var uzskatīt par attiecināmu arī uz noteikumiem par oficiālo statistiku, kas pieņemti valsts līmenī[957]. Regulā ir saglabāts princips, ka oficiālās statistikas darbībām ir nepieciešams pietiekami skaidrs juridiskais pamats[958].

Piemērs. Lietā *Huber pret Bundesrepublik Deutschland*[959] Austrijas uzņēmējs, kurš pārcēlās uz Vāciju, sūdzējās, ka vācu iestādes vāca un glabāja ārvalstu pilsoņu personas datus centrālajā reģistrā (*AZR*) arī statistikas nolūkos, tādējādi pārkāpjot viņa tiesības saskaņā ar Datu aizsardzības direktīvu. Ņemot vērā, ka Direktīvas 95/46/EK mērķis ir nodrošināt vienādu datu aizsardzības līmeni visās dalībvalstīs, EST sprieda, ka, lai nodrošinātu augstu aizsardzības līmeni ES, 7. panta e) punktā ietvertajam nepieciešamības jēdzienam nevar būt atšķirīga nozīme dažādās dalībvalstīs. Tādējādi šis ir jēdziens ar savu neatkarīgu nozīmi ES tiesībās, un tas jāinterpretē veidā, kas pilnībā atspoguļo Direktīvas 95/46/EK mērķi. EST, atzīmējot, ka statistikas nolūkos ir nepieciešama tikai anonīma informācija, nolēma, ka Vācijas reģistrs nav savienojams ar 7. panta e) punktā ietverto nepieciešamības prasību.

EP kontekstā datu turpmāku apstrādi var veikt zinātniskos, vēstures vai statistikas nolūkos, ja tas ir sabiedrības interesēs, un ir jāpiemēro attiecīgi aizsardzības pasākumi[960]. Datu subjektu tiesības var tikt ierobežotas arī tad, ja datus apstrādā statistikas nolūkos, ja vien nepastāv acīmredzams risks pārkāpt viņu tiesības un brīvības[961].

957 Eiropas Parlamenta un Padomes 2009. gada 11. marta Regula (EK) Nr. 223/2009 par Eiropas statistiku un ar ko atceļ Eiropas Parlamenta un Padomes Regulu (EK, Euratom) Nr. 1101/2008 par tādas statistikas informācijas nosūtīšanu Eiropas Kopienu Statistikas birojam, uz kuru attiecas konfidencialitāte, Padomes Regulu (EK) Nr. 322/97 par Kopienas statistiku un Padomes Lēmumu 89/382/EEK, Euratom, ar ko nodibina Eiropas Kopienu Statistikas programmu komiteju, OV 2009 L 87, kas grozīta ar Eiropas Parlamenta un Padomes 2015. gada 29. aprīļa Regulu (ES) 2015/759, ar ko groza Regulu (EK) Nr. 223/2009 par Eiropas statistiku, OV 2015 L 123.

958 Šis princips plašāk izklāstīts Eiropas Statistikas prakses kodeksā, kurā saskaņā ar Eiropas statistikas regulas 11. pantu ir sniegti ētiski norādījumi par to, kā vest oficiālo statistiku, tostarp rūpīgu personas datu izmantošanu.

959 EST 2008. gada 16. decembra spriedums lietā C-524/06 *Heinz Huber pret Bundesrepublik Deutschland* [GC]; skatīt jo īpaši 68. punktu.

960 Modernizētā Konvencija Nr. 108, 5. panta 4. punkta b) apakšpunkts.

961 Turpat, 11. panta 2. punkts.

Statistikas datu ieteikums, kas izdots 1997. gadā, attiecas uz statistikas darbību veikšanu publiskajā un privātajā sektorā[962].

Datus, ko pārzinis ievācis statistikas nolūkos, nedrīkst izmantot citos nolūkos. Dati, kas savākti ar statistiku nesaistītos nolūkos, ir pieejami turpmākai izmantošanai statistikas nolūkos. Saskaņā ar Statistikas datu ieteikumu datus var paziņot trešām personām ar nosacījumu, ka tie paredzēti tikai statistikas nolūkiem. Šādos gadījumos pusēm ir jāvienojas un jāapraksta likumīgas turpmākās izmantošanas apmērs statistikas nolūkos. Tā kā tas nevar aizstāt datu subjekta piekrišanu, ja tāda nepieciešama, valstu tiesību aktos ir jāparedz attiecīgi aizsardzības pasākumi, lai mazinātu personas datu ļaunprātīgas izmantošanas risku, piemēram, pienākumu anonimizēt vai pseidonimizēt datus pirms to izpaušanas.

Statistikas pētījumu speciālistiem saskaņā ar valstu tiesību aktiem ir jāievēro īpaši pienākumi par dienesta noslēpuma glabāšanu, kā tas parasti tiek attiecināts uz oficiālo statistiku. Tas jāattiecina arī uz intervētājiem un citām personām, kuras vāc personas datus, ja viņus nodarbina datu vākšanā no datu subjektiem vai citām personām.

Ja statistikas apsekojums, kurā izmanto personas datus, nav atļauts likumā, datu subjektiem būtu jāsniedz piekrišana savu datu izmantošanai, lai šāds apsekojums būtu likumīgs, vai arī viņiem jābūt iespējai iebilst. Ja intervētāji vāc personas datus statistikas nolūkos, intervējamie skaidri jāinformē par to, vai datu sniegšana ir obligāta saskaņā ar valsts tiesību aktiem.

Ja statistikas apsekojumu nevar veikt, izmantojot anonīmus datus, un ir nepieciešami personas dati, šim nolūkam apkopotie dati pēc iespējas drīz jāanonimizē. Statistikas apsekojuma rezultāti vismaz nedrīkst ļaut identificēt nevienu datu subjektu, izņemot gadījumus, kad tas nepārprotami nerada risku.

Pēc statistiskās analīzes pabeigšanas izmantotie personas dati jādzēš vai jāanonimizē. Tādos gadījumos Statistikas datu ieteikums iesaka identifikācijas datus uzglabāt atsevišķi no citiem personas datiem. Tas nozīmē, piemēram, ka šifrēšanas atslēga vai saraksts, kurā ir identificējošie sinonīmi, ir jāglabā atsevišķi no citiem datiem.

962 Eiropas Padomes Ministru komiteja (1997), Ieteikums Nr. Rec(97)18 dalībvalstīm par personas datu, kas ievākti un apstrādāti statistikas nolūkos, aizsardzību, 1997. gada 30. septembris.

9.5. Finanšu dati

Svarīgākie aspekti

- Lai arī saskaņā ar modernizēto Konvenciju Nr. 108 vai Vispārīgo datu aizsardzības regulu finanšu datus neuzskata par sensitīviem datiem, to apstrādei ir nepieciešami īpaši aizsardzības pasākumi, lai nodrošinātu precizitāti un datu drošību.
- Elektroniskajām norēķinu sistēmām jo īpaši nepieciešama iebūvēta datu aizsardzība, t. i., privātums vai integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma.
- Šajā jomā var rasties īpašas datu aizsardzības problēmas, jo nepieciešami piemēroti autentifikācijas mehānismi.

Piemērs. Lietā *Michaud pret Franciju*[963] prasītājs, Francijā praktizējošs jurists, apstrīdēja savu pienākumu saskaņā ar Francijas tiesību aktiem ziņot par aizdomām par viņa klientu iespējamām nelikumīgi iegūtu līdzekļu legalizācijas darbībām. ECT atzīmēja, ka juristu pienākums nodot administratīvajām iestādēm informāciju par citu personu, kas viņu rīcībā nonākusi profesionālas apmaiņas rezultātā, ir iejaukšanās juristu tiesībās uz viņu korespondences un privātās dzīves neaizskaramību saskaņā ar ECKT 8. pantu, jo šis jēdziens aptver profesionāla vai uzņēmējdarbības rakstura darbības. Tomēr iejaukšanās notika saskaņā ar likumu un tai bija likumīgs mērķis, proti, nekārtību un noziedzīgu nodarījumu novēršana. Tā kā juristiem ir pienākums ziņot par aizdomīgām darbībām tikai ļoti īpašos apstākļos, ECT uzskatīja, ka šis pienākums ir samērīgs. Tiesa atzina, ka šajā lietā 8. pants nav ticis pārkāpts.

Piemērs. Lietā *M.N. un citi pret Sanmarīno*[964] prasītājs, Itālijas pilsonis, noslēdza fiduciāru līgumu ar uzņēmumu, pret kuru tika veikta izmeklēšana. Tas nozīmēja, ka uzņēmumā tika veikta kratīšana un konfiscētas (elektronisko) dokumentu kopijas. Prasītājs iesniedza sūdzību Sanmarīno tiesā, apgalvojot, ka starp viņu un iespējamiem noziegumiem neesot nekādas saistības. Tomēr tiesa atzina viņa sūdzību par nepieņemamu, jo viņš nebija "ieinteresētā puse". ECT sprieda, ka prasītājs bija ievērojami nelabvēlīgākā situācijā

963 ECT 2012. gada 6. decembra spriedums lietā *Michaud pret Franciju*, Nr. 12323/11. Skatīt arī ECT 1992. gada 16. decembra spriedumu lietā *Niemietz pret Vāciju*, Nr. 13710/88, 29. punkts, un ECT 1997. gada 25. jūnija spriedumu lietā *Halford pret Apvienoto Karalisti*, Nr. 20605/92, 42. punkts.

964 ECT 2015. gada 7. jūlija spriedums lietā *M.N. un citi pret Sanmarīno*, Nr. 28005/12.

attiecībā uz tiesisko aizsardzību salīdzinājumā ar "ieinteresēto pusi", tomēr attiecībā uz viņa datiem tika veikta kratīšana un aresta darbības. Tādējādi tiesa uzskatīja, ka ir noticis 8. panta pārkāpums.

Piemērs. Lietā *G.S.B. pret Šveici*[965] informācija no prasītāja bankas konta tika nosūtīta ASV nodokļu iestādēm, balstoties uz administratīvās sadarbības līgumu starp Šveici un ASV. ECT uzskatīja, ka nosūtīšana nav pretrunā ECTK 8. pantam, jo iejaukšanās prasītāja tiesībās uz privātumu bija noteikta likumā, tai bija likumīgs mērķis un tā bija samērīga pret attiecīgajām sabiedrības interesēm.

Datu aizsardzības vispārējā tiesiskā regulējuma (kā noteikts Konvencijā Nr. 108) piemērošana maksājumu kontekstā tika izstrādāta **EP** 1990. gada Ieteikumā Rec(90)19[966]. Šajā ieteikumā precizēta likumīgas datu vākšanas un izmantošanas joma saistībā ar maksājumiem, jo īpaši ar maksājumu kartēm. Tajā arī sniegti sīki izstrādāti ieteikumi vietējiem likumdevējiem attiecībā uz noteikumiem par maksājumu datu izpaušanu trešām personām, par datu saglabāšanas termiņiem, par pārredzamību, datu drošību un pārrobežu datu plūsmām, kā arī par uzraudzību un tiesiskās aizsardzības līdzekļiem. Eiropas Padome ir arī izstrādājusi Atzinumu par nodokļu datu nodošanu[967], kurā sniegti ieteikumi un jautājumi, kas jāņem vērā darbā ar nodokļu datu nodošanu.

ECT ļauj pārsūtīt finanšu datus, jo īpaši informāciju par personas bankas kontu, saskaņā ar ECTK 8. pantu, ja tas ir noteikts likumā, tam ir likumīgs mērķis un tas ir samērīgi pret attiecīgajām sabiedrības interesēm[968].

Saskaņā ar **ES tiesību aktiem** elektroniskajām norēķinu sistēmām, kas paredz personas datu apstrādi, jāatbilst Vispārīgajai datu aizsardzības regulai. Tādēļ šīm sistēmām ir jānodrošina gan integrēta datu aizsardzība, gan datu aizsardzība pēc noklusējuma. Integrēta datu aizsardzība uzliek pienākumu pārzinim veikt attiecīgus tehniskos un organizatoriskos pasākumus, lai ieviestu datu aizsardzības principus. Datu aizsardzība pēc noklusējuma nozīmē, ka pārzinim ir jānodrošina, ka pēc noklusējuma var apstrādāt tikai tos personas datus, kas nepieciešami konkrētam nolūkam (skatīt

965 ECT 2015. gada 22. decembra spriedums lietā *G.S.B. pret Šveici*, Nr. 28601/11.

966 Eiropas Padomes Ministru komiteja (1990), Ieteikums Nr. Rec(90)19 par personas datu aizsardzību, ko izmanto maksājumiem un citām saistītām darbībām, 1990. gada 13. septembris.

967 Eiropas Padome, Konvencijas Nr. 108 konsultatīvā komiteja (2014), Atzinums par automātiskas starpvalstu datu apmaiņas administratīvos un nodokļu nolūkos mehānismu ietekmi uz datu aizsardzību, 2014. gada 4. jūnijs.

968 ECT 2015. gada 22. decembra spriedums lietā *G.S.B. pret Šveici*, Nr. 28601/11.

4.4. iedaļu). Attiecībā uz finanšu datiem EST uzskatīja, ka nodotie nodokļu dati var būt personas dati[969]. 29. panta datu aizsardzības darba grupa izdeva attiecīgas pamatnostādnes dalībvalstīm, iekļaujot kritērijus, kas nodrošina datu aizsardzības noteikumu ievērošanu, veicot automātiski personas datu apmaiņu nodokļu vajadzībām[970]. Turklāt ir pieņemti vairāki tiesību instrumenti, kas regulē finanšu tirgus un kredītiestāžu un ieguldījumu firmu darbību[971]. Citi tiesību instrumenti palīdz cīnīties ar iekšējās informācijas ļaunprātīgu izmantošanu un tirgus manipulācijām[972]. Galvenās jomas, kas ietekmē datu aizsardzību, ir šādas:

- finanšu darījumu uzskaites saglabāšana;
- personas datu nosūtīšana trešām valstīm;
- telefonsarunu vai elektroniskās komunikācijas ierakstīšana, tostarp kompetento iestāžu pilnvaras pieprasīt tālruņa un datu plūsmas ierakstus;
- personiskas informācijas izpaušana, tostarp sankciju publicēšana;
- kompetento iestāžu uzraudzības un izmeklēšanas pilnvaras, tostarp pārbaudes uz vietas un iekļūšana privātās telpās, lai izņemtu dokumentus;
- ziņošanas par pārkāpumiem, t. i., trauksmes celšanas shēmu, mehānismi; un
- sadarbība starp dalībvalstu kompetentajām iestādēm un Eiropas Vērtspapīru un tirgu iestādi (EVTI).

969 EST 2015. gada 1. oktobra spriedums lietā C-201/14 *Smaranda Bara un citi pret Casa Națională de Asigurări de Sănătate un citiem*, 29. punkts.

970 29. panta datu aizsardzības darba grupa (2015), DG29 paziņojums par automātisks starpvalstu personas datu apmaiņu nodokļu vajadzībām, 14/EN WP 230.

971 Eiropas Parlamenta un Padomes 2014. gada 15. maija Direktīva 2014/65/ES par finanšu instrumentu tirgiem un ar ko groza Direktīvu 2002/92/ES un Direktīvu 2011/61/ES, OV 2014 L 173; Eiropas Parlamenta un Padomes 2014. gada 15. maija Regula (ES) Nr. 600/2014 par finanšu instrumentu tirgiem un ar ko groza Regulu (ES) Nr. 648/2012, OV 2014 L 173; Eiropas Parlamenta un Padomes 2013. gada 26. jūnija Direktīva 2013/36/ES par piekļuvi kredītiestāžu darbībai un kredītiestāžu un ieguldījumu brokeru sabiedrību prudenciālo uzraudzību, ar ko groza Direktīvu 2002/87/EK un atceļ Direktīvas 2006/48/EK un 2006/49/EK, OV 2013 L 176.

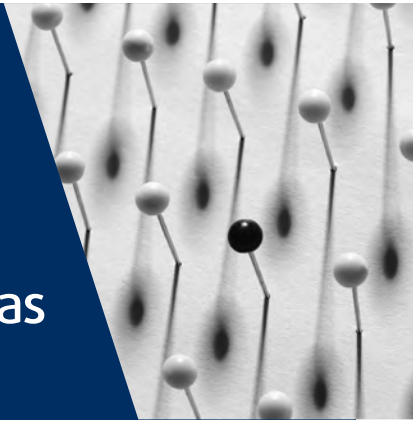
972 Eiropas Parlamenta un Padomes 2014. gada 16. aprīla Regula (ES) Nr. 596/2014 par tirgus ļaunprātīgu izmantošanu (Tirgus ļaunprātīgas izmantošanas regula) un ar ko atceļ Eiropas Parlamenta un Padomes Direktīvu 2003/6/EK un Komisijas Direktīvas 2003/124/EK, 2003/125/EK un 2004/72/EK, OV 2014 L 173.

Īpaši tiek aplūkoti arī citi jautājumi šajās jomās, tostarp datu vākšana par datu subjektu finansiālo stāvokli[973] vai pārrobežu maksājumi ar bankas pārskaitījumu, kas neizbēgami noved pie personas datu plūsmas[974].

973 Eiropas Parlamenta un Padomes 2009. gada 16. septembra Regula (EK) Nr. 1060/2009 par kredītreitingu aģentūrām, OV 2009 L 302, un, kas nesen grozīta ar Eiropas Parlamenta un Padomes 2014. gada 16. aprīļa Direktīvu 2014/51/ES, ar ko groza Direktīvu 2003/71/EK un Direktīvu 2009/138/EK un Regulas (EK) Nr. 1060/2009, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010 attiecībā uz Eiropas Uzraudzības iestādes (Eiropas Apdrošināšanas un fondēto pensiju iestādes) un Eiropas Uzraudzības iestādes (Eiropas Vērtspapīru un tirgu iestādes) pilnvarām, OV 2014 L 153; Eiropas Parlamenta un Padomes 2013. gada 21. maija Regula (ES) Nr. 462/2013, ar ko groza Regulu (EK) Nr. 1060/2009 par kredītreitingu aģentūrām, OV 2013 L 146.

974 Eiropas Parlamenta un Padomes 2007. gada 13. novembra Direktīva 2007/64/EK par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 97/7/EK, 2002/65/EK, 2005/60/EK un 2006/48/EK un atceļ Direktīvu 97/5/EK, OV 2007 L 319, kas grozīta ar Eiropas Parlamenta un Padomes 2009. gada 16. septembra Direktīvu 2009/111/EK, ar ko groza Direktīvas 2006/48/EK, 2006/49/EK un 2007/64/EK attiecībā uz bankām, kuras saistītas ar galvenajām iestādēm, dažiem pašu kapitāla posteņiem, lieliem riska darījumiem, uzraudzības pasākumiem un krīzes pārvaldību, OV 2009 L 302.

10 Mūsdienu problēmas personas datu aizsardzības jomā



Digitālajam laikmetam jeb informācijas tehnoloģiju laikmetam ir raksturīga plaša datoru, interneta un digitālo tehnoloģiju izmantošana. Tā ietver milzīga apjoma datu, tostarp personas datu, vākšanu un apstrādi. Personas datu vākšana un apstrāde globalizētā ekonomikā nozīmē, ka pieaug pārrobežu datu plūsma. Šāda apstrāde var sniegt nozīmīgus un redzamus ieguvumus ikdienas dzīvē, jo meklētājprogrammas atvieglo piekļuvi ievērojamam informācijas un zināšanu apjomam, sociālo tīklu pakalpojumi ļauj cilvēkiem visā pasaulē sazināties, paust viedokli un mobilizēt atbalstu sociāliem, vides un politiskiem mērķiem, savukārt uzņēmumi un patērētāji gūst labumu no efektīvām un iedarbīgām tirgvedības metodēm, kas stimulē ekonomiku. Tehnoloģijas un personas datu apstrāde ir arī neaizstājami instrumenti valsts iestādēm cīņā pret noziedzību un terorismu. Tāpat lieli dati – liela apjoma informācijas vākšana, glabāšana un analīze, lai identificētu modeļus un prognozētu uzvedību, "var būt būtiskas vērtības avots sabiedrībai, uzlabojot produktivitāti, publiskā sektora sniegumu un sociālo līdzdalību"[975].

Lai gan ir daudz ieguvumu, digitālajam laikmetam tomēr raksturīgas arī problēmas privātumam un datu aizsardzībai, jo milzīgs personiskās informācijas apjoms tiek vākts un apstrādāts arvien sarežģītākos un nepārskatāmākos veidos. Tehnoloģiskā progresa rezultātā ir izveidotas masīvas datu kopas, ko var viegli pārbaudīt un tālāk analizēt, meklējot modeļus, vai tādu lēmumu pieņemšanai, kuru pamatā ir algoritmi, kas var sniegt vēl nebijušu ieskatu cilvēku uzvedībā un privātajā dzīvē[976].

975 Eiropas Padomes Konvencijas Nr. 108 konsultatīvā komiteja, *Vadlīnijas personu aizsardzībai attiecībā uz personas datu apstrādi lielo datu pasaulē*, T-PD(2017)01, Strasbūra, 2017. gada 23. janvāris.

976 Eiropas Parlaments (2017), Rezolūcija par lielo datu ietekmi uz pamattiesībām – privātums, datu aizsardzība, nediskriminācija, drošība un tiesību aizsardzība (P8_TA-PROV(2017)0076, Strasbūra, 2017. gada 14. marts.

Jaunās tehnoloģijas ir jaudīgas un var kļūt īpaši bīstamas, nonākot nepareizajās rokās. Valsts iestādes, kas īsteno masu novērošanas pasākumus, kuros var izmantot šīs tehnoloģijas, ir piemērs tam, kādu ietekmi šīs tehnoloģijas var atstāt uz indivīdu tiesībām. Edvarda Snoudena atklāsmes par izlūkošanas aģentūru plaša mēroga interneta un tālruņu novērošanas programmu darbību 2013. gadā dažās valstīs izraisīja nopietnas bažas par briesmām, ko novērošanas pasākumi rada privātumam, demokrātiskai pārvaldībai un vārda brīvībai. Masu novērošana un tehnoloģijas, kas ļauj globāli glabāt un apstrādāt personisku informāciju un masveidā piekļūt datiem, var ietekmēt tiesību uz privātumu būtību[977]. Turklāt tām var būt negatīva ietekme uz politisko kultūru un nelabvēlīga ietekme uz demokrātiju, radošumu un inovācijām[978]. Tikai bailes par to, ka valsts var pastāvīgi izsekot un analizēt pilsoņu izturēšanos un rīcību, var viņiem likt atturēties paust viedokli par konkrētiem jautājumiem un darīt viņus uzmanīgus un piesardzīgus[979]. Šīs problēmas ir pamudinājušas vairākas valsts iestādes, pētniecības centrus un pilsoniskās sabiedrības organizācijas analizēt jauno tehnoloģiju iespējamo ietekmi uz sabiedrību. Eiropas Datu aizsardzības uzraudzītājs 2015. gadā uzsāka vairākas iniciatīvas ar mērķi novērtēt lielo datu un lietu interneta ietekmi uz ētiku. Jo īpaši, tas izveidoja Ētikas padomdevēju grupu, kuras mērķis ir veicināt "atklātu, ar informāciju pamatotu diskusiju par digitālo ētiku, lai ES varētu apzināties ieguvumus, ko tehnoloģija sniedz sabiedrībai un ekonomikai, un vienlaikus tiktu pastiprinātas fizisku personu tiesības un brīvības, īpaši to tiesības uz privātumu un datu aizsardzību"[980].

Personas datu apstrāde ir arī spēcīgs instruments korporāciju rokās. Mūsdienās tas var atklāt detalizētu informāciju par personas veselības vai finansiālo stāvokli, informāciju, ko korporācijas izmanto, pieņemot indivīdiem svarīgus lēmumus, piemēram, par viņiem piemērojamo veselības apdrošināšanas prēmiju vai viņu kredītspēju. Datu apstrādes paņēmieni var ietekmēt arī demokrātiskos procesus, ja tos izmanto politiķi vai korporācijas, lai ietekmētu vēlēšanas, piemēram, izmantojot vēlētāju saziņas "mikromērķēšanu". Citiem vārdiem sakot, lai arī privātums sākotnēji tika uztverts kā tiesības aizsargāt indivīdus pret nepamatotu valsts iestāžu iejaukšanos,

977 Skatīt ANO Ģenerālās asamblejas Īpašā ziņotāja ziņojumu par cilvēktiesību un pamatbrīvību veicināšanu un aizsardzību, apkarojot terorismu, Ben Emmerson, A/69/397, 2014. gada 23. septembris, 59. punkts. Skatīt arī ECT *Faktu lapu par masu novērošanu*, 2017. gada jūlijs.

978 EDAU (2015), *Kā risināt ar lielajiem datiem saistītās problēmas*, Atzinums 7/2015, Brisele, 2015. gada 19. novembris.

979 Skatīt jo īpaši EST 2014. gada 8. aprīļa spriedumu apvienotajās lietās C-293/12 un C-594/12 *Digital Rights Ireland Ltd pret Minister for Communications, Marine un Natural Resources un citiem* un Kärntner Landesregierung un citiem [GC], 37. punkts.

980 EDAU, 2015. gada 3. decembra Lēmums par datu aizsardzības ētisko aspektu ārējās padomdevēju grupas ("Ētikas padomdevēju grupa") izveidi, 2015. gada 3. decembris, 5. apsvērums.

mūsdienās to var apdraudēt arī privātu dalībnieku pilnvaras. Tādējādi rodas jautājumi par tehnoloģiju izmantošanu un paredzamo analīzi lēmumos, kas ietekmē indivīdu ikdienas dzīvi, un pastiprinās nepieciešamība nodrošināt, ka personas datu apstrādē tiek ievērotas pamattiesību prasības.

Datu aizsardzība ir cieši saistīta ar tehnoloģiskām, sociālām un politiskām izmaiņām. Tāpēc nav iespējams izveidot visaptverošu nākotnes problēmu sarakstu. Šajā nodaļā ir aplūkotas atsevišķas jomas saistībā ar lielajiem datiem, interneta sociālajiem tīkliem un ES digitālo vienoto tirgu. Tas nav izsmeļošs šo jomu novērtējums no datu aizsardzības viedokļa, tā vietā uzsvērta iespējamā mijiedarbība starp jaunām vai pārskatītām cilvēku darbībām un datu aizsardzības daudzveidība.

10.1. Lielie dati, algoritmi un mākslīgais intelekts

Svarīgākie aspekti

- Revolucionāras inovācijas IKT jomā veido jaunu dzīvesveidu, kurā sociālās attiecības, uzņēmējdarbība, privātie un sabiedriskie pakalpojumi ir savstarpēji digitāli savienoti, tādējādi iegūstot arvien lielāku datu daudzumu, no kuriem daudzi ir personas dati.
- Valdības, uzņēmumi un pilsoņi arvien vairāk darbojas uz datiem balstītā ekonomikā, kurā dati paši par sevi ir kļuvuši par vērtību.
- Lielo datu jēdziens attiecas gan uz datiem, gan uz to analīzi.
- Uz personas datiem, kas apstrādāti, izmantojot lielo datu analīzi, attiecas ES un EP tiesību akti.
- Atkāpes no datu aizsardzības noteikumiem un tiesībām attiecas tikai uz noteiktām tiesībām un uz konkrētām situācijām, kad tiesību īstenošana būtu neiespējama vai sagādātu datu pārziņiem nesamērīgas pūles.
- Pilnībā automatizēta lēmumu pieņemšana parasti ir aizliegta, izņemot konkrētus gadījumus.
- Personu izpratne un kontrole ir izšķirīga tiesību izpildes nodrošināšanai.

Mūsu arvien digitalizētākajā pasaulē katra darbība atstāj digitālas pēdas, ko var savākt, apstrādāt un novērtēt vai analizēt. Izmantojot jaunās informācijas un

komunikāciju tehnoloģijas, tiek savākts un reģistrēts arvien vairāk datu[981]. Vēl nesen nebija tādu tehnoloģiju, kas spētu analizēt vai novērtēt datu masu vai izdarīt noderīgus secinājumus. Datu vienkārši bija par daudz, lai tos varētu novērtēt, tie bija pārāk sarežģīti, slikti strukturēti un strauji mainīgi, lai noteiktu tendences un paradumus.

10.1.1. Lielo datu, algoritmu un mākslīgā intelekta definēšana

Lielie dati

Termins "lielie dati" ir modes vārds, kas atkarībā no konteksta var norādīt uz vairākiem jēdzieniem. Tas parasti ietver "pieaugošās tehnoloģiskās iespējas vākt, apstrādāt un izvilkt jaunas un paredzamas zināšanas no liela apjoma, straujiem un daudzveidīgiem datiem"[982]. Tāpēc lielo datu jēdziens aptver gan pašus datus, gan datu analīzi.

Datu **avoti** ir dažāda veida, un tie ietver cilvēkus un viņu personas datus, iekārtas vai sensorus, klimata informāciju, satelītattēlus, digitālos attēlus un video vai GPS signālus. Liela daļa datu un informācijas tomēr ir personas dati – jebkas no vārda, fotoattēla, e-pasta adreses, bankas rekvizītiem, GPS izsekošanas datiem, ziņām sociālo tīklu vietnēs, medicīniskās informācijas vai datora IP adreses[983].

Lielie dati attiecas arī uz datu masu un pieejamās informācijas **apstrādi**, analīzi un novērtēšanu, t. i., lai iegūtu lielo datu analīzes nolūkos noderīgu informāciju. Tas nozīmē, ka savāktos datus un informāciju var izmantot mērķiem, kas nav sākotnēji paredzētie, piemēram, statistikas tendencēm vai pielāgotākiem pakalpojumiem, piemēram, reklāmai. Faktiski, ja pastāv tehnoloģijas lielu datu vākšanai, apstrādei un novērtēšanai, jebkura veida informāciju var kombinēt un atkārtoti izvērtēt: finanšu darījumus, kredītspēju, ārstēšanu, privāto patēriņu, profesionālo darbību, izsekošanu

981 Eiropas Komisija, Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai: Ceļā uz plaukstošu ekonomiku, kura balstīta uz datiem, COM(2014) 442 *final*, Brisele, 2014. gada 2. jūlijs.

982 Eiropas Padomes Konvencijas Nr. 108 konsultatīvā komiteja, Vadlīnijas personu aizsardzībai attiecībā uz personas datu apstrādi lielo datu pasaulē, 2017. gada 23. janvāris, 2. lpp.; Eiropas Komisija, Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai: Ceļā uz plaukstošu ekonomiku, kura balstīta uz datiem, COM(2014) 442 *final*, Brisele, 2014. gada 2. jūlijs, 4. lpp.; Starptautiskā telekomunikāciju savienība (2015), Ieteikums Y.3600. Lielie dati: mākoņdatošanā balstītas prasības un iespējas.

983 ES Komisijas faktu lapa par ES datu aizsardzības reformu un lielajiem datiem; Eiropas Padome, Konvencijas Nr. 108 konsultatīvā komiteja, Vadlīnijas personu aizsardzībai attiecībā uz personas datu apstrādi lielo datu pasaulē, 2017. gada 23. janvāris, 2. lpp.

un izmantotos maršrutus, interneta lietojumu, elektronisko karšu un viedtālruņu, video vai saziņas uzraudzību. Lielo datu analīze rada jaunu datu kvantitatīvo dimensiju, kuru var novērtēt un izmantot reāllaikā, piemēram, lai sniegtu patērētājiem pielāgotus pakalpojumus.

Algoritmi un mākslīgais intelekts

Ar mākslīgo intelektu (MI) apzīmē intelektu iekārtām, kas darbojas kā "intelektuālie aģenti". Kā intelektuālais aģents noteiktas ierīces ar programmatūru atbalstu var uztvert savu apkārtējo vidi un veikt darbības saskaņā ar algoritmiem. Terminu MI lieto, ja mašīna imitē "kognitīvās" funkcijas, piemēram, mācīšanos un problēmu risināšanu, ko parasti saista ar fiziskām personām[984]. Lai atdarinātu lēmumu pieņemšanu, mūsdienu tehnoloģijas un programmatūras izmanto algoritmus, ko ierīces izmanto "automatizētu lēmumu" pieņemšanā. Algoritmu vislabāk var raksturot kā pakāpenisku rēķināšanas, datu apstrādes, novērtēšanas un automatizētas domāšanas un lēmumu pieņemšanas procedūru.

Līdzīgi lielo datu analīzei, arī MI un tā radītajai automatizētai lēmumu pieņemšanai ir nepieciešama liela datu apjoma apkopošana un apstrāde. Šie dati var nākt no pašas ierīces (bremžu siltums, degviela u. tml.) vai no apkārtējās vides. Piemēram, profilēšana ir process, kas var paļauties uz automatizētu lēmumu pieņemšanu atbilstoši iepriekš uzstādītiem modeļiem vai faktoriem.

Piemērs. Profilēšana un mērķtiecīga reklāma

Lielajos datos balstīta profilēšana ir saistīta ar tādu modeļu meklēšanu, kas atspoguļo "personības tipa īpašības", piemēram, kad tiešsaistes iepirkšanās uzņēmumi piedāvā produktus, kas jums var patikt, pamatojoties uz informāciju, kas savākta no iepriekš klienta iepirkumu grozā ievietotajiem produktiem. Jo vairāk datu, jo skaidrāka aina. Piemēram, viedtālrunis ir jaudīga aptaujas anketa, ko cilvēki apzināti un neapzināti aizpilda katrā lietojuma reizē.

Mūsdienu psihogrāfijā (zinātnē, kas pēta personību) tiek izmantota *OCEAN* metode, uz kuras pamata tā nosaka apskatāmo raksturu tipus. Rakstura "lielā piecinieka" dimensijas attiecas uz atklātību (cik cilvēks ir atvērts jaunajam),

984 Stuart Russel un Peter Norvig, *Artificial Intelligence: A Modern Approach (2nd ed.)*, 2003, Upper Saddle River, New Jersey: Prentice Hall, 27., 32.–58., 968.–972. lpp.; Stuart Russel un Peter Norvig, *Artificial Intelligence: A Modern Approach (3rd ed.)*, 2009, Upper Saddle River, New Jersey: Prentice Hall, 2. lpp.

apzinātību (kāda ir personas nosliece uz perfekcionismu), ekstraversiju (cik sabiedrisks ir cilvēks), laipnību (cik patīkams ir cilvēks) un neirotismu (cik ievainojams ir cilvēks). Šī informācija raksturo konkrēto personu, tās vajadzības un bailes, kā tā rīkosies u. tml. Pēc tam to papildina cita informācija par personu, kas iegūta no visiem pieejamajiem avotiem, no datu brokeriem, sociālajiem tīkliem (ieskaitot "patīk" pie ziņām un ievietotajiem fotoattēliem), tiešsaistē klausītās mūzikas vai GPS un izsekošanas datiem.

Pēc tam tiek salīdzināta to profilu masa, kas izveidoti, izmantojot lielo datu analīzes paņēmienus, lai identificētu līdzīgus modeļus un radītu personību kopas. Tāpēc informācija par noteiktu personību uzvedību un attieksmi ir apgriezta. Piekļūstot lielajiem datiem un tos lietojot, tiek apgriezts otrādi personības tests, un tagad tiek izmantota informācija par rīcību un attieksmi, lai aprakstītu indivīda personību. Apkopojot informāciju par "patīk" sociālajos tīklos, izsekojot datus, klausīto mūziku vai skatītās filmas, var iegūt skaidru priekšstatu par indivīda personību, ļaujot uzņēmumiem sniegt pielāgotu reklāmu un/vai informāciju atbilstoši šā cilvēka "personībai". Vissvarīgākais ir tas, ka šo informāciju var apstrādāt reāllaikā[985].

10.1.2. Līdzsvarojot lielo datu ieguvumus un riskus

Mūsdienu apstrādes paņēmieni ļauj apstrādāt lielas datu masas, ātri importēt jaunus datus, nodrošināt informācijas apstrādi reāllaikā īsā reaģēšanas posmā (pat sarežģītu pieprasījumu gadījumā), nodrošināt iespēju izpildīt vairākus un vienlaicīgus pieprasījumus, kā arī analizēt dažāda veida informāciju (fotoattēlus, tekstus vai skaitļus). Šīs tehnoloģiskās inovācijas ļauj reāllaikā strukturēt, apstrādāt un novērtēt datu un informācijas masas[986]. Eksponenciāli palielinot pieejamo un analizēto datu daudzumu, tagad var gūt rezultātus, kas mazāka mēroga analīzē nebūtu iespējami. Lielie dati ir palīdzējuši attīstīt jaunu uzņēmējdarbības jomu, kurā gan uzņēmumiem, gan patērētājiem var rasties jauni pakalpojumi. ES pilsoņu personas datu vērtība līdz

985 Apstrādes paņēmieni un jaunas programmatūras novērtē informāciju par to, kas cilvēkam patīk, ko viņš skatās, iepērkoties tiešsaistē, vai reāllaikā ieliek tiešsaistes iepirkumu grozā, un ļauj piedāvāt "produktus", kas varētu šo cilvēku interesēt, pamatojoties uz apkopoto informāciju.

986 Lielo datu apstrādes programmatūru izstrāde joprojām ir sākuma stadijā. Tomēr nesen tika izstrādātas analītiskas programmas, jo īpaši masveida datu un informācijas, kas saistīta ar personu darbībām, analīzei reāllaikā. Iespēja analizēt un apstrādāt lielos datus strukturēti ir radījusi jaunus profilēšanas un mērķtiecīgas reklāmas līdzekļus. Eiropas Komisija, Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai: Ceļā uz plaukstošu ekonomiku, kura balstīta uz datiem, COM(2014) 442 *final*, Brisele, 2014. gada 2. jūlijs; ES Komisijas faktu lapa par ES datu aizsardzības reformu un lielajiem datiem un Eiropas Padomes Vadlīnijas personu aizsardzībai attiecībā uz personas datu apstrādi lielo datu pasaulē, 2017. gada 23. janvāris, 2. lpp.

2020. gadam var pieaugt līdz gandrīz vienam triljonam EUR gadā[987]. Tāpēc lielie dati var piedāvāt jaunas **iespējas**, kas izriet no masveida datu novērtēšanas, sniedzot jaunu sociālu, ekonomisku vai zinātnisku ieskatu, kas var dot labumu gan indivīdiem, gan uzņēmumiem un valdībām[988].

Lielo datu analīze var atklāt modeļus starp dažādiem avotiem un datu kopām, sniedzot noderīgu informāciju tādās jomās kā zinātne un medicīna. Tas attiecas, piemēram, uz tādām jomām kā veselība, pārtikas nodrošinātība, intelektiskas transporta sistēmas, energoefektivitāte vai pilsētplānošana. Šo informācijas reāllaika analīzi var izmantot ieviesto sistēmu uzlabošanai. Pētījumos jaunu informāciju var gūt, apvienojot lielu daudzumu datu un statistiskos novērtējumus, jo īpaši disciplīnās, kurās līdz mūsdienām liels datu apjoms tika novērtēts tikai manuāli. Balstoties uz salīdzinājumiem ar pieejamās informācijas masu, var tikt izstrādātas jaunas individuāliem pacientiem pielāgotas procedūras. Uzņēmumi cer, ka lielo datu analīze sniegs viņiem konkurences priekšrocības, ļaus ietaupīt un radīs jaunas uzņēmējdarbības jomas, izmantojot tiešu, individualizētu klientu apkalpošanu. Valdības aģentūras cer panākt uzlabojumus krimināltiesību jomā. Komisijas Digitālā vienotā tirgus stratēģijā Eiropai ir atzīts uz datiem balstītu tehnoloģiju, pakalpojumu un lielo datu potenciāls kļūt par ekonomikas izaugsmes, inovāciju un digitalizācijas katalizatoru ES[989].

Tomēr lielie dati arī rada **riskus**, kas parasti saistīti ar tā "trīs V" atribūtiem – apstrādāto datu apjomu, ātrumu un dažādību (*volume, velocity, variety*). Apjoms apzīmē apstrādāto datu daudzumu, dažādība norāda uz datu veidu skaitu un atšķirīgumu, savukārt ātrums apzīmē datu apstrādes ātrumu. Konkrēti apsvērumi par datu aizsardzību rodas jo īpaši, ja lielo datu analīzi izmanto lielām datu kopām nolūkā iegūt jaunas un paredzamas zināšanas lēmumu pieņemšanai attiecībā uz indivīdiem un/vai grupām[990]. Ar lieliem datiem saistīti datu aizsardzības un privātuma riski ir uzsvērti

987 ES Komisijas faktu lapa par ES datu aizsardzības reformu un lielajiem datiem.

988 Starptautiskā Datu aizsardzības un privātuma komisāru konference (2014), Rezolūcija par lielajiem datiem un Eiropas Komisija, Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai: Ceļā uz plaukstošu ekonomiku, kura balstīta uz datiem, COM(2014) 442 *final*, Brisele, 2014. gada 2. jūlijs, 2. lpp.; ES Komisijas faktu lapa par ES datu aizsardzības reformu un lielajiem datiem un Eiropas Padomes Vadlīnijas personu aizsardzībai attiecībā uz personas datu apstrādi lielo datu pasaulē, 2017. gada 23. janvāris, 1. lpp.

989 Eiropas Parlamenta 2017. gada 14. marta rezolūcija par lielo datu ietekmi uz pamattiesībām – privātums, datu aizsardzība, nediskriminācija, drošība un tiesībaizsardzība (2016/2225(INI)).

990 Eiropas Padomes Konvencijas Nr. 108 konsultatīvā komiteja, Vadlīnijas personu aizsardzībai attiecībā uz personas datu apstrādi lielo datu pasaulē, 2017. gada 23. janvāris, 2. lpp.

EDAU un 29. panta darba grupas atzinumos, Eiropas Parlamenta rezolūcijās un Eiropas Padomes politikas dokumentos[991].

Pie riskiem var pieskaitīt lielo datu pretlikumīgu apstrādi, ko veic personas ar piekļuvei informācijas masai, manipulējot, diskriminējot vai apspiežot indivīdus vai īpašas sabiedrības grupas[992]. Ja tiek vākts, apstrādāts un novērtēts liels personu datu vai informācijas daudzums par indivīdu uzvedību, to izmantošana var izraisīt nopietnus pamattiesību un brīvību pārkāpumus, kas pārsniedz tiesības uz privātumu. Nav iespējams precīzi izmērīt, cik lielā mērā var tikt ietekmēts privātums un personas dati. Eiropas Parlaments konstatēja metodikas trūkumu, lai varētu veikt pierādījumos balstītu lielo datu kopējās ietekmes novērtējumu, taču ir pierādījumi, kas liecina, ka lielo datu analīzei var būt būtiska horizontāla ietekme gan publiskajā, gan privātajā sektorā[993].

Vispārīgajā datu aizsardzības regulā ir ietvertas normas par tiesības nebūt automatizēta lēmuma, tostarp profilēšanas, subjektam[994]. Privātuma problēma rodas gadījumos, kad tiesību iebilst īstenošanai nepieciešama cilvēka līdzdalība, ļaujot datu subjektiem paust savu viedokli un apstrīdēt lēmumu[995]. Tas var radīt grūtības nodrošināt pienācīgu personas datu aizsardzības līmeni, ja, piemēram, nav iespējama cilvēka līdzdalība vai algoritmi ir pārāk sarežģīti un iesaistīto datu apjoms ir pārāk liels, lai indivīdiem sniegtu noteiktu lēmumu pamatojumu un/vai iepriekšēju informāciju viņu piekrišanas saņemšanai. MI izmantošanas un automatizētas lēmumu pieņemšanas piemērs ir hipotēku piešķiršanas pieteikumu vai darbā pieņemšanas procesa jaunākās attīstības tendences. Pieteikumi tiek noraidīti vai atteikti, pamatojoties uz faktu, ka pieteikuma iesniedzēji neatbilst iepriekš noteiktiem parametriem vai faktoriem.

991 Skatīt, piemēram, EDAU (2015), *Kā risināt ar lielajiem datiem saistītās problēmas*, Atzinums 7/2015, Brisele, 2015. gada 19. novembris; EDAU (2016), *Pamattiesību saskaņota īstenošana lielo datu laikmetā*, Atzinums 8/2016, 2016. gada 23. septembris; Eiropas Parlamenta (2016) Rezolūcija par lielo datu ietekmi uz pamattiesībām – privātums, datu aizsardzība, nediskriminācija, drošība un tiesībaizsardzība P8_TA(2017)0076, Strasbūra, 2017. gada 14. marts; Eiropas Padomes Konvencijas Nr. 108 konsultatīvā komiteja, Vadlīnijas personu aizsardzībai attiecībā uz personas datu apstrādi lielo datu pasaulē, T-PD(2017)01, Strasbūra, 2017. gada 23. janvāris.

992 Starptautiskā Datu aizsardzības un privātuma komisāru konference (2014), Rezolūcija par lielajiem datiem.

993 Eiropas Parlamenta 2017. gada 14. marta rezolūcija par lielo datu ietekmi uz pamattiesībām — privātums, datu aizsardzība, nediskriminācija, drošība un tiesībaizsardzība (2016/2225(INI)).

994 Vispārīgā datu aizsardzības regula, 22. pants.

995 Turpat, 22. panta 3. punkts.

10.1.3. Ar datu aizsardzību saistītas problēmas

Runājot par datu aizsardzību, galvenie jautājumi skar, no vienas puses, apstrādāto personas datu apjomu un daudzveidību, un, no otras puses, apstrādi un tās rezultātus. Sarežģītu algoritmu un programmatūru ieviešana, lai masu datus pārveidotu par resursiem lēmumu pieņemšanas nolūkos, īpaši skar indivīdus un grupas, jo sevišķi profilēšanas vai marķēšanas gadījumos, un galu galā rada daudzas datu aizsardzības problēmas[996].

Pārziņu un apstrādātāju identifikācija un viņu atbildība

Lielie dati un MI rada vairākus jautājumus saistībā ar pārziņu un apstrādātāju identifikāciju un viņu atbildību: kurš ir datu īpašnieks situācijās, kad tiek vākts un apstrādāts tik liels datu apjoms? Kurš ir pārzinis, ja datus apstrādā intelektiskās ierīces un programmatūras? Kādi ir tieši katra apstrādes procesa dalībnieka pienākumi? Un kādiem nolūkiem var izmantot lielos datus?

Jautājums par atbildību MI kontekstā kļūs vēl sarežģītāks, kad MI pieņem lēmumu, kura pamatā ir datu apstrāde, ko tas pats ir izstrādājis. Vispārīgajā datu aizsardzības regulā ir sniegts datu pārziņa un apstrādātāja atbildības tiesiskais regulējums. Par personas datu nelikumīgu apstrādi ir atbildīgs datu pārzinis un datu apstrādātājs[997]. Mākslīgais intelekts un automatizēta lēmumu pieņemšana liek uzdot jautājumus, kurš atbild par pārkāpumiem, kas ietekmē datu subjektu privātumu, ja apstrādāto datu sarežģītību un daudzumu nevar precīzi noteikt. Ja MI un algoritmus uzskata par produktiem, rodas jautājums par personisko atbildību, ko reglamentē Vispārīgā datu aizsardzības regula, no vienas puses, un produktatbildību, ko regula nereglamentē, no otras puses[998]. Būtu nepieciešami atbildību reglamentējoši noteikumi, lai aizpildītu plaisu starp personisko atbildību un produktatbildību robotikas un MI jomā, tostarp, piemēram, automatizētu lēmumu pieņemšanu[999].

996 Eiropas Padomes Konvencijas Nr. 108 konsultatīvā komiteja, Vadlīnijas personu aizsardzībai attiecībā uz personas datu apstrādi lielo datu pasaulē, 2017. gada 23. janvāris, 2. lpp.

997 Vispārīgā datu aizsardzības regula, 77. –79. pants un 82. pants.

998 Eiropas Parlaments, Eiropas civiltiesību noteikumi par robotiku, Iekšpolitikas ģenerāldirektorāts, (2016. gada oktobris), 14. lpp.

999 Roberto Violas runa mediju seminārā par Eiropas tiesībām par robotiku Eiropas Parlamentā. (RUNA 16/02/2017); Eiropas Parlamenta paziņojums par pieprasījumu Komisijai priekšlikumam civiltiesiskās atbildības noteikumiem par robotiku un MI.

Ietekme uz datu aizsardzības principiem

Iepriekš aprakstītais lielo datu raksturs, analīze un izmantojums rada problēmas dažu Eiropas datu aizsardzības tiesību aktu tradicionālo pamatprincipu piemērošanā[1000]. Šādas problēmas galvenokārt ir saistītas ar likumības, datu minimizēšanas, nolūka ierobežojuma un pārredzamības principiem.

Saskaņā ar datu minimizēšanas principu personas datiem jābūt adekvātiem, atbilstošiem, un tajos ir jāietver tikai tas, kas nepieciešams tiem nolūkiem, kādiem tos apstrādā. Tomēr lielo datu uzņēmējdarbības modelis var būt datu minimizēšanas pretstats, jo prasa arvien vairāk datu, bieži vien neprecizētiem mērķiem.

Tas pats attiecas uz nolūka ierobežojuma principu, saskaņā ar kuru dati ir jāapstrādā noteiktiem nolūkiem, un tos nevar izmantot nolūkiem, kas nav savienojami ar sākotnējo vākšanas nolūku, izņemot gadījumus, kad šādai apstrādei ir juridiskais pamats, piemēram, bet ne tikai datu subjekta piekrišana (skatīt 4.1.1. iedaļu).

Visbeidzot, lielie dati rada problēmas attiecībā uz datu precizitātes principu, jo lielo datu lietotnēm ir tendence vākt datus no dažādiem avotiem, bez iespējas pārbaudīt un/vai uzturēt savākto datu precizitāti[1001].

Konkrēti noteikumi un tiesības

Vispārīgs noteikums joprojām nosaka, ka personas dati, ko apstrādā, izmantojot lielo datu analīzi, ietilpst datu aizsardzības tiesību aktu darbības jomā. Tomēr ES un EP tiesību aktos ir ieviesti īpaši noteikumi vai atkāpes konkrētiem gadījumiem saistībā ar algoritmiski sarežģītu datu apstrādi.

EP tiesiskajā regulējumā modernizētajā Konvencijā Nr. 108 datu subjektam tiek piešķirtas jaunas tiesības, lai lielo datu laikmetā būtu iespējams efektīvāk kontrolēt viņa vai viņas personas datus. Šāds piemērs ir modernizētās Konvencijas 9. panta 1. punkta a), c) un d) apakšpunkts par tiesībām nebūt tāda lēmuma subjektam, kas viņu būtiski ietekmē, kas pieņemts, pamatojoties tikai uz automatizētu datu apstrādi neņemot vērā viņa vai viņas uzskatus; tiesības pēc pieprasījuma saņemt informāciju par datu apstrādes pamatojumu, ja tiek piemēroti šādas apstrādes rezultāti, kā arī

1000 Eiropas Padome, *Vadlīnijas personu aizsardzībai attiecībā uz personas datu apstrādi lielo datu pasaulē*, T-PD (2017) 01, Strasbūra, 2017. gada 23. janvāris.

1001 EDAU (2016), *Pamattiesību saskaņota īstenošana lielo datu laikmetā*, Atzinums 8/2016, 2016. gada 23. septembris, 8. lpp.

tiesības iebilst. Citi modernizētās Konvencijas Nr. 108 noteikumi, jo īpaši par pārredzamību un papildu pienākumiem, papildina aizsardzības mehānismu, kas izveidots ar modernizēto Konvenciju Nr. 108 digitālo problēmu risināšanai.

Saskaņā ar ES tiesību aktiem, izņemot VDAR 23. pantā uzskaitītos gadījumus, ir jānodrošina visu personas datu apstrādes **pārredzamība**. Tas ir jo īpaši svarīgi saistībā ar interneta pakalpojumiem un citu sarežģītu automatizētu datu apstrādi, piemēram, algoritmu izmantošanu lēmumu pieņemšanā. Šādos gadījumos datu apstrādes sistēmu īpašībām ir jābūt tādām, lai datu subjekti varētu patiešām saprast, kas tiek darīts ar viņu datiem. Lai nodrošinātu godprātīgu un pārredzamu apstrādi, Vispārīgajā datu aizsardzības regulā ir noteikts, ka pārzinim ir jāsniedz datu subjektam jēgpilna informācija par automatizētā lēmumu pieņemšanā, tostarp profilēšanā, izmantoto loģiku[1002]. Eiropas Padomes Ministru komiteja savā Ieteikumā par vārda brīvības un privātās dzīves tiesību aizsardzību un veicināšanu, ievērojot tīkla neitralitāti, ieteica interneta pakalpojumu sniedzējiem "sniegt lietotājiem skaidru, pilnīgu un publiski pieejamu informāciju par jebkuru datu plūsmas pārvaldības praksi, kas var ietekmēt lietotāju piekļuvi saturam, lietojumprogrammām vai pakalpojumiem un to izplatīšanu"[1003]. Pārskati par interneta datu plūsmas pārvaldības praksi, ko sagatavojušas visu dalībvalstu kompetentās iestādes, ir jāsagatavo atklātā un pārredzamā veidā, un tiem jābūt pieejamiem sabiedrībai bez maksas[1004].

Datu pārziņiem ir pienākums **informēt** datu subjektus neatkarīgi no tā, vai dati ir vākti no viņiem, ne tikai sniedzot precīzu informāciju par vāktajiem datiem un paredzēto apstrādi (skatīt 6.1.1. iedaļu), bet arī attiecīgos gadījumos par automatizētas lēmumu pieņemšanas procesu esamību, sniedzot "jēgpilnu informāciju par tajā ietverto loģiku"[1005], šādu procesu mērķiem un iespējamajām sekām. Vispārīgajā datu aizsardzības regulā arī precizēts (tikai gadījumos, kad personas dati nav iegūti no datu subjekta), ka pārzinim nav pienākuma sniegt datu subjektam šādu informāciju, ja " šādas informācijas sniegšana nav iespējama vai tā prasītu nesamērīgi lielas pūles"[1006]. Tomēr, kā uzsvērts 29. panta darba grupas pamatnostādnēs par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas (ES) 2016/679

1002 Vispārīgā datu aizsardzības regula, 13. panta 2. punkta f) apakšpunkts.

1003 Eiropas Padomes Ministru komiteja (2016), Ministru komitejas Ieteikums CM/Rec(2016)1 dalībvalstīm par vārda brīvības un privātās dzīves tiesību aizsardzību un veicināšanu, ievērojot tīkla neitralitāti, 2016. gada 13. janvāris, 5.1. punkts.

1004 Turpat, 5.2. punkts.

1005 Vispārīgā datu aizsardzības regula, 13. panta 2. punkta f) apakšpunkts un 14. panta 2. punkta g) apakšpunkts.

1006 Turpat, 14. panta 5. punkta b) apakšpunkts.

nolūkiem, apstrādes sarežģītība pati par sevi nedrīkstētu atturēt datu pārzini sniegt datu subjektam skaidrus paskaidrojumus par mērķiem un datu apstrādē izmantoto analīzi[1007].

Uz datu subjektu tiesībām **piekļūt**, **labot** un **dzēst** savus personas datus, kā arī tiesības **ierobežot** apstrādi neattiecas līdzīgi atbrīvojumi. Taču datu pārzini var atbrīvot no pienākuma informēt datu subjektu par viņa personas datu labojumiem vai dzēšanu (skatīt 6.1.4. iedaļu), ja šāda paziņojuma sniegšana nebūtu "iespējama vai tā prasītu nesamērīgi lielas pūles"[1008].

Datu subjektiem saskaņā ar VDAR 21. pantu ir arī tiesības **iebilst** (skatīt 6.1.6. iedaļu) pret jebkādu viņu personas datu apstrādi, arī lielo datu analīzi. Kaut arī datu pārziņus var atbrīvot no šā pienākuma, ja viņi var pierādīt svarīgākas leģitīmās intereses, tomēr šāds atbrīvojums netiek piemērots, apstrādājot datus tiešās tirgvedības nolūkos.

Datu pārziņi var arī atsaukties uz īpašām atkāpēm no šīm tiesībām, apstrādājot personas datus arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos vai statistikas nolūkos[1009].

Saistībā ar **profilēšanu un automatizētu lēmumu pieņemšanu** VDAR ir ieviesti īpaši noteikumi: 22. panta 1. punktā noteikts, ka datu subjektam "ir tiesības nebūt tāda lēmuma subjektam, kura pamatā ir tikai automatizēta apstrāde (..), kas attiecībā uz datu subjektu rada tiesiskās sekas". Kā uzsvērts 29. panta darba grupas pamatnostādnēs, šajā pantā noteikts vispārīgs pilnībā automatizētu lēmumu pieņemšanas aizliegums[1010]. Datu pārziņus var atbrīvot no šāda aizlieguma ievērošanas tikai trīs konkrētos gadījumos – ja lēmums: 1) ir vajadzīgs, lai izpildītu līgumu starp datu subjektu un datu pārzini; 2) ir atļauts saskaņā ar Savienības vai valsts tiesību aktiem; vai 3) pamatojas uz nepārprotamu piekrišanu[1011].

1007 29. panta darba grupa, *Pamatnostādnes par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem*, WP 251, 2017. gada 3. oktobris, 14. lpp.

1008 Vispārīgā datu aizsardzības regula, 19. pants.

1009 Turpat, 89. panta 2. un 3. punkts.

1010 29. panta darba grupa, *Pamatnostādnes par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem*, WP 251, 2017. gada 3. oktobris, 9. lpp.

1011 Vispārīgā datu aizsardzības regula, 22. panta 2. punkts.

Individuāla kontrole

Lielo datu analīzes sarežģītības un pārredzamības trūkuma dēļ var būt nepieciešams pārskatīt idejas par individuālu personas datu kontroli. Tā ir jāpielāgo attiecīgajam sociālajam un tehnoloģiskajam kontekstam, ņemot vērā indivīdu zināšanu trūkumu. Tāpēc datu aizsardzībai attiecībā uz lielajiem datiem vajadzētu pieņemt plašāku datu izmantojuma kontroles ideju, saskaņā ar kuru individuālā kontrole kļūst par sarežģītāku procesu ar vairākkārtēju risku novērtējumu saistībā ar datu izmantošanu[1012].

Cik labs ir lielo datu izmantojums, atkarīgs no tā, cik labi ar tiem var paredzēt testējamo personu (vai patērētāju) vēlmes vai uzvedību. Pašreizējie prognozēšanas modeļi, kuru pamatā ir lielo datu analīze, tiek pastāvīgi pilnveidoti. Jaunākās attīstības tendences ietver ne tikai datu izmantošanu personību (piemēram, uzvedības un attieksmes) kategorizēšanai, bet arī uzvedības analīzei, analizējot balss modeļus un ziņojumu rakstīšanas intensitāti vai ķermeņa temperatūru. Visu šo informāciju var izmantot reāllaikā, salīdzinot ar informāciju, kas iegūta no lielo datu novērtējumiem, lai, piemēram, tikšanās laikā ar bankas pārstāvi novērtētu kredītspēju. Novērtējums netiek veikts, ņemot vērā indivīda, kurš piesakās kredīta saņemšanai, sasniegumus, bet drīzāk ņemot vērā uzvedības iezīmes, kas iegūtas, analizējot un novērtējot lielo datu sniegto informāciju, t. i., vai kandidāta balss tonis ir stingrs vai glaimojošs, kandidāta ķermeņa valodu vai ķermeņa temperatūru.

Profilēšana un mērķtiecīga reklāma ne vienmēr ir problēma, ja cilvēki **apzinās**, ka attiecībā uz viņiem tiek izmantota īpaši pielāgota reklāma. Profilēšana kļūst par problēmu, ja to izmanto, lai manipulētu ar indivīdiem, t.i., meklējot noteiktas personības vai cilvēku grupas politisko kampaņu nolūkiem. Piemēram, var uzrunāt neizlēmušu vēlētāju grupas, izmantojot politiskus ziņojumus, kas pielāgoti viņu "personībai" un uzskatiem. Cits jautājums varētu būt šādas profilēšanas izmantošana, lai noteiktām personām liegtu piekļuvi precēm un pakalpojumiem. Viens aizsardzības pasākums, kas var nodrošināt aizsardzību pret lielo datu un personiskās informācijas ļaunprātīgu izmantošanu, ir pseidonimizācija (skatīt 2.1.1. iedaļu)[1013]. Ja personas dati ir tiešām anonimizēti, t. i., nav informācijas, kas atstātu norādes uz datu subjektu, šie gadījumi neietilpst Vispārīgās datu aizsardzības regulas darbības jomā. Datu subjektu un personu piekrišana lielo datu apstrādei rada arī problēmas saistībā ar datu aizsardzības tiesību aktiem. Tas attiecas uz piekrišanu būt pielāgotas reklāmas un

1012 Eiropas Padomes Konvencijas Nr. 108 konsultatīvā komiteja, *Vadlīnijas personu aizsardzībai attiecībā uz personas datu apstrādi lielo datu pasaulē*, T-PD(2017)01, Strasbūra, 2017. gada 23. janvāris.

1013 Turpat, 2. lpp.

profilēšanas subjektam, ko var pamatot ar "klientu pieredzi", un piekrišanu izmantot lielu daudzumu personas datu, lai pilnveidotu un izstrādātu uz informāciju balstītus analītiskos rīkus. Izpratne vai nepietiekama informētība par lielo datu apstrādi rada vairākus jautājumus attiecībā uz līdzekļiem, ar kādiem datu subjekti var īstenot savas tiesības, ņemot vērā, ka lielo datu apstrāde var balstīties gan uz pseidonimizētu, gan uz anonimizētu informāciju, kam piemēro algoritmus. Lai gan Vispārīgā datu aizsardzības regula attiecas uz pseidonimizētiem datiem, anonimizētiem datiem to nepiemēro. Personīgo datu apstrādes individuāla kontrole un izpratne par to ir ļoti svarīga lielo datu analīzē, jo bez tās subjektiem nebūs skaidra priekšstata par to, kas ir datu pārzinis vai apstrādātājs, liedzot viņiem efektīvi īstenot savas tiesības.

10.2. Tīmekļi 2.0 un 3.0: sociālie tīkli un lietu internets

Svarīgākie aspekti

- Sociālās tīklošanās pakalpojumi (STP) ir tiešsaistes saziņas platformas, kas ļauj indivīdiem pievienoties līdzīgi domājošu lietotāju tīkliem vai izveidot tādus.
- Lietu internets ir priekšmetu savienošana ar internetu un priekšmetu savstarpēja savienošana.
- Datu subjektu piekrišana ir visizplatītākais juridiskais pamats datu pārziņu veiktai likumīgai datu apstrādei sociālajos tīklos.
- Sociālo tīklu lietotājus parasti aizsargā "mājsaimniecības atbrīvojums". Tomēr šo atkāpi var atcelt īpašos gadījumos.
- Sociālo tīklu pakalpojumu sniedzējus neaizsargā "mājsaimniecības atbrīvojums".
- Integrētajai datu aizsardzībai un datu aizsardzībai pēc noklusējuma ir izšķiroša nozīme, lai nodrošinātu datu drošību šajā jomā.

10.2.1. Tīmekļa 2.0 un 3.0 definēšana

Sociālās tīklošanās pakalpojumi

Sākotnēji internets bija iecerēts kā tīkls, ar ko savstarpēji savienot datorus un pārsūtīt ziņojumus ar ierobežotām datu apmaiņas iespējām, tīmekļa vietnēs piedāvājot

indivīdiem iespēju tikai pasīvi aplūkot to saturu[1014]. Tīmekļa 2.0 laikmetā internets pārtapa par forumu, kurā lietotāji mijiedarbojas, sadarbojas un ģenerē ievades datus. Šo laikmetu raksturo sociālās tīklošanās pakalpojumu ievērojamie panākumi un plaša izmantošana, kas šobrīd veido miljoniem cilvēku būtisku ikdienas dzīves sastāvdaļu.

Sociālās tīklošanās pakalpojumus (STP) jeb "sociālos medijus" var vispārīgi definēt kā "tiešsaistes saziņas platformas, ar kuru palīdzību lietotāji var pievienoties domubiedru tīkliem vai tādus veidot"[1015]. Lai pievienotos tīklam vai tādu izveidotu, personas tiek uzaicinātas sniegt personas datus un izveidot savu profilu. STP ļauj lietotājiem ģenerēt digitālo "saturu", sākot no fotogrāfijām un videoierakstiem līdz laikrakstu saitēm un personīgām ziņām, lai paustu savu viedokli. Izmantojot šīs tiešsaistes saziņas platformas, lietotāji var mijiedarboties un sazināties ar daudziem citiem lietotājiem. Svarīgi ir tas, ka lielākā daļa populāro STP neprasa reģistrācijas maksu. Tā vietā, lai pieprasītu lietotājiem maksāt par pievienošanos tīklam, STP pakalpojumu sniedzēji lielāko daļu ieņēmumu gūst no mērķtiecīgas reklāmas. Reklāmdevēji var lielā mērā gūt labumu no personiskās informācijas, kas ik dienas tiek atklāta šajās vietnēs. Ja ir informācija par lietotāja vecumu, dzimumu, atrašanās vietu un interesēm, reklāmdevējs ar savām reklāmām var sasniegt "īstos" cilvēkus.

Eiropas Padomes Ministru komiteja pieņēma Ieteikumu par cilvēktiesību aizsardzību attiecībā uz sociālās tīklošanās pakalpojumiem[1016], kur īpašā sadaļā aplūkota datu aizsardzība, un 2018. gadā tas tika papildināts ar vēl vienu ieteikumu par interneta starpnieku nozīmi un atbildību[1017].

Piemērs. Nora ir ļoti laimīga, jo viņas partneris ierosināja apprecēties. Viņa vēlas padalīties ar draugiem un ģimeni ar šo labo ziņu un nolemj sociālajā tīklā ievietot emocionālu ziņu, paužot savu prieku, un nomaina savu attiecību statusu uz "saderinājusies". Turpmākajās dienās, ierakstoties savā kontā, Nora redz kāzu kleitu un ziedu veikalu reklāmas. Kāpēc tā?

1014 Eiropas Komisija (2016), *Lietu interneta veicināšana Eiropā*, SWD(2016) 110 *final*.

1015 29. panta darba grupa (2009), *Atzinums 5/2009 par tiešsaistes sociālo tīklu veidošanu*, WP 163, 2009. gada 12. jūnijs, 4. lpp.

1016 Eiropas Padomes Ministru komiteja, Ministru komitejas Ieteikums CM/Rec(2012)4 dalībvalstīm par cilvēktiesību aizsardzību attiecībā uz sociālās tīklošanās pakalpojumiem, 2012. gada 4. aprīlis.

1017 Eiropas Padomes Ministru komiteja, Ministru komitejas Ieteikums CM/Rec(2018)2 dalībvalstīm par interneta starpnieku nozīmi un atbildību, 2018. gada 7. marts.

Veidojot sludinājumu vietnē *Facebook*, kāzu kleitu un ziedu uzņēmumi atlasīja noteiktus parametrus, lai šos sludinājumus redzētu tādi cilvēki kā Nora. Tā kā Noras profilā norādīts, ka viņa ir sieviete, saderinājusies, dzīvo Parīzē netālu no rajona, kurā atrodas kleitu un ziedu veikali, kuri bija ievietojuši šos sludinājumus, viņa tos uzreiz redz.

Lietu internets

Lietu internets (*IoT*) ir nākamais solis interneta attīstībā: tīmekļa 3.0 laikmets. Izmantojot *IoT*, ierīces var tikt savienotas un mijiedarboties ar citām ierīcēm ar interneta starpniecību. Tas ļauj ar komunikāciju tīklu palīdzību savstarpēji savienot objektus un cilvēkus, ziņot par viņu stāvokli un/vai par apkārtējās vides stāvokli[1018]. *IoT* un savienotās ierīces jau ir realitāte, un paredzams, ka nākamajos gados to skaits ievērojami palielināsies, radot un attīstot viedierīces, kas tālāk radīs viedās pilsētas, viedās mājas un viedos uzņēmumus.

Piemērs. *IoT* var būt īpaši lietderīgs veselības aprūpes jomā. Uzņēmumi jau ir izstrādājuši ierīces, sensorus un lietotnes, kas ļauj uzraudzīt pacienta veselību. Izmantojot valkājamu trauksmes pogu un citus bezvadu sensorus, kas izvietoti dažādās vietās mājā, ir iespējams izsekot vecāka gadagājuma cilvēku ikdienas gaitām vienatnē un nosūtīt brīdinājumus, ja viņu ikdienas grafikā atklāti nopietni traucējumi. Piemēram, gados vecāki cilvēki plaši izmanto kritiena detektorus. Šie sensori var precīzi konstatēt kritienus un par kritienu paziņot indivīda ārstam un/vai ģimenei.

Piemērs. Barselona ir viens no atzīstamākajiem viedās pilsētas piemēriem. Kopš 2012. gada pilsētā tiek ieviestas inovatīvas tehnoloģijas ar mērķi izveidot viedu sabiedriskā transporta, atkritumu apsaimniekošanas, autostāvvietu un ielu apgaismojuma sistēmu. Piemēram, lai uzlabotu atkritumu apsaimniekošanu, pilsētā izmanto viedās tvertnes. Tās ļauj uzraudzīt atkritumu līmeni, optimizējot savākšanas maršrutus. Kad tvertnes ir gandrīz pilnas, tās caur mobilo sakaru tīklu pārraida signālus, kas tiek nosūtīti uz programmatūras lietotni, kuru izmanto atkritumu apsaimniekošanas uzņēmums. Tādējādi

1018 Eiropas Komisija, Komisijas dienestu darba dokuments, *Lietu interneta veicināšana Eiropā*, SWD(2016) 110, 2016. gada 19. aprīlis.

uzņēmums var plānot labāko atkritumu savākšanas maršrutu, nosakot prioritāti un/vai organizējot tikai to atkritumu tvertņu savākšanu, kas faktiski ir jāiztukšo.

10.2.2. Līdzsvarojot ieguvumus un riskus

STP plašais pieaugums un panākumi pēdējos desmit gados liecina, ka tie sniedz **būtiskas priekšrocības**. Piemēram, mērķtiecīga reklāma (kā aprakstīts izceltajā piemērā) ir īpaši inovatīvs veids, kādā uzņēmumiem sasniegt auditoriju, piedāvājot viņiem konkretizētu tirgu. Atbilstošākas un interesantākas reklāmas rādīšana var arī būt patērētāju interesēs. Vēl svarīgāk ir tas, ka sociālās tīklošanās pakalpojumi un sociālie mediji var pozitīvi ietekmēt sabiedrību un pārmaiņu ieviešanu. Tie dod lietotājiem iespēju sazināties, mijiedarboties, organizēt grupas un pasākumus par viņus skarošiem jautājumiem.

Paredzams, ka arī *IoT* sniegs būtiskus ieguvumus ekonomikai, un tie ietilpst ES Digitālā vienotā tirgus attīstības stratēģijā. Tiek lēsts, ka 2020. gadā *IoT* savienojumu skaits palielināsies līdz sešiem miljardiem. Paredzams, ka šī savienojamības paplašināšana sniegs būtiskus ieguvumus ekonomikai, attīstot inovatīvus pakalpojumus un lietotnes, labāku veselības aprūpi, labāku izpratni par patērētāju vajadzībām un paaugstinātu efektivitāti.

Tajā pašā laikā, ņemot vērā milzīgo personiskās informācijas daudzumu, ko izveido sociālo mediju lietotāji un pēc tam apstrādā pakalpojumu sniedzēji, STP paplašināšanās rada **pieaugošas bažas** par veidiem, kā aizsargāt privātumu un personas datus. STP var apdraudēt tiesības uz privāto dzīvi un tiesības uz vārda brīvību. Šādi draudi var būt: "juridisko un procesuālo aizsardzības pasākumu neesamība attiecībā uz procesiem, kas var izraisīt lietotāju izslēgšanu; bērnu un jauniešu nepietiekama aizsardzība pret kaitīgu saturu vai uzvedību; citu personu tiesību neievērošana; privātumam draudzīgu noklusējuma iestatījumu neesamība; pārredzamības trūkums attiecībā uz nolūkiem, kādiem personas dati tiek vākti un apstrādāti"[1019]. Eiropas datu aizsardzības tiesībās ir mēģināts reaģēt uz privātuma/datu aizsardzības problēmām, ko rada sociālie mediji. Tādi principi kā piekrišana, privātums/integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma, kā arī indivīdu tiesības ir īpaši svarīgi sociālo mediju un tīklošanās pakalpojumu kontekstā.

1019 Eiropas Padome, Ieteikums Rec(2012)4 dalībvalstīm par cilvēktiesību aizsardzību attiecībā uz sociālās tīklošanās pakalpojumiem, 2012. gada 4. aprīlis.

IoT kontekstā lielais personas datu apjoms, ko ģenerē dažādas savstarpēji savienotas ierīces, rada arī privātuma un datu aizsardzības riskus. Lai arī pārredzamība ir svarīgs Eiropas datu aizsardzības tiesību princips, pieslēgto ierīču skaita dēļ ne vienmēr ir skaidrs, kurš spēj vākt datus, piekļūt tiem un izmantot no *IoT* ierīcēm vāktos datus[1020]. Tomēr saskaņā ar ES un EP tiesību aktiem pārredzamības princips uzliek pienākumu pārziņiem skaidrā un saprotamā veidā informēt datu subjektus par to, kā tiek izmantoti viņu dati. Skartās personas ir skaidri jāinformē par riskiem, noteikumiem, aizsardzības pasākumiem un tiesībām attiecībā uz viņu personas datu apstrādi. *IoT* savienotās ierīces, kā arī dažādās apstrādes darbības un iesaistītie dati varētu arī radīt problēmas attiecībā uz prasību saņemt nepārprotamu un apzinātu piekrišanu datu apstrādei, ja šāda apstrāde balstīta piekrišanā. Indivīdiem bieži trūkst izpratne par šādas apstrādes tehniskajām funkcijām un līdz ar to par viņu piekrišanas sekām.

Vēl viena būtiska problēma ir drošība, ņemot vērā, ka savienotās ierīces ir īpaši neaizsargātas pret drošības riskiem. Savienotajām ierīcēm ir atšķirīgs drošības līmenis. Tā kā tās darbojas ārpus standarta IT infrastruktūras, tām var trūkt atbilstošas apstrādes jaudas un uzglabāšanas iespēju, lai mitinātu drošības programmatūras vai izmantotu tādas metodes kā šifrēšana, pseidonimizācija vai anonimizēšana, lai aizsargātu lietotāju personisko informāciju.

Piemērs. Vācijā regulatori nolēma aizliegt rotaļlietu, kas pieslēgta internetam, ņemot vērā nopietnās bažas par rotaļlietas ietekmi uz bērnu privātās dzīves neaizskaramību. Regulatori uzskatīja, ka ar internetu savienota lelle ar nosaukumu *Cayla* būtībā ir slēpta spiegošanas ierīce. Lelle darbojās, nosūtot bērna, kurš ar to spēlējās, audio jautājumus uz lietotni digitālā ierīcē, kas to pārtulkoja tekstā un meklēja atbildi internetā. Pēc tam lietotne nosūtīja atbildi lellei, kura to norunāja bērnam. Ar šo lelli bērna, kā arī tuvējo pieaugušo saziņa varēja tikt ierakstīta un pārsūtīta uz lietotni. Ja leļļu ražotāji nebūtu pieņēmuši atbilstošus aizsardzības pasākumus, jebkurš varētu lelli izmantot sarunu noklausīšanai.

1020 Eiropas Datu aizsardzības uzraudzītājs (2017), *Izprast lietu internetu*.

10.2.3. Ar datu aizsardzību saistītas problēmas

Piekrišana

Eiropā personas datu apstrāde ir likumīga tikai tad, ja to atļauj Eiropas datu aizsardzības tiesību akti. STP pakalpojumu sniedzējiem likumīgu datu apstrādes pamatu parasti nodrošina datu subjektu piekrišana. Piekrišana ir jāsniedz labprātīgi, tai jābūt konkrētai, apzinātai un nepārprotamai (skatīt 4.1.1. iedaļu)[1021]. "Labprātīgi sniegta" būtībā nozīmē, ka datu subjektiem jābūt spējīgiem izdarīt īstenu un patiesu izvēli. Piekrišana ir "konkrēta" un "apzināta", ja tā ir saprotama, skaidri un precīzi norāda uz pilnīgu datu apstrādes tvērumu, nolūkiem un sekām. Sociālo mediju kontekstā ir apšaubāms, vai piekrišana ir labprātīgi sniegta, konkrēta un apzināta par visiem apstrādes veidiem, ko veic STP operators un trešās personas.

Piemērs. Lai pievienotos un piekļūtu STP, indivīdiem bieži vien ir jāpiekrīt dažāda veida personas datu apstrādei, turklāt nereti viņiem netiek sniegtas nepieciešamās specifikācijas vai alternatīvas. Kā piemēru var minēt nepieciešamību sniegt piekrišanu uz uzvedību balstītas reklāmas saņemšanai, lai reģistrētos STP. Kā 29. panta darba grupa atzīmē atzinumā par piekrišanas definīciju, "daži sociālie tīkli ir kļuvuši ļoti populāri, dažas lietotāju grupas (piemēram, pusaudži) ir ar mieru saņemt paradumorientētas reklāmas piedāvājumus, lai izvairītos no riska, ka viņiem daļēji varētu tikt liegta sociālā saziņa. Ir jānodrošina iespēja, lai lietotāji varētu sniegt labprātīgu un konkrētu piekrišanu paradumorientētas reklāmas saņemšanai neatkarīgi no piekļuves sociālajiem tīkliem"[1022].

Saskaņā ar Vispārīgo datu aizsardzības regulu bērnu, kuri ir jaunāki par 16 gadiem, personas datus principā nedrīkst apstrādāt, balstoties uz viņu piekrišanu[1023]. Ja ir nepieciešama piekrišana apstrādei, to sniedz bērna vecāki vai aizbildnis. Bērni ir pelnījuši īpašu aizsardzību, jo viņi, iespējams, ir mazāk informēti par riskiem un sekām saistībā ar datu apstrādi. Tas ir ļoti svarīgi sociālo mediju kontekstā, jo bērni ir neaizsargātāki pret noteiktām šādu mediju izmantošanas negatīvajām sekām, piemēram, iebiedēšanu tiešsaistē, kibervajāšanu vai identitātes zādzību.

1021 Vispārīgā datu aizsardzības regula, 4. un 7. pants; modernizētā Konvencija Nr. 108, 5. pants.

1022 29. panta darba grupa (2011), *Atzinums 15/2011 par jēdziena "piekrišana" definīciju*, WP 187, 2011. gada 13. jūlijs, 18. lpp.

1023 Skatīt Vispārīgās datu aizsardzības regulas 8. pantu. ES dalībvalstis var likumā noteikt zemāku vecuma robežu, taču ne zemāku par 13 gadiem.

Drošība un privātums/integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma

Personas datu apstrādei ir raksturīgi drošības riski, ņemot vērā pastāvīgo drošības pārkāpuma iespēju, kas noved pie apstrādāto personas datu nejaušas vai nelikumīgas iznīcināšanas, nozaudēšanas, izmaiņām, neatļautas piekļuves vai izpaušanas. Saskaņā ar Eiropas tiesību aktiem datu aizsardzības jomā pārziņiem un apstrādātājiem ir pienākums ieviest attiecīgus tehniskos un organizatoriskos pasākumus, lai novērstu jebkādu neatļautu iejaukšanos datu apstrādes darbībās. Šis pienākums ir jāievēro arī sociālās tīklošanās pakalpojumu sniedzējiem, uz kuriem attiecas Eiropas datu aizsardzības noteikumi.

Privātuma/integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma principi uzliek pārziņiem pienākumu uzturēt viņu produktu integrētu drošību un automātiski piemērot atbilstošus privātuma un datu aizsardzības iestatījumus. Tas nozīmē, ka tad, kad persona nolemj pievienoties sociālajam tīklam, pakalpojumu sniedzējs, iespējams, automātiski nepadara visu informāciju par jauno pakalpojuma lietotāju pieejamu visiem tā lietotājiem. Pievienojoties pakalpojumam, noklusējuma privātuma un datu aizsardzības iestatījumiem vajadzētu būt tādiem, lai informācija būtu pieejama tikai personas izvēlētajiem kontaktiem. Piekļuves paplašināšanai personām ārpus šā saraksta jābūt iespējamai tikai pēc tam, kad lietotājs ir veicis darbības, lai manuāli mainītu noklusējuma privātuma un datu aizsardzības iestatījumus. Tam var būt ietekme arī gadījumos, kad notiek datu pārkāpums, lai gan ir ieviesti drošības pasākumi. Šādos gadījumos pakalpojumu sniedzējiem jāinformē skartie lietotāji, ja tas, iespējams, rada lielu risku datu subjekta tiesībām un brīvībām[1024].

Privātums/integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma ir īpaši svarīgi STP kontekstā, jo papildus neatļautas piekļuves riskiem, kas saistīti ar lielāko daļu apstrādes veidu, personiskās informācijas apmaiņa sociālajos medijos rada papildu drošības riskus. Bieži tas notiek tāpēc, ka indivīdiem trūkst izpratnes par to, *kurš* var piekļūt viņu informācijai un kā šie cilvēki to var izmantot. Plašas sociālo mediju izmantošanas rezultātā ir palielinājies identitātes zādzību gadījumu un cietušo skaits.

1024 Turpat, 34. pants.

Piemērs. Identitātes zādzība ir parādība, kad persona iegūst informāciju, datus vai dokumentus, kas pieder citai personai (cietušajam), un pēc tam izmanto šo informāciju, uzdodoties par cietušo nolūkā iegūt preces un pakalpojumus uz cietušā vārda. Piemēram, Pauls, kuram ir konts sociālo mediju vietnē. Pauls ir skolotājs un aktīvs savas kopienas loceklis, ekstraverts, un viņu īpaši nesatrauc viņa sociālo mediju konta privātuma un datu aizsardzības iestatījumi. Viņam ir garš kontaktu saraksts, kurā nereti ietilpst cilvēki, kurus viņš ne vienmēr pazīst personīgi. Tā kā viņš strādā lielā skolā un ir diezgan iecienīts skolas futbola komandas treneris, viņš domā, ka šie cilvēki, visticamāk, ir skolēnu vecāki vai draugi. Paula e-pasta adrese un dzimšanas diena viņa sociālo mediju kontā ir redzamas. Turklāt Pauls regulāri ievieto sava suņa Tobija fotogrāfijas, pievienojot tādus parakstus kā "Es ar Tobiju mūsu rīta skrējienā". Pauls nav sapratis, ka viens no populārākajiem drošības jautājumiem, aizsargājot savu e-pastu vai mobilā tālruņa kontu, ir "kā sauc jūsu mīluli". Izmantojot Paula sociālo mediju profilā pieejamo informāciju, Niks viegli uzlauž Paula kontu.

Privātpersonu tiesības

STP sniedzējiem ir jāievēro indivīdu tiesības (skatīt 6.1. iedaļu), tostarp tiesības būt informētiem par apstrādes nolūku un to, kā personas datus var izmantot tiešās tirgvedības nolūkos. Indivīdiem ir jābūt tiesībām piekļūt personas datiem, ko viņi izveidojuši sociālās tīklošanās platformā, un pieprasīt to dzēšanu. Pat ja indivīdi ir piekrituši personas datu apstrādei un augšupielādējuši informāciju tiešsaistē, viņiem ir jābūt iespējai lūgt "tikt aizmirstiem", ja viņi vairs nevēlas saņemt sociālās tīklošanās pakalpojumus. Turklāt tiesības uz datu pārnesamību ļauj lietotājiem saņemt to personas datu kopijas, ko viņi ir snieguši sociālās tīklošanās pakalpojumu sniedzējam, strukturētā, plaši izmantotā un mašīnlasāmā formātā un pārnest savus datus no viena sociālās tīklošanās pakalpojumu sniedzēja citam[1025].

Pārziņi

Sarežģīts jautājums, kas bieži rodas sociālo mediju kontekstā, ir jautājums par to, kas ir pārzinis, proti, kas ir tā persona, kurai ir pienākums un atbildība nodrošināt datu aizsardzības noteikumu ievērošanu. Sociālās tīklošanās pakalpojumu sniedzējus uzskata par pārziņiem saskaņā ar Eiropas datu aizsardzības tiesību aktiem.

1025 Vispārīgā datu aizsardzības regula, 21. pants.

Tas ir acīmredzami, ņemot vērā "pārziņa" plašo definīciju un faktu, ka šie pakalpojumu sniedzēji nosaka indivīdu kopīgi izmantoto personas datu apstrādes nolūku un līdzekļus. Saskaņā ar ES tiesību aktiem, ja pārziņi piedāvā pakalpojumus datu subjektiem ES, tiem ir jāievēro Vispārīgās datu aizsardzības regulas noteikumi, pat ja viņi nav reģistrēti ES.

Vai tomēr sociālās tīklošanās pakalpojumu lietotājus var uzskatīt arī par pārziņiem? Ja indivīdi apstrādā personas datus "tikai personiska vai mājsaimnieciska pasākuma gaitā", datu aizsardzības noteikumus nepiemēro. Eiropas datu aizsardzības tiesību aktos to sauc par "mājsaimniecības atbrīvojumu". Tomēr dažos gadījumos uz sociālās tīklošanās pakalpojuma lietotāju mājsaimniecības atbrīvojums neattiecas.

Lietotāji tiešsaistē brīvprātīgi dalās ar savu personisko informāciju. Taču tiešsaistē kopīgotā informācija bieži ietver citu personu personisko informāciju.

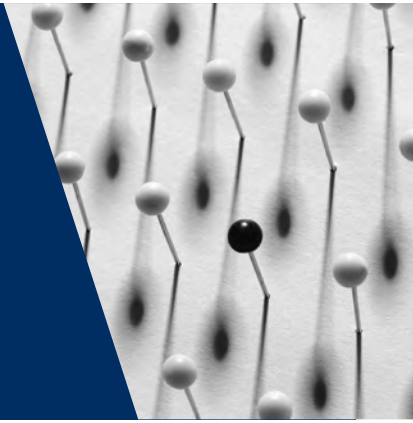
> Piemērs. Paulam ir konts ļoti populārā sociālās tīklošanās platformā. Pauls plāno kļūt par aktieri un savā kontā ievieto fotoattēlus, videoklipus un ziņas, aprakstot viņa aizraušanos ar mākslu. Popularitāte ir svarīga viņa nākotnei. Tāpēc viņš ir izlēmis, ka profilam jābūt pieejamam ne tikai tuviem kontaktiem, bet visiem interneta lietotājiem neatkarīgi no tā, vai viņi ir tīkla dalībnieki. Vai Pauls var ievietot fotogrāfijas un videoklipus ar sevi un ar savu draudzeni Sāru bez viņas piekrišanas? Sāra kā sākumskolas skolotāja cenšas savu privāto dzīvi nodalīt no darba devēja, skolēniem un viņu vecākiem. Iedomājieties gadījumu, kad Sāra, kura neizmanto sociālos tīklus, no viņu kopīgā drauga Nika uzzina, ka tiešsaistē ievietota viņas fotogrāfija ballītē ar Paulu. Šādā gadījumā uz Paula datu apstrādi neattieksies ES tiesību akti, jo uz viņu attiecas "mājsaimniecības atbrīvojums".

Tomēr lietotājiem joprojām ir svarīgi izprast un apzināties, ka, augšupielādējot informāciju par citām personām bez viņu piekrišanas, var tikt pārkāptas šo personu tiesības uz privāto dzīvi un datu aizsardzību. Pat tad, ja tiek piemērots mājsaimniecības atbrīvojums, piemēram, ja lietotājam ir profils, kas tiek publiskots tikai viņa izvēlētajam kontaktpersonu sarakstam, par personiskas informācijas publicēšanu par citiem lietotājiem šis lietotājs joprojām var tikt saukts pie atbildības. Kaut arī datu aizsardzības noteikumi netiktu piemēroti, ja piemēro mājsaimniecības atbrīvojumu, atbildība varētu iestāties, piemērojot citus valsts noteikumus, piemēram, par neslavas celšanu vai personības aizskārumu. Visbeidzot, mājsaimniecības atbrīvojumi aizsargā tikai

STP lietotājus, jo uz datu pārziņiem un apstrādātājiem, kuri nodrošina līdzekļus šādai privātai apstrādei, attiecas ES datu aizsardzības tiesību akti[1026].

Pēc Direktīvas par privāto dzīvi un elektronisko komunikāciju reformas datu aizsardzības, privātuma un drošības noteikumi, kas saskaņā ar pašreizējo tiesisko regulējumu ir piemērojami telekomunikāciju pakalpojumu sniedzējiem, būtu piemērojami arī mašīnas-mašīnas komunikācijai un elektronisko komunikāciju pakalpojumiem, tostarp, piemēram, *over-the-top* pakalpojumiem.

1026 Turpat, 18. apsvērums.



Papildliteratūra

1. nodaļa

Araceli Mangas, M. (ed.) (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*, Vienna, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C. 'Four fundamental rights: finding the balance', *International Data Privacy Law*, 6. sēj., Nr. 3, 195.–209. lpp.

González Fuster, G. and 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.(1) sēj., 73.–82. lpp.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. and Nouwt, S. (Eds.) (2009), *Reinventing Data Protection*, Springer.

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'.

Kranenborg, H. (2015), "Google and the Right to be Forgotten", *European Data Protection Law Review*, 1. sēj., Nr. 1, 70.–79. lpp.

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. sēj., Nr. 3, 569.–597. lpp.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press.

Kokott, J. and 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. sēj., Nr. 4, 222.–228. lpp.

EDRi, *An introduction to data protection*, Brussels.

Frowein, J. un Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. un Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Munich, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. and Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Munich, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. and Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. and Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Brussels, Emile Bruylant.

Simitis, S. (1997), 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?', *Neue Juristische Wochenschrift*, Nr. 5, 281.–288. lpp.

Warren, S. and Brandeis, L. (1890), 'The right to privacy', *Harvard Law Review,* 4. sēj., Nr. 5, 193.–220. lpp.

White, R. and Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

2. nodaļa

Acquisty, A., and Gross R. (2009), 'Predicting Social Security numbers from public data', *Proceedings of the National Academy of Science*, 2009. gada 7. jūlijs.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., and Blondel V. D. (2013), 'Unique in the Crowd: the Privacy Bounds of Human Mobility', *Nature Scientific Reports*, 3. sēj., 2013.

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. and 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. sēj., Nr. 6, 1701.–1777. lpp.

Samarati, P. and 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. sēj., Nr. 5, 557.–570. lpp.

Tinnefeld, M., Buchner, B. and Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Munich, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*.

3.–6. nodaļa

Brühann, U. (2012), 'Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr' in: Grabitz, E., Hilf, M. and Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Munich, 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. and Kaye, J. (2010), 'Revoking consent: a 'blind spot' in data protection law?', *Computer Law & Security Review*, 26. sēj., Nr. 3, 273.–283. lpp.

Dammann, U. and Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. and Papakonstantinou, V. (2012), 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis', *Computers & Law Magazine of SCL*, 22. sēj., Nr. 6, 1.–5. lpp.

De Hert, P. and 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. sēj., Nr. 2, 130.–142. lpp.

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. sēj., Nr. 2, 473.–506. lpp.

FRA (European Union Agency for Fundamental Rights) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, Publications Office of the European Union (Publications Office).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conference edition), Vienna, *FRA*.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxembourg, Publications Office.

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. and Saxby, S. (2011), '30 years on – The review of the Council of Europe Data Protection Convention 108', *Computer Law & Security Review*, 27. sēj., Nr. 3, 223.–231. lpp.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, Privacy Impact Assessment.

7. nodaļa

Eiropas Datu aizsardzības uzraudzītājs (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. and 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.

29. panta darba grupa (2005), *Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta vienotu interpretāciju*.

8. nodaļa

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.

Europol (2012), *Data Protection at Europol*, Luxembourg, Publications Office.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, The Hague, Eurojust.

De Hert, P. and Papakonstantinou, V. (2012), 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis', *Computers & Law Magazine of SCL*, 22. sēj., Nr. 6, 1.–5. lpp.

Drewer, D. and Ellermann, J. (2012), 'Europol's data protection framework as an asset in the fight against cybercrime', *ERA Forum*, 13. sēj., Nr. 3, 381.–395. lpp.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlin, Springer.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and 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. sēj., Nr. 5, 722.–776. lpp.

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. nodaļa

Büllesbach, A., Gijrath, S., Poullet, Y. and Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. and Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and 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. sēj., Nr. 5, 722.–776. lpp.

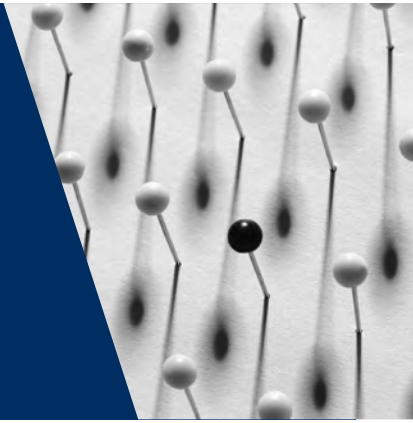
Rosemary, J. and Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

10. nodaļa

El Emam, K. and Álvarez, C. (2015), 'A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques', *International Data Privacy Law*, 5. sēj., Nr. 1, 73.–87. lpp.

Mayer-Schönberger, V. and Cate, F. (2013), 'Notice and consent in a world of Big Data', *International Data Privacy Law*, 3. sēj., Nr. 2, 67.–73. lpp.

Rubistein, I. (2013), 'Big Data: The End of Privacy or a New Beginning?', *International Data Privacy Law*, 3. sēj., Nr. 2, 74.–87. lpp.



Judikatūra

Eiropas Cilvēktiesību tiesas judikatūras izlase

Piekļuve personas datiem
Gaskin pret Apvienoto Karalisti, Nr. 10454/83, 1989. gada 7. jūlijs
Godelli pret Itāliju, Nr. 33783/09, 2012. gada 25. septembris
K.H. un citi pret Slovākiju, Nr. 32881/04, 2009. gada 28. aprīlis
Leander pret Zviedriju, Nr. 9248/81, 1987. gada 26. marts
M.K. pret Franciju, Nr. 19522/09, 2013. gada 18. aprīlis
Odièvre pret Franciju [GC], Nr. 42326/98, 2003. gada 13. februāris

Datu aizsardzības līdzsvarošana ar vārda brīvību un tiesībām uz informāciju
Axel Springer AG pret Vāciju [GC], Nr. 39954/08, 2012. gada 7. februāris
Bohlen pret Vāciju, Nr. 53495/09, 2015. gada 19. februāris
Coudec un Hachette Filipacchi Associés pret Franciju [GC], Nr. 40454/07, 2015. gada 10. novembris
Magyar Helsinki Bizottság pret Ungāriju [GC], Nr. 18030/11, 2016. gada 8. novembris
Müller un citi pret Šveici, Nr. 10737/84, 1988. gada 24. maijs
Vereinigung bildender Künstler pret Austriju, Nr. 68345/01, 2007. gada 25. janvāris
Von Hannover pret Vāciju (Nr. 2) [GC], Nr. 40660/08 un Nr. 60641/08, 2012. gada 7. februāris
Satakunnan Markkinapörssi Oy un Satamedia Oy pret Somiju [GC], Nr. 931/13, 2017. gada 27. jūnijs

Datu aizsardzības līdzsvarošana ar reliģiskās pārliecības brīvību
Sinan Işık pret Turciju, Nr. 21924/05, 2010. gada 2. februāris

Problēmas datu aizsardzībai tiešsaistē
K.U. pret Somiju, Nr. 2872/02, 2008. gada 2. decembris

Datu subjekta piekrišana
Elberte pret Latviju, Nr. 61243/08, 2015. gada 13. janvāris
Sinan Işık pret Turciju, Nr. 21924/05, 2010. gada 2. februāris
Y pret Turciju, Nr. 648/10, 2015. gada 17. februāris

Sarakste
Amann pret Šveici [GC], Nr. 27798/95, 2000. gada 16. februāris
Association for European Integration and Human Rights un Ekimdzhiev pret Bulgāriju, Nr. 62540/00, 2007. gada 28. jūnijs
Bernh Larsen Holding AS un citi pret Norvēģiju, Nr. 24117/08, 2013. gada 14. marts
Cemalettin Canli pret Turciju, Nr. 22427/04, 2008. gada 18. novembris
D.L. pret Bulgāriju, Nr. 7472/14, 2016. gada 19. maijs
Dalea pret Franciju, Nr. 964/07, 2010. gada 2. februāris
Gaskin pret Apvienoto Karalisti, Nr. 10454/83, 1989. gada 7. jūlijs
Haralambie pret Rumāniju, Nr. 21737/03, 2009. gada 27. oktobris
Khelili pret Šveici, Nr. 16188/07, 2011. gada 18. oktobris
Leander pret Zviedriju, Nr. 9248/81, 1987. gada 26. marts
Malone pret Apvienoto Karalisti, Nr. 8691/79, 1984. gada 2. augusts
Rotaru pret Rumāniju [GC], Nr. 28341/95, 2000. gada 4. maijs
S. un Marper pret Apvienoto Karalisti [GC], Nr. 30562/04 un Nr. 30566/04, 2008. gada 4. decembris
Shimovolos pret Krieviju, Nr. 30194/09, 2011. gada 21. jūnijs
Silver un citi pret Apvienoto Karalisti, Nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 1983. gada 25. marts
The Sunday Times pret Apvienoto Karalisti, Nr. 6538/74, 1979. gada 26. aprīlis

Sodāmības reģistri
Aycaguer pret Franciju, Nr. 8806/12, 2017. gada 22. jūnijs
B.B. pret Franciju, Nr. 5335/06, 2009. gada 17. decembris
Brunet pret Franciju, Nr. 21010/10, 2014. gada 18. septembris
M.K. pret Franciju, Nr. 19522/09, 2013. gada 18. aprīlis
M.M. pret Apvienoto Karalisti, Nr. 24029/07, 2012. gada 13. novembris

Datu drošība
Haralambie pret Rumāniju, Nr. 21737/03, 2009. gada 27. oktobris
K.H. un citi pret Slovākiju, Nr. 32881/04, 2009. gada 28. aprīlis

DNS datubāzes
S. un Marper pret Apvienoto Karalisti [GC], Nr. 30562/04 un Nr. 30566/04, 2008. gada 4. decembris

GPS dati
Uzun pret Vāciju, Nr. 35623/05, 2010. gada 2. septembris

Veselības dati
Avilkina un citi pret Krieviju, Nr. 1585/09, 2013. gada 6. jūnijs
Biriuk pret Lietuvu, Nr. 23373/03, 2008. gada 25. novembris
I pret Somiju, Nr. 20511/03, 2008. gada 17. jūlijs
L.H. pret Latviju, Nr. 52019/07, 2014. gada 29. aprīlis
L.L. pret Franciju, Nr. 7508/02, 2006. gada 10. oktobris
M.S. pret Zviedriju, Nr. 20837/92, 1997. gada 27. augusts
Szuluk pret Apvienoto Karalisti, Nr. 36936/05, 2009. gada 2. jūnijs
Y pret Turciju, Nr. 648/10, 2015. gada 17. februāris
Z pret Somiju, Nr. 22009/93, 1997. gada 25. februāris

Identitāte
Ciubotaru pret Moldovu, Nr. 27138/04, 2010. gada 27. aprīlis
Godelli pret Itāliju, Nr. 33783/09, 2012. gada 25. septembris
Odièvre pret Franciju [GC], Nr. 42326/98, 2003. gada 13. februāris

Informācija par profesionālo darbību
G.S.B. pret Šveici, Nr. 28601/11, 2015. gada 22. decembris
M.N. un citi pret Sanmarīno, Nr. 28005/12, 2015. gada 7. jūlijs
Michaud pret Franciju, Nr. 12323/11, 2012. gada 6. decembris
Niemietz pret Vāciju, Nr. 13710/88, 1992. gada 16. decembris

Sakaru pārtveršana
Amann pret Šveici [GC], Nr. 27798/95, 2000. gada 16. februāris
Brito Ferrinho Bexiga Villa-Nova pret Portugāli, Nr. 69436/10, 2015. gada 1. decembris
Copland pret Apvienoto Karalisti, Nr. 62617/00, 2007. gada 3. aprīlis
Halford pret Apvienoto Karalisti, Nr. 20605/92, 1997. gada 25. jūnijs
Iordachi un citi pret Moldovu, Nr. 25198/02, 2009. gada 10. februāris
Kopp pret Šveici, Nr. 23224/94, 1998. gada 25. marts
Liberty un citi pret Apvienoto Karalisti, Nr. 58243/00, 2008. gada 1. jūlijs
Malone pret Apvienoto Karalisti, Nr. 8691/79, 1984. gada 2. augusts

Mustafa Sezgin Tanrıkulu pret Turciju, Nr. 27473/06, 2017. gada 18. jūlijs
Pruteanu pret Rumāniju, Nr. 30181/05, 2015. gada 3. februāris
Szuluk pret Apvienoto Karalisti, Nr. 36936/05, 2009. gada 2. jūnijs

Saistību turētāju pienākumi
B.B. pret Franciju, Nr. 5335/06, 2009. gada 17. decembris
I pret Somiju, Nr. 20511/03, 2008. gada 17. jūlijs
Mosley pret Apvienoto Karalisti, Nr. 48009/08, 2011. gada 10. maijs

Personas dati
Amann pret Šveici [GC], Nr. 27798/95, 2000. gada 16. februāris
Uzun pret Vāciju, Nr. 35623/05, 2010
Bernh Larsen Holding AS un citi pret Norvēģiju, Nr. 24117/08, 2013. gada 14. marts

Fotogrāfijas
Sciacca pret Itāliju, Nr. 50774/99, 2005. gada 11. janvāris
Von Hannover pret Vāciju, Nr. 59320/00, 2004. gada 24. jūnijs

Tiesības tikt aizmirstam
Segerstedt-Wiberg un citi pret Zviedriju, Nr. 62332/00, 2006. gada 6. jūnijs
Satakunnan Markkinapörssi Oy un Satamedia Oy pret Somiju [GC], Nr. 931/13, 2017. gada 27. jūnijs

Tiesības iebilst
Leander pret Zviedriju, Nr. 9248/81, 1987. gada 26. marts
M.S. pret Zviedriju, Nr. 20837/92, 1997. gada 27. augusts
Mosley pret Apvienoto Karalisti, Nr. 48009/08, 2011. gada 10. maijs
Rotaru pret Rumāniju [GC], Nr. 28341/95, 2000. gada 4. maijs
Sinan Işık pret Turciju, Nr. 21924/05, 2010. gada 2. februāris

Sensitīvu personas datu kategorijas
Brunet pret Franciju, Nr. 21010/10, 2014. gada 18. septembris
I pret Somiju, Nr. 20511/03, 2008. gada 17. jūlijs
Michaud pret Franciju, Nr. 12323/11, 2012. gada 6. decembris
S. un Marper pret Apvienoto Karalisti [GC], Nr. 30562/04 un Nr. 30566/04, 2008. gada 4. decembris

Uzraudzība un piespiedu izpilde (dažādu dalībnieku, tostarp datu aizsardzības iestāžu, nozīme)
I pret Somiju, Nr. 20511/03, 2008. gada 17. jūlijs
K.U. pret Somiju, Nr. 2872/02, 2008. gada 2. decembris
Von Hannover pret Vāciju, Nr. 59320/00, 2004. gada 24. jūnijs
Von Hannover pret Vāciju (Nr. 2) [GC], Nr. 40660/08 un Nr. 60641/08, 2012. gada 7. februāris

Novērošanas metodes
Allan pret Apvienoto Karalisti, Nr. 48539/99, 2002. gada 5. novembris
Association for European Integration and Human Rights un Ekimdzhiev pret Bulgāriju, Nr. 62540/00, 2007. gada 28. jūnijs
Bărbulescu pret Rumāniju [GC], Nr. 61496/08, 2017. gada 5. septembris
D.L. pret Bulgāriju, Nr. 7472/14, 2016. gada 19. maijs
Dragojević pret Horvātiju, Nr. 68955/11, 2015. gada 15. janvāris
Karabeyoğlu pret Turciju, Nr. 30083/10, 2016. gada 7. jūnijs
Klass un citi pret Vāciju, Nr. 5029/71, 1978. gada 6. septembris
Rotaru pret Rumāniju [GC], Nr. 28341/95, 2000. gada 4. maijs
Szabó un Vissy pret Ungāriju, Nr. 37138/14, 2016. gada 12. janvāris
Taylor-Sabori pret Apvienoto Karalisti, Nr. 47114/99, 2002. gada 22. oktobris
Uzun pret Vāciju, Nr. 35623/05, 2010. gada 2. septembris
Versini-Campinchi un Crasnianski pret Franciju, Nr. 49176/11, 2016. gada 16. jūnijs
Vetter pret Franciju, Nr. 59842/00, 2005. gada 31. maijs
Vukota-Bojić pret Šveici, Nr. 61838/10, 2016. gada 18. oktobris
Roman Zakharov pret Krieviju [GC], Nr. 47143/06, 2015. gada 4. decembris

Videonovērošana
Köpke pret Vāciju, Nr. 420/07, 2010. gada 5. oktobris
Peck pret Lielbritāniju, Nr. 44647/98, 2003. gada 28. janvāris

Balss paraugi
Wisse pret Franciju, Nr. 71611/01, 2005. gada 20. decembris
P.G. un J.H. pret Apvienoto Karalisti, Nr. 44787/98, 2001. gada 25. septembris

Eiropas Savienības Tiesas judikatūras izlase

Ar Datu aizsardzības direktīvu saistīta judikatūra

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA "'Rīgas satiksme"*, 2017. gada 4. maijs
[Likumīgas apstrādes princips; trešās personas likumīgo interešu īstenošana]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce pret Salvatore Manni*, 2017. gada 9. marts
[Tiesības uz personas datu dzēšanu; tiesības iebilst pret apstrādi]

Apvienotās lietas C-203/15 un C-698/15 *Tele2 Sverige AB pret Post- och telestyrelsen* un *Secretary of State for the Home Department pret Tom Watson un citiem* [GC], 2016. gada 21. decembris
[Elektroniskās komunikācijas konfidencialitāte; elektronisko komunikāciju pakalpojumu sniedzēji; pienākums, kas saistīts ar vispārīgu un nekritisku datu plūsmas un atrašanās vietas saglabāšanu; iepriekš nav pārskatīta tiesā vai neatkarīgā administratīvā iestādē; Eiropas Savienības Pamattiesību harta; savietojamība ar ES tiesību aktiem]

C-582/14, *Patrick Breyer pret Bundesrepublik Deutschland*, 2016. gada 19. oktobris
["Personas datu" definīcija; interneta protokola adreses; datu saglabāšana, ko veic tiešsaistes plašsaziņas pakalpojumu sniedzējs; valsts tiesību akti, kas liedz ņemt vērā pārziņa likumīgās intereses]

C-362/14, *Maximillian Schrems pret Datu aizsardzības komisāru* [GC], 2015. gada 6. oktobris
[Likumīgas apstrādes princips; pamattiesības; lēmuma par drošības zonu spēkā neesamība; neatkarīgu uzraudzības iestāžu pilnvaras]

C-230/14, *Weltimmo s. r. o. pret Nemzeti Adatvédelmi és Információszabadság Hatóság*, 2015. gada 1. oktobris
[Dalībvalstu uzraudzības iestāžu pilnvaras]

C-201/14 *Smaranda Bara un citi pret Casa Națională de Asigurări de Sănătate un citiem*, 2015. gada 1. oktobris
[Tiesības tikt informētam par personas datu apstrādi]

C-212/13, *František Ryneš pret Úřad pro ochranu osobních údajů*, 2014. gada 11. decembris
[“Datu apstrādes” un “pārziņa” jēdziens]

C-473/12 *Institut professionnel des agents immobiliers (IPI) pret Geoffrey Englebert un citiem*, 2013. gada 7. novembris
[Tiesības tikt informētam par personas datu apstrādi]

T-462/12 R, *Pilkington Group Ltd pret Eiropas Komisiju*, Vispārējās tiesas priekšsēdētāja rīkojums, 2013. gada 11. marts

C-342/12, *Worten – Equipamentos para o Lar SA pret Autoridade para as Condições de Trabalho (ACT)*, 2013. gada 30. maijs

[Jēdziens “personas dati”; darba laika uzskaite; datu kvalitātes principi un datu apstrādes likumības kritēriji; par darba apstākļu uzraudzību atbildīgās valsts iestādes piekļuve; darba devēja pienākums darīt pieejamu darba laika uzskaiti, lai ar to nekavējoties varētu iepazīties]

Apvienotās lietas C-293/12 un C-594/12 *Digital Rights Ireland Ltd pret Minister for Communications, Marine and Natural Resources un citiem* un *Kärntner Landesregierung un citiem* [GC], 2014. gada 8. aprīlis
[ES primāro tiesību pārkāpšana ar Datu saglabāšanas direktīvu; likumīga apstrāde; nolūka un glabāšanas ierobežojums]

C-288/12, *Eiropas Komisija pret Ungāriju* [GC], 2014. gada 8. aprīlis
[Valsts datu aizsardzības uzraudzītāja atcelšanas no amata likumība]

Apvienotās lietas C-141/12 un C-372/12, *YS pret Minister voor Immigratie, Integratie en Asiel* un *Minister voor Immigratie, Integratie en Asiel pret M un S*, 2014. gada 17. jūlijs
[Datu subjekta piekļuves tiesību apjoms; personu aizsardzība attiecībā uz personas datu apstrādi; jēdziens “personas dati”; uzturēšanās atļaujas pieprasītāja dati un juridiskā analīze, kas ietverti pārvaldes dokumentā, kurš ir lēmuma projekts; Eiropas Savienības Pamattiesību harta]

C-131/12, *Google Spain SL un Google Inc. pret Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014. gada 13. maijs
[Meklētājprogrammu pakalpojumu sniedzēju pienākums pēc datu subjekta lūguma atturēties no personas datu uzrādīšanas meklēšanas rezultātos; Datu aizsardzības direktīvas piemērojamība; jēdziens "datu apstrāde"; "pārziņu" nozīme; datu aizsardzības līdzsvarošana ar vārda brīvību; tiesības tikt aizmirstam]

C-614/10, *Eiropas Komisija pret Austrijas Republiku* [GC], 2012. gada 16. oktobris
[Valsts uzraudzības iestādes neatkarība]

Apvienotās lietas C-468/10 un C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) un Federación de Comercio Electrónico y Marketing Directo (FECEMD) pret Administración del Estado*, 2011. gada 24. novembris.
[Datu aizsardzības direktīvas 7. panta f) punkta – "citu likumīgā intereses" – pareiza īstenošana valsts tiesībās]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) pret Netlog NV*, 2012. gada 16. februāris
[Sociālās tīklošanās pakalpojumu sniedzēju pienākums novērst tīkla lietotāju nelikumīgu mūzikas un audiovizuālo darbu izmantošanu]

C-70/10, *Scarlet Extended SA pret Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011. gada 24. novembris
[Informācijas sabiedrība; autortiesības; internets; vienādranga programmatūras; interneta pakalpojumu sniedzēji; elektronisko komunikāciju filtrēšanas sistēmas ieviešana, lai novērstu apmaiņu ar datnēm, ar kurām tiek pārkāptas autortiesības; vispārējā pienākuma pārraudzīt pārsūtīto informāciju neesamība]

C-543/09, *Deutsche Telekom AG pret Bundesrepublik Deutschland*, 2011. gada 5. maijs
[Atjaunotas piekrišanas nepieciešamība]

Apvienotās lietas C-92/09 un C-93/09 *Volker und Markus Schecke GbR un Hartmut Eifert pret Land Hessen* [GC], 2010. gada 9. novembris
[Jēdziens "personas dati"; juridiskā pienākuma publicēt personas datus par dažu ES lauksaimniecības fondu atbalsta saņēmējiem samērīgums]

C-553/07, *College van burgemeester en wethouders van Rotterdam pret M. E. E. Rijkeboer*, 2009. gada 7. maijs
[Datu subjekta piekļuves tiesības]

C-518/07, *Eiropas Komisija pret Bundesrepublik Deutschland* [GC], 2010. gada 9. marts
[Valsts uzraudzības iestādes neatkarība]

C-73/07, *Tietosuojavaltuutettu pret Satakunnan Markkinapörssi Oy un Satamedia Oy* [GC], 2008. gada 16. decembris
["Žurnālistikas darbības" jēdziens Datu aizsardzības direktīvas 9. panta nozīmē]

C-524/06, *Heinz Huber pret Bundesrepublik Deutschland* [GC], 2008. gada 16. decembris
[Datu par ārvalstniekiem turēšanas statistikas reģistrā likumība]

C-275/06, *Productores de Música de España (Promusicae) pret Telefónica de España SAU* [GC], 2008. gada 29. janvāris
[Jēdziens "personas dati"; interneta piekļuves sniedzēju pienākums atklāt intelektuālā īpašuma aizsardzības apvienībai KaZaA tīmekļa datņu koplietošanas platformas lietotāju identitāti]

C-101/01, *Kriminālprocess pret Bodil Lindqvist*, 2003. gada 6. novembris
[Īpašu kategoriju personas dati]

Apvienotās lietas C-465/00, C-138/01 un C-139/01 *Rechnungshof pret Österreichischer Rundfunk un citi* un *Christa Neukomm un Jospeh Lauermann pret Österreichischer Rundfunk*, 2003. gada 20. maijs
[Juridiskā pienākuma publicēt personas datus par noteiktu ar publisko sektoru saistītu iestāžu kategoriju darbinieku algām samērīgums]

C-434/16, *Peter Nowak pret Data Protection Commissioner*, ģenerāladvokātes Kokotes (Kokott) secinājumi, 2017. gada 20. jūlijs
[Personas datu jēdziens; piekļuve saviem pārbaudes darba izlabotajam eksemplāram; eksaminētāja labojumi]

C-291/12, *Michael Schwarz pret Stadt Bochum*, 2013. gada 17. oktobris
[Lūgums sniegt prejudiciālu nolēmumu; brīvības, drošības un tiesiskuma telpa; biometriskā pase; pirkstu nospiedumi; juridiskais pamats; samērīgums]

Ar Direktīvu (ES) 2016/681 saistītā judikatūra

Tiesas (virspalātas) atzinums 1/15, 2017. gada 26. jūlijs

[Juridiskais pamats; Nolīguma starp Kanādu un Eiropas Savienību projekts par pasažieru datu reģistra datu nosūtīšanu un apstrādi; nolīguma projekta savietojamība ar LESD 16. pantu un Eiropas Savienības Pamattiesību hartas 7. un 8. pantu un 52. panta 1. punktu]

Ar Eiropas Savienības iestāžu datu aizsardzības regulu saistītā judikatūra

C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) pret Eiropas Pārtikas nekaitīguma iestādi (EFSA), Eiropas Komisiju*, 2015. gada 16. jūlijs

[Piekļuve dokumentiem]

C-28/08 P, *Eiropas Komisija pret The Bavarian Lager Co. Ltd.* [GC], 2010. gada 29. jūnijs

[Piekļuve dokumentiem]

Ar Direktīvu 2002/58/EK saistītā judikatūra

C-536/15 *Tele2 (Netherlands) BV un citi pret Autoriteit Consument en Markt (AMC)*, 2017. gada 15. marts

[Nediskriminācijas princips; personas datu par abonentiem nodošana saistībā ar telefona uzziņu dienestu un abonentu sarakstu pakalpojumu sniegšanu; abonenta piekrišana; izšķiršana atkarībā no dalībvalsts, kurā tiek sniegti publiski pieejami telefona izziņu dienestu un abonentu sarakstu pakalpojumi]

Apvienotās lietas C-203/15 un C-698/15 *Tele2 Sverige AB pret Post- och telestyrelsen* un *Secretary of State for the Home Department pret Tom Watson un citiem* [GC], 2016. gada 21. decembris

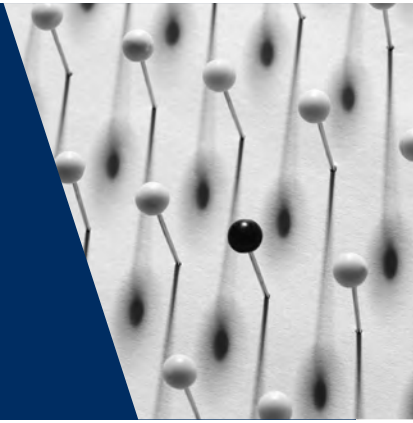
[Elektroniskās komunikācijas konfidencialitāte; elektronisko komunikāciju pakalpojumu sniedzēji; pienākums, kas saistīts ar vispārīgu un nekritisku datu plūsmas un atrašanās vietas saglabāšanu; iepriekš nav pārskatīta tiesā vai neatkarīgā administratīvā iestādē; Eiropas Savienības Pamattiesību harta; savietojamība ar ES tiesību aktiem]

C-70/10, *Scarlet Extended SA pret Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011. gada 24. novembris

[Informācijas sabiedrība; autortiesības; internets; vienādranga programmatūras; interneta pakalpojumu sniedzēji; elektronisko komunikāciju filtrēšanas sistēmas ieviešana, lai novērstu apmaiņu ar datnēm, ar kurām tiek pārkāptas autortiesības; vispārējā pienākuma pārraudzīt pārsūtīto informāciju neesamība]

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB pret Perfect Communication Sweden AB*, 2012. gada 19. aprīlis

[Autortiesības un blakustiesības; datu apstrāde internetā; ekskluzīvo tiesību aizskārums; audiogrāmatas, kas, izmantojot interneta piekļuves nodrošinātāja piešķirto IP adresi, padarītas pieejamas sabiedrībai ar FTP servera starpniecību internetā; tiesas rīkojums interneta piekļuves nodrošinātājam izpaust IP adreses lietotāja vārdu vai nosaukumu un adresi]



Rādītājs

Eiropas Savienības Tiesas judikatūra

Eiropas Cilvēktiesību tiesas judikatūra

Valstu tiesu judikatūra

Liela daļa informācijas par Eiropas Savienības Pamattiesību aģentūru ir pieejama internetā. Tai var piekļūt *FRA* tīmekļa vietnē: fra.europa.eu

Plašāka informācija par Eiropas Cilvēktiesību tiesas judikatūru ir pieejama tiesas tīmekļa vietnē: echr.coe.int. *HUDOC* meklēšanas portāls nodrošina piekļuvi spriedumiem un lēmumiem angļu un/vai franču valodā, tulkojumiem citās valodās, judikatūras kopsavilkumiem, paziņojumiem presei un citai informācijai par tiesas darbu (https://hudoc.echr.coe.int).

Kā saņemt Eiropas Padomes izdevumus

Eiropas Padomes izdevniecība publicē darbus visās organizācijas kompetences jomās, tostarp cilvēktiesību, tiesību zinātnes, veselības, ētikas, sociālo lietu, vides, izglītības, kultūras, sporta, jaunatnes un arhitektūras mantojuma jomā. Grāmatas un elektroniskās publikācijas no plašā kataloga var pasūtīt internetā (http://book.coe.int).

Virtuālajā lasītavā lietotāji bez maksas var iepazīties ar tikko publicēto svarīgāko darbu fragmentiem un dažu oficiālu dokumentu pilniem tekstiem.

Informācija par Eiropas Padomes konvencijām, kā arī to pilni teksti ir pieejami Līgumu biroja tīmekļa vietnē: http://conventions.coe.int/

Kā sazināties ar ES

Klātienē

Visā Eiropas Savienībā ir simtiem *Europe Direct* informācijas centru. Sev tuvākā centra adresi varat atrast tīmekļa lapā https://europa.eu/european-union/contact_lv.

Pa tālruni vai e-pastu

Europe Direct ir dienests, kas atbild uz jūsu jautājumiem par Eiropas Savienību. Ar šo dienestu varat sazināties šādi:
– pa bezmaksas tālruni: 00 800 6 7 8 9 10 11 (daži operatori par šiem zvaniem var iekasēt maksu);
– pa šādu parasto tālruņa numuru: +32 22999696;
– pa e-pastu, izmantojot šo tīmekļa lapu: https://europa.eu/european-union/contact_lv

Kā atrast informāciju par ES

Internetā

Informācija par Eiropas Savienību visās oficiālajās ES valodās ir pieejama portālā *Europa*: https://europa.eu/european-union/index_lv

ES publikācijas

ES bezmaksas un maksas publikācijas varat lejupielādēt vai pasūtīt šeit: https://op.europa.eu/lv/publications. Vairākus bezmaksas publikāciju eksemplārus varat saņemt, sazinoties ar *Europe Direct* vai tuvāko informācijas centru (sk. https://europa.eu/european-union/contact_lv).

ES tiesību akti un ar tiem saistītie dokumenti

Ar visu ES juridisko informāciju, arī kopš 1951. gada pieņemtajiem ES tiesību aktiem visās oficiālajās valodās, varat iepazīties vietnē *EUR-Lex*: http://eur-lex.europa.eu

ES atvērtie dati

ES atvērto datu portāls (http://data.europa.eu/lv) dod piekļuvi ES datu kopām. Datus var lejupielādēt un bez maksas izmantot kā komerciāliem, tā nekomerciāliem mērķiem.

doi:10.2811/828873 TK-05-17-225-LV-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

Straujā informācijas tehnoloģiju attīstība ir saasinājusi nepieciešamību pēc stabila personas datu aizsardzības regulējuma, tiesībām, kuras aizsargā gan Eiropas Savienības (ES), gan Eiropas Padomes (EP) instrumenti. Šo svarīgo tiesību aizsardzība rada jaunas un būtiskas problēmas, jo tehnoloģiju attīstība paplašina tādu jomu robežas kā novērošana, sakaru pārtveršana un datu glabāšana. Šī rokasgrāmata ir paredzēta, lai iepazīstinātu ar šo jauno tiesību jomu praktizējošus juristus, kuri nespecializējas datu aizsardzībā. Šeit ir sniegts pārskats par ES un EP piemērojamiem tiesiskajiem regulējumiem. Tajā arī skaidrota būtiskā judikatūra, sniedzot kopsavilkumu gan par Eiropas Savienības Tiesas, gan par Eiropas Cilvēktiesību tiesas svarīgākajiem nolēmumiem. Turklāt šeit ir sniegti hipotētiski scenāriji, kas praktiski ilustrē šajā nepārtraukti mainīgajā jomā radušos dažādus jautājumus.

***FRA* – EIROPAS SAVIENĪBAS PAMATTIESĪBU AĢENTŪRA**
Schwarzenbergplatz 11, 1040 Vīne, Austrija
Tālr. +43 158030-0 – Fakss +43 158030-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

EIROPAS CILVĒKTIESĪBU TIESA
EIROPAS PADOME
67075 Strasbūra *Cedex*, Francija
Tālr. +33 (0) 3 88 41 20 18 – Fakss +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int – twitter.com/ECHR_CEDH

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS
Rue Wiertz 60, 1047 Brisele, Beļģija
Tālr. +32 2 283 19 00
edps.europa.eu – edps@edps.europa.eu – twitter.com/EU_EDPS

Eiropas Savienības Publikāciju birojs

ISBN 978-92-871-9828-0 (Eiropas Padome)
ISBN 978-92-9461-557-2 (*FRA*)