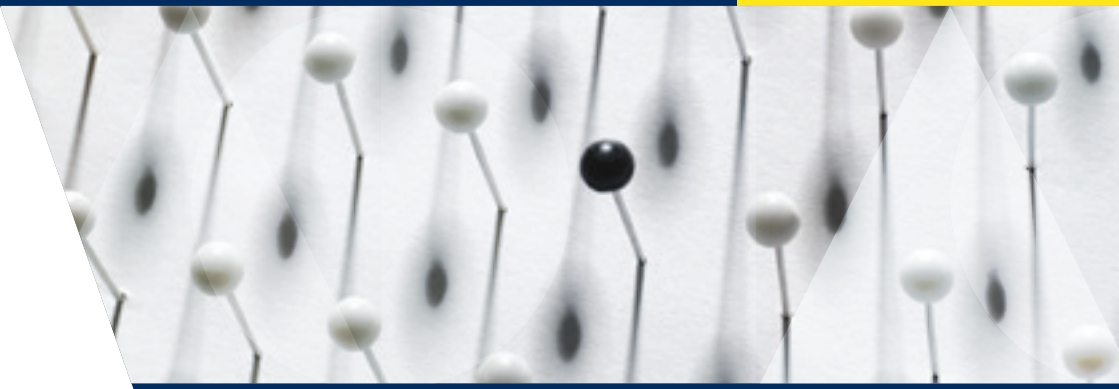
ROKASGRĀMATA



Rokasgrāmata par Eiropas tiesību aktiem datu aizsardzības jomā

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

Šīs rokasgrāmatas manuskripts pabeigts 2014. gada aprīlī.
Atjauninājumi nākotnē būs pieejami *FRA* tīmekļa vietnē fra.europa.eu, Eiropas Padomes tīmekļa vietnē http://coe.int/dataprotection un Eiropas Cilvēktiesību tiesas tīmekļa vietnē *Case-Law*, izvēlnē http://echr.coe.int

Europe Direct dienests jums palīdzēs rast atbildes uz jautājumiem par Eiropas Savienību

Bezmaksas tālruņa numurs (*):

00 800 6 7 8 9 10 11

(*) Informāciju sniedz bez maksas, tāpat arī lielākā daļa zvanu ir bezmaksas (izņemot dažus operatorus, viesnīcas vai taksofonus).

Foto: © iStockphoto

Papildu informācija par Eiropas Savienību ir pieejama portālā *Europa* (http://europa.eu).

Kataloga dati ir atrodami šīs publikācijas beigās.

Luksemburga: Eiropas Savienības Publikāciju birojs, 2015. gads

ISBN 978-92-871-9942-3 (Eiropas Padome)
ISBN 978-92-9239-337-3 (*FRA*)
doi:10.2811/54847

Printed in Belgium

IESPIESTS UZ PAPĪRA, KAS BALINĀTS BEZ ELEMENTĀRA HLORA (*ECF*)

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

Rokasgrāmata par Eiropas tiesību aktiem datu aizsardzības jomā

Priekšvārds

Šo rokasgrāmatu par Eiropas tiesību aktiem datu aizsardzības jomā ir kopīgi sagatavojušas Eiropas Savienības Pamattiesību aģentūra (FRA) un Eiropas Padome kopā ar Eiropas Cilvēktiesību tiesas Reģistru. Tā ir trešā juridisko rokasgrāmatu sērijā, ko kopīgi sagatavojušas FRA un Eiropas Padome. 2011. gada martā tika sagatavota pirmā rokasgrāmata par Eiropas nediskriminēšanas tiesību aktiem, bet 2013. gada jūnijā otrā rokasgrāmata – par Eiropas tiesību aktiem, kuri attiecas uz patvērumu, robežām un imigrāciju.

Mēs esam nolēmuši turpināt savu sadarbību par ļoti aktuālu tēmu, kas mūs visus skar ik dienu, proti, personas datu aizsardzību. Eiropā darbojas viena no spēcīgākajām aizsardzības sistēmām šajā jomā, kuras pamatā ir Eiropas Padomes 108. konvencija, Eiropas Savienības (ES) instrumenti, kā arī Eiropas Cilvēktiesību tiesas (ECT) un Eiropas Savienības Tiesas (Tiesas) prakse.

Šīs rokasgrāmatas mērķis ir padziļināt izpratni un uzlabot zināšanas par datu aizsardzības noteikumiem Eiropas Savienības un Eiropas Padomes dalībvalstīs, būt par galveno orientieri, pie kā lasītāji var vērsties. Tā ir paredzēta profesionāliem juristiem bez specializācijas, tiesnešiem, valstu datu aizsardzības iestādēm un citām personām, kuras strādā datu aizsardzības jomā.

Līdz ar Lisabonas līguma stāšanos spēkā 2009. gada decembrī ES Pamattiesību harta kļuva juridiski saistoša, un ar to tiesības uz personas datu aizsardzību tika paaugstinātas, iegūstot atsevišķu pamattiesību statusu. Labāka sapratne par Eiropas Padomes 108. konvenciju un ES instrumentiem, kas nobruģēja ceļu datu aizsardzībai Eiropā, kā arī par Tiesas un ECT praksi ir būtiska pamattiesību aizsardzībai.

Mēs vēlamies pateikties Ludviga Bolcmaņa Cilvēktiesību Institūtam par tā ieguldījumu šīs rokasgrāmatas sagatavošanā. Tāpat mēs vēlamies izteikt pateicību Eiropas Datu aizsardzības uzraudzītāja birojam par tā atsauksmēm projekta sagatavošanas laikā. Mēs jo īpaši pateicamies Eiropas Komisijas datu aizsardzības nodaļai par tās atbalstu šīs rokasgrāmatas sagatavošanas laikā.

Philippe Boillat

Eiropas Padomes Cilvēktiesību
un juridisko lietu ģenerāldirektorāta
ģenerāldirektors

Morten Kjaerum

Eiropas Savienības
Pamattiesību aģentūras
direktors

Saturs

Abreviatūras un akronīmi

108. konvencija	Eiropas Padomes Konvencija par personu aizsardzību attiecībā uz personas datu automātisko [automatizēto] apstrādi
ANO	Apvienoto Nāciju Organizācija
AUI	Apvienotās uzraudzības iestāde
BCR	saistošs korporatīvais noteikums
CCTV	slēgta kontūra televīzija
CETS	Eiropas Padomes Līgumu sērija
CIS	Muitas informācijas sistēma
CRM	Klientu attiecību pārvaldība
C-SIS	Centrālā Šengenas informācijas sistēma
EAW	Eiropas apcietināšanas orderis
EBTA	Eiropas Brīvās tirdzniecības asociācija
ECK	Eiropas Cilvēktiesību konvencija
ECT	Eiropas Cilvēktiesību tiesa
EDAU	Eiropas Datu aizsardzības uzraudzītājs
EEZ	Eiropas Ekonomikas zona
EK	Eiropas Kopiena
ENISA	Eiropas Tīklu un informācijas drošības aģentūra
ENU	*Europol* valstu vienība
EP	Eiropas Padome
ES	Eiropas Savienība
ESAO	Ekonomiskās sadarbības un attīstības organizācija
ESMA	Eiropas Vērtspapīru un tirgu iestāde
eTEN	Transeiropas Telekomunikāciju tīkli
eu-LISA	ES Aģentūra lielapjoma IT sistēmu darbības pārvaldībai *brīvības, drošības un tiesiskuma telpā*

EuroPriSe	Eiropas privātuma zīmogs
FRA	Eiropas Savienības Pamattiesību aģentūra
GPS	Globālā pozicionēšanas (vietnoteices) sistēma
Harta	Eiropas Savienības Pamattiesību harta
LES	Līgums par Eiropas Savienību
LESD	Līgums par Eiropas Savienības darbību
N-SIS	Valstu Šengenas informācijas sistēma
NVO	Nevalstiska organizācija
PIN	Personas identifikācijas numurs
PNR	Pasažieru datu reģistrs
SEPA	Vienotā *euro* maksājumu telpa
SIS	Šengenas informācijas sistēma
SWIFT	Vispasaules Starpbanku finanšu telekomunikāciju sabiedrība
Tiesa	Eiropas Savienības Tiesa (pirms 2009. gada decembra to dēvēja par Eiropas Kopienu Tiesu, EKT)
VCD	Vispārējā cilvēktiesību deklarācija
VIS	Vīzu informācijas sistēma

Kā lietot šo rokasgrāmatu

Šajā rokasgrāmatā ir sniegts pārskats par tiesību aktiem, kas piemērojami datu aizsardzībai saistībā ar Eiropas Savienību (ES) un Eiropas Padomi (EP).

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 citām iestādēm, tostarp nevalstiskajām organizācijām (NVO), kuriem/kurām var nākties saskarties ar juridiskajiem jautājumiem par datu aizsardzību.

Tā ir pirmais atskaites punkts gan par ES tiesību aktiem, gan par Eiropas Cilvēktiesību konvenciju (ECK) par datu aizsardzību, un paskaidro, kā šī joma tiek regulēta saskaņā ar ES tiesību aktiem un saskaņā ar ECK, kā arī saskaņā ar EP Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko [automatizēto] apstrādi (108. konvencija) un citiem EP instrumentiem. Katrā nodaļā ir atsevišķa tabula ar piemērojamiem juridiskajiem noteikumiem, tostarp svarīgi prakses piemēri no abām atsevišķajām Eiropas tiesību sistēmām. Tad abu šo Eiropas sistēmu attiecīgie tiesību akti ir norādīti viens aiz otra, attiecīgi kā tos var piemērot konkrētajai tēmai. Tas ļauj lasītājam redzēt, kur abas tiesību sistēmas sakrīt un kur atšķiras.

Tabulās katras nodaļas sākumā ir uzskaitītas attiecīgajā nodaļā aplūkotās tēmas un ir nosaukti piemērojamie juridiskie noteikumi un citi būtiski materiāli, piemēram, judikatūra. Tēmu secība var nedaudz atšķirties no teksta struktūras pašā nodaļā, ja to uzskata par vēlamu nodaļas satura konspektīvam izklāstam. Tabulas attiecas gan uz EP, gan ES tiesību aktiem. Tam jāpalīdz lietotājiem atrast galveno informāciju par savu situāciju, jo īpaši, ja uz tiem attiecas tikai EP tiesību akti.

Praktiķi ārpus-ES [trešās] valstīs, kas ir EP dalībvalstis un ECK un 108. konvencijas dalībnieces, var piekļūt par savu valsti būtiskajai informācijai tieši EP iedaļās. Praktiķiem ES dalībvalstīs būs jāizmanto abas iedaļas, jo šīm valstīm uzliek saistības abas tiesību sistēmas. Tie, kuriem vajag vairāk informācijas par kādu konkrētu jautājumu, rokasgrāmatas „papildliteratūras" iedaļā var atrast atsauču sarakstu uz specializētāku materiālu.

EP tiesiskais regulējums ir norādīts ar īsām atsaucēm uz atlasītām Eiropas Cilvēktiesību tiesas (ECT) lietām. Tās ir atlasītas no liela ECT spriedumu un lēmumu skaita par datu aizsardzības jautājumiem.

ES tiesiskais regulējums ir atrasts veiktajos leģislatīvajos pasākumos, attiecīgajos līgumu noteikumos un Eiropas Savienības Pamattiesību hartā, kā interpretēts Eiropas Savienības Tiesas („Tiesa", pirms 2009. gada dēvēta par Eiropas Kopienu Tiesu („EKT")) tiesu praksē.

Šajā rokasgrāmatā aprakstītā vai citētā tiesu prakse sniedz svarīgus gan ECT, gan Tiesas prakses pamattekstu piemērus. Pamatnostādnes šīs rokasgrāmatas beigās ir domātas kā palīgs lasītājam, meklējot tiesu prakses piemērus tiešsaistē.

Vēl, lai turpmāk atspoguļotu Eiropas datu aizsardzības noteikumu piemērošanu praksē, jo īpaši, ja par konkrēto tēmu nav konkrētas ECT vai Tiesas prakses, teksta logos ir sniegti praktiski atspoguļojumi ar hipotētiskiem scenārijiem.

Šīs rokasgrāmatas sākumā ir īsumā aprakstīts, kāda loma ir abām tiesību sistēmām, kā noteikts ECK un ES tiesību aktos (1. nodaļa). 2. līdz 8. nodaļā ir aplūkoti šādi jautājumi:

- datu aizsardzības terminoloģija;
- Eiropas tiesību aktu datu aizsardzības jomā pamatprincipi;
- Eiropas tiesību aktu datu aizsardzības jomā normas;
- datu subjektu tiesības un to īstenošana;
- pārrobežu datu plūsma;
- datu aizsardzība policijas un krimināltiesību kontekstā;
- citi specifiski Eiropas tiesību akti datu aizsardzības jomā.

1

Eiropas tiesību aktu datu aizsardzības jomā konteksts un vēsture

ES	Aplūkotie jautājumi	EP
Tiesības uz 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		ECK 8. pants (tiesības uz personas privāto un ģimenes dzīvi, korespondences noslēpumu un dzīvokļa neaizskaramību) Konvencija par personu aizsardzību attiecībā uz personas datu automātisko [automatizēto] apstrādi (108. konvencija)
Tiesību līdzsvarošana		
Tiesas apvienotās lietas C-92/09 un C-93/09, *Volker un Markus Schecke GbR un Hartmut Eifert pret Land Hessen*, 2010	**Vispārīgi**	
Tiesas lieta C-73/07, *Tietosuojavaltuutettu pret Satakunnan Markkinapörssi Oy un Satamedia Oy*, 2008	**Vārda brīvība**	ECT lieta *Axel Springer AG pret Vāciju*, 2012 ECT lieta *Mosley pret Apvienoto Karalisti*, 2011
	Brīvība mākslās un zinātnēs	ECT lieta *Vereinigung bildender Künstler pret Austriju*, 2007
Tiesas lieta C-275/06, *Productores de Música de España (Promusicae) pret Telefónica de España SAU*, 2008	**Īpašuma aizsardzība**	
Tiesas lieta C-28/08 P, *Eiropas Komisija pret The Bavarian Lager Co. Ltd*, 2010	**Piekļuve dokumentiem**	ECT lieta *Társaság a Szabadságjogokért pret Ungāriju*, 2009

1.1. Tiesības uz datu aizsardzību

Galvenie punkti

- Saskaņā ar ECK 8. pantu tiesības uz aizsardzību pret personas datu vākšanu un lietošanu ir daļa no tiesībām uz personas privāto un ģimenes dzīvi, korespondences noslēpumu un dzīvokļa neaizskaramību.
- EP 108. konvencija ir pirmais starptautiskais juridiski saistošais instruments, kas konkrēti skar datu aizsardzību.
- Saskaņā ar ES tiesību aktiem datu aizsardzību pirmoreiz regulēja Datu aizsardzības direktīva.
- Saskaņā ar ES tiesību aktiem datu aizsardzība ir atzīta par vienu no pamattiesībām.

Tiesības uz personas privātās dzīves aizsardzību pret iejaukšanos, jo īpaši no valsts puses, pirmoreiz starptautiskā juridiskā dokumentā tika noteiktas Apvienoto Nāciju Organizācijas (ANO) 1948. gada Vispārējās cilvēktiesību deklarācijas (VCD) 12. pantā par tiesībām uz privātās un ģimenes dzīves neaizskaramību.[1] VCD ietekmēja citu cilvēktiesību instrumentu izstrādi Eiropā.

1.1.1. Eiropas Cilvēktiesību konvencija

Eiropas Padome tika izveidota pēc Otrā Pasaules kara, lai dotu iespēju Eiropas valstīm kopīgi veicināt tiesiskumu (likuma varu), demokrātiju, cilvēktiesības un sociālo attīstību. Šajā nolūkā 1950. gadā tā pieņēma Eiropas Cilvēktiesību konvenciju (ECK), kas stājās spēkā 1953. gadā.

Valstīm ir starptautisks pienākums ievērot ECK. Visas EP dalībvalstis tagad ir transponējušas vai ieviesušas ECK savā valsts tiesiskajā regulējumā, kas tām liek rīkoties saskaņā ar Konvencijas noteikumiem.

Lai nodrošinātu, ka līgumslēdzējas puses ievēro savus pienākumus atbilstīgi ECK, Strasbūrā, Francijā, 1959. gadā tika nodibināta Eiropas Cilvēktiesību tiesa (ECT). ECT, izskatot personu, personu grupu, NVO vai juridisku personu iesniegtas sūdzības par domājamiem Konvencijas pārkāpumiem, nodrošina, ka valstis ievēro savus pienākumus atbilstīgi Konvencijai. 2013. gadā Eiropas Padomē bija 47 dalībvalstis, 28 no

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

kurām ir arī ES dalībvalstis. Prasības iesniedzējam ECT nav jābūt kādas dalībvalsts valstspiederīgajam. ECT var arī izskatīt starpvalstu prasības, ko viena vai vairākas EP dalībvalstis cēlušas pret citu dalībvalsti.

Tiesības uz personas datu aizsardzību ir daļa no tiesībām, kuras tiek aizsargātas saskaņā ar ECK 8. pantu un garantē tiesības uz personas privāto un ģimenes dzīvi, korespondences noslēpumu un dzīvokļa neaizskaramību, un izklāsta nosacījumus, ar kādiem tiek atļauti šo tiesību ierobežojumi.[2]

Savā judikatūrā ECT ir izskatījusi daudzas situācijas, kurās ir radies jautājums par datu aizsardzību, kā arī jautājumi par saziņas pārtveršanu,[3] dažādām uzraudzības formām[4] un aizsardzību pret personas datu uzglabāšanu, ko veic valsts iestādes.[5] Tā ir izskaidrojusi, ka ECK 8. pants ne tikai nosaka valstīm par pienākumu atturēties no jebkādām darbībām, kas var pārkāpt šīs Konvencijas tiesības, bet, ka zināmos apstākļos tām ir arī pozitīvs pienākums aktīvi nodrošināt privātās un ģimenes dzīves faktisku neaizskaramību.[6] Daudzi no šiem gadījumiem attiecīgajās nodaļās tiks skatīti sīkāk.

1.1.2. Eiropas Padomes 108. konvencija

Līdz ar informācijas tehnoloģiju attīstību 20. gadsimta 60. gados izveidojās arvien lielāka vajadzība pieņemt detalizētākas normas, lai aizsargātu personas, aizsargājot to (personas) datus. Līdz 20. gadsimta 70. gadu vidum Eiropas Padomes Ministru Komiteja pieņēma vairākas rezolūcijas par personas datu aizsardzību, atsaucoties uz ECK 8. pantu[7]. 1981. gadā tika atvērta parakstīšanai Konvencija par

2 EP, Eiropas Cilvēktiesību konvencija, *CETS* Nr. 005, 1950. gads.

3 Sk., piemēram, ECT 1984. gada 2. augusta spriedumu lietā *Malone pret Apvienoto Karalisti*, prasības pieteikums Nr. 8691/79; ECT 2007. gada 3. aprīļa spriedumu lietā *Copland pret Apvienoto Karalisti*, prasības pieteikums Nr. 62617/00.

4 Sk., piemēram, ECT 1978. gada 6. septembra spriedumu lietā *Klass un citi pret Vāciju*, prasības pieteikums Nr. 5029/71; ECT 2010. gada 2. septembra spriedumu lietā *Uzun pret Vāciju*, prasības pieteikums Nr. 35623/05.

5 Sk., piemēram, ECT 1987. gada 26. marta spriedumu lietā *Leander pret Zviedriju*, prasības pieteikums Nr. 9248/81; ECT 2008. gada 4. decembra spriedumu lietā *S. un Marper pret Apvienoto Karalisti*, prasības pieteikumi Nr. 30562/04 un Nr. 30566/04.

6 Sk., piemēram, ECT 2008. gada 17. jūlija spriedumu lietā *I. pret Somiju*, prasības pieteikums Nr. 20511/03; ECT 2008. gada 2. decembra spriedumu lietā *K.U. pret Somiju*, prasības pieteikums Nr. 2872/02.

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

personu aizsardzību attiecībā uz personas datu automātisko [automatizēto] apstrādi (108. konvencija)[8]. 108. konvencija bija un joprojām paliek vienīgais juridiski saistošais starptautiskais instruments datu aizsardzības jomā.

108. konvencija attiecas uz visu datu apstrādi ko veic kā privātais, tā arī sabiedriskais sektors, kā piemēram datu apstrāde ko veic tiesu un tiesībaizsardzības iestādes. Tā aizsargā personu pret iespējamām ļaunprātībām saistībā ar personas datu ievākšanu un apstrādi, un vienlaikus cenšas regulēt personas datu pārrobežu plūsmu. Kas attiecas uz personas datu ievākšanu un apstrādi, Konvencijā noteiktie principi konkrēti skar tādu datu godprātīgu un likumīgu ievākšanu un automatizētu apstrādi, kas tiek glabāti krātuvē īpašiem likumīgiem mērķiem, nevis izmantošanai, kas nav saderīga ar minētajiem nolūkiem, kā arī netiek glabāti ilgāk nekā nepieciešams. Tas attiecas arī uz datu kvalitāti, tiem jo īpaši jābūt pienācīgiem, būtiskiem un ne pārmērīgiem (samērīgums), kā arī precīziem.

Papildus garantiju sniegšanai attiecībā uz personas datu ievākšanu un apstrādi, tā neļauj, ja vien nav pienācīgu juridisko garantiju, apstrādāt „sensitīvus" datus, kā, piemēram, par personas rasi, politiskajiem uzskatiem, veselību, reliģisko pārliecību, dzimumdzīvi vai sodāmības reģistru.

Konvencijā ir arī nostiprinātas personas tiesības zināt, ka par viņu tiek uzglabāta informācija, un attiecīgā gadījumā lūgt to labot. Konvencijā noteikto tiesību ierobežošana ir iespējama tikai tad, ja ir iesaistītas svarīgākas intereses, piemēram, valsts drošība vai aizsardzība.

Lai gan konvencija paredz personas datu brīvu plūsmu starp Konvencijas Līgumslēdzējām Valstīm, tā arī nosaka dažus ierobežojumus šādām plūsmām uz valstīm, kurās tiesiskais regulējums neparedz līdzvērtīgu aizsardzību.

Lai turpmāk izstrādātu 108. konvencijā noteiktos vispārīgos principus un normas, EP Ministru komiteja ir pieņēmusi vairākus ieteikumus, kas nav juridiski saistoši (sk. 7. un 8. nodaļu).

8 EP Konvencija par personu aizsardzību attiecībā uz personas datu automātisko [automatizēto] apstrādi, *CETS* Nr. 108, 1981. gads.

Visas ES dalībvalstis ir ratificējušas 108. konvenciju. 1999. gadā 108. konvenciju grozīja, lai dotu iespēju ES kļūt par Līgumslēdzēju Pusi.[9] 2001. gadā tika pieņemts 108. konvencijas papildprotokols, ieviešot noteikumus par pārrobežu datu plūsmām valstīm, kas nav Konvencijas Līgumslēdzējas Puses, tā dēvētajām trešām valstīm, un par valstu datu aizsardzības uzraudzības iestāžu obligātu izveidi.[10]

Pārskats

Pēc lēmuma modernizēt 108. konvenciju, 2011. gadā tika rīkota sabiedriska apspriešana, kas ļāva apstiprināt divus galvenos darba mērķus: pastiprināt privātuma aizsardzību digitālajā jomā un nostiprināt konvencijas izpildes kontroles mehānismus.

108. konvencijai var pievienoties valstis, kas nav EP dalībvalstis, tostarp ārpuseiropas valstis. Konvencijas kā universāla standarta potenciāls un tās atvērtais raksturs var būt par pamatu datu aizsardzības veicināšanai globālā mērogā.

Pašlaik 45 no 46 108. konvencijas līgumslēdzējpusēm ir EP dalībvalstis. Urugvaja, pirmā ārpuseiropas valsts, pievienojās 2013. gada augustā, un Maroka, kuru pievienoties 108. konvencijai ir uzaicinājusi Ministru komiteja, pašlaik kārto pievienošanās formalitātes.

1.1.3. Eiropas Savienības tiesību akti datu aizsardzības jomā

ES tiesību sastāvā ir līgumi un sekundārās ES tiesības. Līgumi, proti, Līgums par Eiropas Savienību (TEU) un Līgums par Eiropas Savienības darbību (LESD), ir apstiprināti visās ES dalībvalstīs un tiek dēvēti arī par „primārajām ES tiesībām". ES regulas, direktīvas un lēmumus ir pieņēmušas ES iestādes, kurām tādas pilnvaras ir piešķirtas saskaņā ar līgumiem; minētos dokumentus bieži dēvē par „sekundārajām ES tiesībām".

ES galvenais juridiskais datu aizsardzības dokuments ir Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva 95/46/EK par personu aizsardzību attiecībā

9 Strasbūrā Ministru komitejas pieņemtie 1999. gada 15. jūnija grozījumi EP Konvencijā par personu aizsardzību attiecībā uz personu datu automātisko apstrādi (ETS Nr. 108), atļaujot Eiropas Kopienām pievienoties; 108. konvencijas grozītās redakcijas 23. panta 2. punkts.

10 EP, Konvencijas par personu aizsardzību attiecībā uz personu datu automātisko [automatizētu] apstrādi papildprotokols par uzraudzības institūcijām un pārrobežu datu plūsmām, *CETS* Nr. 181, 2001. gads.

uz personas datu apstrādi un šādu datu brīvu apriti (*Datu aizsardzības direktīva*).[11] To pieņēma 1995. gadā – laikā, kad vairākas dalībvalstis jau bija pieņēmušas valsts datu aizsardzības likumus. Preču, kapitāla, pakalpojumu un personu brīva aprite iekšējā tirgū prasīja brīvu datu plūsmu, ko nevarētu īstenot, ja dalībvalstis nevarētu paļauties uz vienveidīgu augstu datu aizsardzības līmeni.

Tā kā datu aizsardzības direktīvas pieņemšanas mērķis bija saskaņot[12] datu aizsardzības tiesību aktus valsts mērogā, direktīva piešķir tādu specifiskuma pakāpi, kas ir salīdzināms ar pakāpi, kas paredzēta (toreiz) spēkā esošajos valsts datu aizsardzības tiesību aktos. Tiesa atgādina, ka "ar Direktīvu 95/46 ... ir paredzēts visās dalībvalstīs nodrošināt vienādu personu tiesību un brīvību aizsardzību saistībā ar personas datu apstrādi... Attiecīgajā jomā piemērojamo valstu tiesību aktu tuvināšana nedrīkst vājināt to sniegto aizsardzību, bet tai, tieši pretēji, jācenšas nodrošināt augstu aizsardzības līmeni visa ES. Tādējādi ... minēto valsts tiesību aktu saskaņošana nav tikai minimāla, bet tai ir jābūt tādai saskaņošanai, kas faktiski ir pilnīga."[13] Tāpēc dalībvalstīm ir tikai ierobežota rīcības brīvība šīs direktīvas īstenošanā.

Datu aizsardzības direktīva ir plānota tā, lai piešķirtu būtiskumu 108. konvencijā ietvertajiem tiesību uz privātumu principiem un paplašinātu tos. Tas, ka visas 15 ES dalībvalstis 1995. gadā bija arī 108. konvencijas Līgumslēdzējas Puses, izslēdz pretrunīgu normu pieņemšanu abos minētajos juridiskajos instrumentos. Datu aizsardzības direktīva tomēr izmanto 108. konvencijas 11. pantā paredzēto iespēju pievienot aizsardzības instrumentus. Jo īpaši, ieviešot neatkarīgu uzraudzību kā instrumentu atbilstības uzlabošanai ar datu aizsardzības normām, izrādījās, ka tas ir nozīmīgs ieguldījums Eiropas tiesību aktu datu aizsardzības jomā efektīvai darbībai. (Rezultātā šī iezīme tika pārņemta EP tiesībās 2001. gadā ar 108. konvencijas papildprotokolu.)

Datu aizsardzības direktīvas teritoriālā piemērošana ir plašāka nekā tikai 28 ES dalībvalstīs – to piemēro arī valstīs, kas nav ES dalībvalstis, bet ir Eiropas Ekonomikas zonas (EEZ) daļa[14] – proti, Islandē [Īslandē], Lihtenšteinā un Norvēģijā.

Tiesai Luksemburgā ir jurisdikcija noteikt, vai dalībvalsts ir izpildījusi savus pienākumus atbilstoši datu aizsardzības direktīvai, un sniegt prejudiciālus nolēmumus par

11 Datu aizsardzības direktīva, OV 1995 L 281, 31. lpp.

12 Sk., piemēram, datu aizsardzības direktīvas preambulas 1., 4., 7. un 8. apsvērumu.

13 Tiesas 2011. gada 24. novembra spriedums apvienotajās lietās C-468/10 un C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) pret Administración del Estado,* 28. un 29. pumkts.

14 Līgums par Eiropas Ekonomikas zonu, OV 1994 L 1, kas stājās spēkā 1994. gada 1. janvārī.

direktīvas spēkā esību un interpretāciju, lai nodrošinātu tās efektīvu un vienveidīgu piemērošanu dalībvalstīs. Svarīgs izņēmums no datu aizsardzības direktīvas piemērojamības ir tā sauktais izņēmums mājsaimniecības vajadzībām, proti, ja personas datus apstrādā privātas personas tikai saviem vai mājsaimniecības nolūkiem.[15] Tādu apstrādi parasti uzskata par daļu no privātas personas brīvībām.

Atbilstoši ES primārajām tiesībām, kas bija spēkā datu aizsardzības direktīvas pieņemšanas laikā, direktīvas materiālā darbības joma ir ierobežota un attiecas tikai uz iekšējā tirgus lietām. Vissvarīgākie ārpus tās piemērošanas jomas ir sadarbības jautājumi policijas un krimināltiesību jomā. Datu aizsardzība šajās jomās rodas no dažādiem juridiskajiem instrumentiem, kas ir aprakstīti 7. nodaļā.

Tā kā datu aizsardzības direktīvu varēja adresēt tikai ES dalībvalstīm, bija vajadzīgs papildu juridiskais instruments, lai izveidotu datu aizsardzību attiecībā uz personas datu apstrādi ES iestādēs un struktūrās. Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti (*Regula par aizsardzību attiecībā uz personas datu apstrādi ES iestādēs*) pilda šo uzdevumu.[16]

Papildus, pat jomās, uz ko attiecas datu aizsardzības direktīva, bieži vien ir vajadzīgi detalizētāki datu aizsardzības noteikumi, lai sasniegtu vajadzīgo skaidrību citu likumīgo interešu līdzsvarošanā. Divi piemēri ir Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju (*Direktīva par privātumu un elektronisko komunikāciju*)[17] un 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 (*Datu saglabāšanas direktīva,* 2014. gada 8. aprīlī

15 Datu aizsardzības direktīva, 3. panta 2. punkta otrais ievilkums.

16 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.

17 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 [privātumu] un elektronisko komunikāciju*), OV 2002 L 201.

atzīta par spēkā neesošu).[18] Citi piemēri tiks apspriesti 8. nodaļā. Minētajiem noteikumiem jābūt saskaņā ar datu aizsardzības direktīvu.

Eiropas Savienības Pamattiesību harta

Eiropas Kopienu sākotnējos līgumos nebija ietvertas nekādas atsauces uz cilvēktiesībām vai to aizsardzību. Toreizējā Eiropas Kopienu Tiesa pakāpeniski, saņemot izskatīšanai lietas par cilvēktiesību pārkāpumiem jomās, kas ietilpst ES tiesību darbības jomā, tā tomēr izstrādāja jaunu pieeju. Lai piešķirtu aizsardzību personām, tā pārcēla pamattiesības tā dēvētajos Eiropas tiesību vispārējos principos. Pēc Tiesas domām, šie vispārējie principi atspoguļo valstu Konstitūcijās un cilvēktiesību līgumos, jo īpaši ECK, atrodamo cilvēktiesību aizsardzības saturu. Tiesa apgalvoja, ka tas nodrošinātu ES tiesību aktu atbilstību minētajiem principiem.

Atzīstot, ka tās politika var ietekmēt cilvēktiesības, un cenšoties panākt, lai pilsoņu justos „tuvāki" ES, ES 2000. gadā pasludināja Eiropas Savienības Pamattiesību hartu (Harta). Šajā Hartā ir iekļauts vesels diapazons Eiropas pilsoņu civilo, politisko, ekonomisko un sociālo tiesību, apkopojot konstitucionālās tradīcijas un starptautiskos pienākumus, kas ir kopīgi dalībvalstīm. Hartā aprakstītās tiesības ir sadalītas sešās sadaļās: cieņa, brīvības, vienlīdzība, solidaritāte, pilsoņu tiesības un taisnīgums.

Lai gan sākotnēji Harta bija tikai politisks dokuments, Harta kļuva juridiski saistoša[19] kā ES primārs tiesību akts (sk. LES 6. panta 1. punktu) līdz ar Lisabonas līguma stāšanos spēkā 2009. gada 1. decembrī.[20]

ES primārie tiesību akti ietver arī vispārīgu ES leģislatīvo kompetenci datu aizsardzības jomā (LESD 16. pants).

Harta ne tikai garantē privātās un ģimenes dzīves neaizskaramību (7. pants), bet arī nosaka tiesības uz datu aizsardzību (8. pants), skaidri paaugstinot šīs aizsardzības līmeni līdz pamattiesību līmenim ES tiesību aktos. ES iestādēm un dalībvalstīm jāievēro un jāgarantē šīs tiesības, kas attiecas arī uz dalībvalstīm, kad tās īsteno

18 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 (*Datu saglabāšanas direktīva*), OV 2006 L 105, 2014. gada 8. aprīlī atzīta par spēkā neesošu

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

20 Sk. Eiropas Kopienas (2012), Līgums par Eiropas Savienību, OV 2012 C 326; un Eiropas Kopienas (2012), LESD, OV 2012 C 326, konsolidētās versijas.

Savienības tiesību aktus (Hartas 51. pants). Tā kā Hartas 8. pants ir rediģēts vairākus gadus pēc datu aizsardzības direktīvas, tas ir jāsaprot kā tāds, kas ietver agrāk pastāvējušos ES datu aizsardzības tiesību aktus. Tāpēc Harta ne tikai skaidri piemin tiesības uz datu aizsardzību 8. panta 1. punktā, bet arī atsaucas uz galvenajiem datu aizsardzības principiem 8. panta 2. punktā. Visbeidzot, Hartas 8. panta 3. punktā ir nodrošināts, ka minēto principu īstenošanu kontrolēs neatkarīga iestāde.

Pārskats

2012. gada janvārī Eiropas Komisija ierosināja datu aizsardzības reformu paketi, apgalvojot, ka pašreizējās datu aizsardzības normas ir jāmodernizē, ņemot vērā straujo tehnoloģisko attīstību un globalizāciju. Šajā reformu paketē ietilpst priekšlikums Vispārējai Datu aizsardzības regulai,[21] ar kuru plānots aizstāt Datu aizsardzības direktīvu, kā arī jauna Datu aizsardzības direktīva[22], kura paredz datu aizsardzību policijas un tiesu iestāžu sadarbības kriminālietās jomā. Šīs rokasgrāmatas publicēšanas laikā diskusijas par reformu paketi turpinājās.

1.2. Tiesību līdzsvarošana

Galvenais punkts

- Tiesības uz datu aizsardzību nav absolūtas tiesības; tās jālīdzsvaro ar citām tiesībām.

Pamattiesības uz personas datu aizsardzību saskaņā ar Hartas 8. pantu „nav tomēr absolūta prerogatīva, bet ir jāņem vērā saistībā ar tās funkciju sabiedrībā".[23] Tādējādi Hartas 52. panta 1. punktā ir pieļauts, ka tādām tiesībām, kādas ir paredzētas tās 7. un 8. pantā, var tikt noteikti izmantošanas ierobežojumi, ciktāl šie ierobežojumi ir noteikti tiesību aktos, tajos respektē šo tiesību un brīvību būtību un, ievērojot samērīguma principu, tie ir nepieciešami un patiešām atbilst vispārējas nozīmes mērķiem,

21 Eiropas Komisija (2012), *Priekšlikums Eiropas Parlamenta un Padomes Regulai par personu aizsardzību attiecībā uz personas datu apstrādi un par šādu datu brīvu apriti (Vispārīgā datu aizsardzības regula)*, COM(2012) 11 final, Briselē, 2012. gada 25. janvārī.

22 Eiropas Komisija (2012), *Priekšlikums Eiropas Parlamenta un Padomes direktīvai 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 (Vispārīgā datu aizsardzības direktīva)*, COM(2012) 10 final, Briselē, 2012. gada 25. janvārī.

23 Sk., piemēram, Tiesas 2010. gada 9. novembra spriedumu apvienotajās lietā C-92/09 un C-93/09, *Volker un Markus Schecke GbR un Hartmut Eifert pret Land Hessen*, 48. punkts.

ko atzinusi [Eiropas] Savienība, vai vajadzībai aizsargāt citu personu tiesības un brīvības.[24]

ECK sistēmā datu aizsardzību garantē 8. pants (tiesības uz privātās un ģimenes dzīves neaizskaramību) un, tāpat kā Hartas sistēmā, šīs tiesības ir jāpiemēro, ievērojot citu konkurējošo tiesību tvērumu. Atbilstoši ECK 8. panta 2. punktam, „[v]alsts institūcijas nedrīkst traucēt nevienam baudīt šīs tiesības, izņemot gadījumos, kas paredzēti likumā un ir nepieciešami demokrātiskā sabiedrībā, [...] lai aizstāvētu citu tiesības un brīvības".

Vēlāk gan ECT, gan Tiesa ir vairākkārt apgalvojušas, ka līdzsvarošana ar citām tiesībām ir nepieciešama, piemērojot un interpretējot ECK 8. pantu un Hartas 8. pantu.[25] Ar vairākiem svarīgiem piemēriem tiks parādīts, kā šādu līdzsvaru sasniedz.

1.2.1. Vārda brīvība

Viena no tiesībām, kas var nonākt pretrunā tiesībām uz datu aizsardzību, ir tiesības uz vārda brīvību.

Vārda brīvība ir aizsargāta Hartas 11. pantā („Vārda un informācijas brīvība"). Šīs tiesības ietver „uzskatu brīvību un brīvību saņemt un izplatīt informāciju vai idejas bez valsts iestāžu iejaukšanās un neatkarīgi no valstu robežām". [Hartas] 11. pants atbilst ECK 10. pantam. Atbilstoši Hartas 52. panta 3. punktam, ciktāl tajā ir ietvertas tiesības, kuras atbilst ECK garantētajām tiesībām, „šo tiesību nozīme un apjoms ir tāds pats kā minētajā Konvencijā noteiktajām tiesībām". Tāpēc ierobežojumi, ko likumīgi drīkst noteikt Hartas 11. pantā garantētajām tiesībām, nedrīkst pārsniegt ierobežojumus, kas noteikti ECK 10. panta 2. punktā, proti, tiem jābūt paredzētiem tiesību aktos un tiem jābūt nepieciešamiem demokrātiskā sabiedrībā „citu reputācijas vai tiesību aizsardzībai [...]". Šis jēdziens ietver tiesības uz datu aizsardzību.

24 Turpat, 50. punkts.

25 ECT 2012. gada 7. februāra spriedums lietā *Von Hannover pret Vāciju (Nr. 2)* [GC], prasības pieteikumi Nr. 40660/08 un Nr. 60641/08, Tiesas 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), Tiesas 2008. gada 29. janvāra spriedums lietā C-275/06 *Productores de Música de España (Promusicae) pret Telefónica de España SAU* (68. punkts). Sk. arī Eiropas Padome (2013), Eiropas Cilvēktiesību tiesas praksi par personas datu aizsardzību, DP (2013) Tiesu prakse, pieejama šādā tīmekļa vietnē: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP 2013 Case Law_Eng_FINAL.pdf.

Attiecības starp personas datu aizsardzību un vārda brīvību regulē datu aizsardzības direktīvas 9. pants ar nosaukumu „Personas datu apstrāde un vārda brīvība".[26] Atbilstoši šim pantam „[d]alībvalstis nosaka izņēmumus vai atkāpes no direktīvas II nodaļas, IV nodaļas un VI nodaļas noteikumiem attiecībā uz datu aizsardzību un tādējādi attiecībā uz pamattiesībām uz privātumu. Šādas atkāpes drīkst izdarīt tikai un vienīgi žurnālistikas nolūkiem vai mākslinieciskās vai literārās izteiksmes nolūkiem, kas ietilpst pamattiesību uz vārda brīvību darbības jomā, tiktāl, ciktāl tās vajadzīgas, lai saskaņotu tiesības uz privātās dzīves neaizskaramību ar normām, kas reglamentē vārda brīvību".

Piemērs: Lietā *Tietosuojavaltuutettu pret Satakunnan Markkinapörssi Oy* un *Satamedia Oy*[27] Tiesu lūdza interpretēt datu aizsardzības direktīvas 9. pantu un definēt attiecības starp datu aizsardzību un preses brīvību. Tiesai bija jāizskata gadījums, kurā Markkinapörssi un Satamedia bija izplatījusi no Somijas nodokļu iestādēm likumīgi iegūtus nodokļu datus par aptuveni 1,2 miljoniem fizisku personu. It īpaši, Tiesai 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 Satakunnan darbības bija „personas datu apstrāde" datu aizsardzības direktīvas 3. panta 1. punkta nozīmē, Tiesa turpmāk izskaidroja direktīvas 9. pantu. 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, paredzētās atkāpes no datu aizsardzības un tās ierobežojumi ir jāīsteno stingri ievērojot vajadzīgās robežas. Minētajos apstākļos Tiesa uzskatīja, ka tādas darbības, kādas bija veikušas Markkinapörssi un Satamedia saistībā ar datiem, kas iegūti no saskaņā ar valsts tiesību aktiem 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 minētās darbības var veikt ne tikai plašsaziņas līdzekļu uzņēmumi, un tās var būt saistītas ar mērķi gūt peļņu. Tiesa tomēr atstāja valsts tiesas ziņā noteikt, vai konkrētais gadījums bija tieši šāds gadījums.

26 Datu aizsardzības direktīvas 9. pants.

27 Tiesas 2008. gada 16. decembra spriedums lietā C-73/07, *Tietosuojavaltuutettu pret Satakunnan Markkinapörssi Oy un Satamedia Oy* (56., 61. un 62. punkts).

Par tiesību uz datu aizsardzību saskaņošanu ar tiesībām uz vārda brīvību ECT ir pieņēmusi vairākus etalonspriedumus.

Piemērs: Lietā *Axel Springer AG pret Vāciju*[28] ECT uzskatīja, ka valsts tiesas noteiktais aizliegums avīzes īpašniekam, kurš vēlējās publicēt rakstu par populāra aktiera apcietināšanu un notiesāšanu, pārkāpa ECK 10. panta prasības. ECT atkārtoti uzsvēra kritērijus, ko tā bija noteikusi savā praksē, līdzsvarojot tiesības uz vārda brīvību ar tiesībām uz privātās dzīves neaizskaramību:

- pirmkārt, vai notikums, par ko bija publicētais raksts, bija vispārējas nozīmes notikums: personas apcietināšana un notiesāšana bija publisks tiesas fakts un tātad vispārējas nozīmes notikums;

- otrkārt, vai attiecīgā persona bija publiska persona: attiecīgā persona bija pietiekami labi pazīstams aktieris, lai viņu varētu uzskatīt par publisku personu, un

- treškārt, kā tika iegūta informācija un vai tā ir ticama: informāciju ir sniedzis valsts prokurora birojs, un abās publikācijās ietvertās informācijas precizitāti lietas dalībnieki neapstrīdēja.

Tāpēc ECT sprieda, ka uzņēmumam noteiktais publicēšanas ierobežojums nebija samērīgs prasītāja privātās dzīves aizsardzības likumīgajam mērķim. Tiesa secināja, ka ir bijis ECK 10. panta prasību pārkāpums.

Piemērs: Lietā *Von Hannover pret Vāciju* (Nr. 2)[29] ECT neatklāja, ka būtu pārkāptas tiesības uz privātās dzīves neaizskaramību saskaņā ar ECK 8. pantu, kad tiesa Monako Princesei Karolīnai atteica izdot aizliegumu publicēt fotogrāfiju, kurā bija redzama pati Princese un viņas vīrs slēpošanas atvaļinājuma laikā. Fotogrāfijai bija pievienots raksts, kur cita starpā bija ziņas par Prinča Renjē slikto veselību. ECT secināja, ka valsts tiesas bija rūpīgi līdzsvarojušas izdevniecību tiesības uz vārda brīvību ar prasības iesniedzēju tiesībām uz viņu privātās dzīves neaizskaramību. To, ka valsts tiesas bija noraksturojušas Prinča Renjē slimību kā mūsdienu sabiedrības notikumu, nevarēja uzskatīt par nesaprātīgu,

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

29 ECT 2012. gada 7. februāra spriedums lietā *Von Hannover pret Vāciju (Nr. 2)* [GC], prasības pieteikumi Nr. 40660/08 un Nr. 60641/08, 118. un 124. punkts.

un ECT spēja pieņemt, ka fotogrāfija, ņemot vērā rakstu, vismaz nelielā mērā veicināja vispārējas nozīmes debates. Tiesa secināja, ka ECK 8. panta prasības nav pārkāptas.

ECT praksē viens no būtiskākajiem kritērijiem attiecībā uz minēto tiesību līdzsvarošanu ir tas, vai konkrētā izpausme veicina vispārējas nozīmes debates vai nē.

Piemērs: Lietā *Mosley pret Apvienoto Karalisti* [30] valsts nedēļas laikraksts publicēja prasības iesniedzēja intīmas fotogrāfijas. Prasības iesniedzējs apgalvoja, ka ir pārkāptas ECK 8. panta prasības, jo viņš nebija spējis lūgt tiesas aizliegumu pirms konkrēto fotogrāfiju publicēšanas, jo nebija nekādas iepriekšējas paziņošanas prasības, kas būtu jāievēro laikrakstam, ja tas publicē materiālu, kas var pārkāpt kādas personas tiesības uz privātumu. Lai gan minētā materiāla izplatīšana notika galvenokārt izklaides, nevis izglītošanas nolūkā, uz to nešaubīgi attiecās ECK 10. pantā paredzētā aizsardzība, kas tomēr „pakļāvās" ECK 8. panta prasībām, ja informācija bija privāta un intīma rakstura un tās izplatīšana nebija vispārējās interesēs. Tomēr īpaši rūpīgi bija jāizskata ierobežojumi, kas var būt kā cenzūra pirms publicēšanas. Attiecībā uz stindzinošo efektu, kādu varētu radīt prasība par iepriekšēju paziņojumu, attiecībā uz šaubām par tā efektivitāti un attiecībā uz plašo izvērtēšanas un rīcības brīvību šajā jomā ECT secināja, ka 8. pantā nav prasības par juridiski saistošu iepriekšēju paziņojumu. Attiecīgi tiesa secināja, ka nav bijis 8. panta prasību pārkāpuma.

Piemērs: Lietā *Biriuk pret Lietuvu*[31] prasības iesniedzēja pieprasīja dienas laikrakstam atlīdzināt zaudējumus, jo tas bija publicējis rakstu ar apgalvojumu, ka viņa ir HIV pozitīva. Minēto informāciju it kā bija apstiprinājuši vietējās slimnīcas ārsti. ECT neuzskatīja, ka konkrētais raksts veicina jebkādas vispārējas intereses debates, un atkārtoti uzsvēra, ka personas datu, kā arī medicīnas datu aizsardzība ir būtiski svarīga, lai persona varētu izmantot savas tiesības uz privātās un ģimenes dzīves neaizskaramību, ko garantē ECK 8. pants. Tiesa piešķīra īpašu nozīmi faktam, ka atbilstoši ziņojumam laikrakstā slimnīcas medicīniskais personāls bija sniedzis informāciju par prasītājas inficēšanos ar HIV, acīmredzami pārkāpjot savu pienākumu neizpaust profesionālo [medicīnas] noslēpumu. Tādējādi valsts nebija izpildījusi savu pienākumu nodrošināt prasītājas tiesības uz viņas privātās dzīves neaizskaramību. Tiesa secināja 8. panta prasību pārkāpumu.

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

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

1.2.2. Piekļuve dokumentiem

Informācijas brīvība saskaņā ar Hartas 11. pantu un ECK 10. pantu aizsargā tiesības ne tikai sniegt, bet arī *saņemt* informāciju. Arvien vairāk pieaug apziņa par to, cik svarīga demokrātiskas sabiedrības darbībai ir valdības caurskatāmība. Līdz ar to pēdējās divās desmitgadēs tiesības uz piekļuvi publisku iestāžu dokumentiem ir atzītas par ikviena ES pilsoņa, kā arī ikvienas fiziskas vai juridiskas personas, kuras pastāvīgā dzīvesvieta ir vai kura ir reģistrējusi uzņēmējdarbību kādā dalībvalstī, svarīgām tiesībām.

Saskaņā ar EP tiesību aktiem var atsaukties uz principiem, kuri nostiprināti leteikumā par piekļuvi oficiālajiem dokumentiem un ko izmantoja, sagatavojot Konvenciju par piekļuvi oficiālajiem dokumentiem (*205. konvencija*).[32] **Saskaņā ar ES tiesību aktiem** piekļuves tiesības dokumentiem garantē Regula Nr. 1049/2001 par publisku piekļuvi Eiropas Parlamenta, Padomes un Komisijas dokumentiem (*Piekļuves dokumentiem regula*).[33] Hartas 42. pants un LESD 15. panta 3. punkts ir paplašinājuši šīs piekļuves tiesības „Savienības iestāžu un struktūru dokumentiem neatkarīgi no to veida". Saskaņā ar Hartas 52. panta 2. punktu piekļuves tiesības dokumentiem īsteno arī saskaņā ar nosacījumiem un ierobežojumiem, kā paredzēts LESD 15. panta 3. punktā. Šīs tiesības var nonākt konfliktā ar tiesībām uz datu aizsardzību, ja piekļuve dokumentam atklātu citu personu datus. Tāpēc lūgumi piekļūt valsts iestāžu rīcībā esošiem dokumentiem vai informācijai var būt jālīdzsvaro ar to personu tiesībām uz datu aizsardzību, kuru dati ir ietverti lūgtajos dokumentos.

Piemērs: Lietā *Komisija pret Bavarian Lager*[34] Tiesa definēja personas datu aizsardzības tvērumu saistībā ar piekļuvi ES iestāžu dokumentiem un attiecībām starp Regulu Nr. 1049/2001 (*Piekļuves dokumentiem regula*) un Regulu Nr. 45/2001 (*Datu aizsardzības regula*). 1992. gadā izveidotā *Bavarian Lager* ieveda pudelēs iepildītu Vācijas alu Apvienotajā Karalistē, kas paredzēts galvenokārt bāriem. Tā tomēr saskārās ar grūtībām, jo Lielbritānijas tiesību akti *de facto* izrādīja labvēlību valsts ražotājiem. Atbildot uz *Bavarian Lager* sūdzību, Eiropas Komisija nolēma celt prasību pret Apvienoto Karalisti par valsts

32 Eiropas Padome, Ministru komiteja (2002), 2001. gada 21. februāra Ieteikums Nr. Rec(2002)2 dalībvalstīm par piekļuvi oficiāliem dokumentiem; Eiropas Padomes 2009. gada 18. jūnija Konvencija par piekļuvi oficiāliem dokumentiem, *CETS* Nr. 205. Konvencija vēl nav stājusies spēkā.

33 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).

34 Tiesas 2010. gada 29. jūnija spriedums lietā C-28/08 P, *Eiropas Komisija pret The Bavarian Lager Co. Ltd.* (60., 63., 76., 78. un 79. punkts).

pienākumu neizpildi, kā rezultātā Apvienotā Karaliste grozīja apstrīdētos noteikumus un saskaņoja tos ar ES tiesībām. Tad *Bavarian Lager* palūdza Komisijai citu dokumentu starpā tās sanāksmes protokola kopiju, kurā piedalījās Komisijas, Lielbritānijas iestāžu un *Confédération des Brasseurs du Marché Commun* (*CBMC*) pārstāvji. Komisija piekrita atklāt dažus sanāksmes dokumentus, bet izdzēsa piecus protokolā norādītus uzvārdus – divas personas bija konkrēti iebildušas pret to identitātes atklāšanu, un ar trim pārējiem Komisijai nebija izdevies sazināties. Ar 2004. gada 18. marta lēmumu Komisija noraidīja jaunu *Bavarian Lager* prasību, kurā bija prasīts pilnīgs sanāksmes protokols, konkrēti norādot uz minēto personu privātās dzīves aizsardzību, ko garantē datu aizsardzības regula. Tā kā šī nostāja Bavarian Lager neapmierināja, tā cēla prasību Pirmās instances tiesā, kas ar 2007. gada 8. novembra spriedumu atcēla Komisijas lēmumu (lieta T194/04, *Bavarian Lager pret Komisiju*), it īpaši uzskatot, ka vienkārši ierakstot sanāksmes dalībnieku sarakstā konkrēto personu, kas minētajā sanāksmē pārstāvēja savas attiecīgās struktūras, vārdus, netiek radīts nekāds apdraudējums minēto personu privātajai dzīvei.

Pēc Komisijas apelācijas sūdzības Tiesa atcēla Pirmās instances tiesas spriedumu. Tiesa uzskatīja, ka Piekļuves dokumentiem regulā ir noteikts „īpašs un pastiprināts tiesiskais regulējums attiecībā uz tās personas aizsardzību, kuras personas dati attiecīgajā gadījumā varētu tikt izpausti sabiedrībai". Pēc Tiesas domām, ja lūgumā, kas pamatots uz Piekļuves dokumentiem regulu, tādējādi ir prasīta piekļuve dokumentiem, kuros ir personas dati, datu aizsardzības regulas noteikumi kļūst piemērojami to kopumā. Tiesa tad secināja, ka Komisija bija pareizi noraidījusi prasību piekļūt pilnam 1996. gada oktobra sanāksmes protokolam. Ja nav piecu tās sanāksmes dalībnieku piekrišanas, Komisija pietiekami izpildīja savu atvērtības pienākumu, izdodot konkrēto dokumentu ar dzēstiem minēto personu vārdiem.

Turklāt, pēc Tiesas domām, „tā kā Bavarian Lager nav sniegusi nedz skaidru un likumīgu pamatojumu, nedz pārliecinošus argumentus nolūkā pierādīt vajadzību nodot šos personas datus, Komisija nespēja izsvērt dažādās lietas dalībnieku intereses. Tāpat tā nevarēja pārbaudīt, vai ir pamats pieņemt, ka ar šo nodošanu varētu tikt ierobežotas datu subjektu likumīgās intereses", kā prasīts datu aizsardzības regulā.

Saskaņā ar šo spriedumu, lai neievērotu tiesības uz datu aizsardzību attiecībā uz piekļuvi dokumentiem, ir vajadzīgs konkrēts un pamatots iemesls. Piekļuves tiesības dokumentiem nevar automātiski atcelt tiesības uz datu aizsardzību.[35]

Īpašs piekļuves lūguma aspekts tika aplūkots nākamajā ECT spriedumā.

Piemērs: Lietā *Társaság a Szabadságjogokért pret Ungāriju*[36] prasītāja, cilvēktiesību NVO, bija lūgusi Konstitucionālajai Tiesai piekļuvi informācijai par lietu, kurā vēl nebija pieņemts spriedums. Neapspriedusies ar Parlamenta locekli, kas tai bija iesniedzis minēto lietu, Konstitucionālā Tiesa noraidīja piekļuves lūgumu, pamatojot ar to, ka tai iesniegtās sūdzības var tikt darītas pieejamas trešām personām tikai ar sūdzības iesniedzēja piekrišanu. Valsts tiesas apstiprināja šo atteikumu, pamatojot ar to, ka tādu personas datu aizsardzību nevar atcelt citas likumīgas intereses, tostarp pieejamība publiskai informācijai. Prasītāja bija rīkojusies kā „sociāls uzraugs", kura darbībām tika garantēta līdzīga aizsardzība, kāda bija piešķirta presei. Attiecībā uz preses brīvību ECT bija pastāvīgi apgalvojusi, ka sabiedrībai ir tiesības saņemt vispārējas intereses informāciju. Prasītājas lūgtā informācija bija „gatava un pieejama" un neprasīja nekādu datu vākšanu. Minētajos apstākļos valstij bija pienākums netraucēt prasītājas lūgtās informācijas plūsmu. Kopumā ECT uzskatīja, ka šķēršļi, kas plānoti, lai kavētu piekļuvi vispārējas intereses informācijai, var atturēt plašsaziņas līdzekļos vai saistītajās jomās strādājošos no sava būtiskā uzdevuma – būt par „publisku uzraugu" – veikšanas. Tiesa secināja, ka ir bijis 10. panta prasību pārkāpums.

Saskaņā ar ES tiesību aktiem caurskatāmības svarīgums ir stingri noteikts. Caurskatāmības [atklātības] princips ir nostiprināts LES 1. un 10. pantā un LESD 15. panta 1. punktā.[37] Atbilstīgi Regulas (EK) Nr. 1049/2001 preambulas 2. apsvērumam tas dod iespēju pilsoņiem vēl vairāk iesaistīties lēmumu pieņemšanā un nodrošina

35 Sk. tomēr Eiropas Datu aizsardzības uzraudzītāja (EDAU) detalizētās apspriedes (2011), *Publiska piekļuve dokumentiem, kas satur personas datus pēc nolēmuma lietā* Bavarian Lager, Briselē, 2011. gada 24. martā, pieejams: www.EDAU.europa.eu/EDAUWEB/webdav/site/mySite/shared/Documents/EDAU/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 ECT 2009. gada 14. aprīļa spriedums lietā *Társaság a Szabadságjogokért pret Ungāriju*, prasības pieteikums Nr. 37374/05; sk. 27, 36.–38. punktu.

37 ES (2012), Līguma par Eiropas Savienību un LESD konsolidētās versijas, OV 2012 C 326.

lielāku pārvaldes sistēmas leģitimitāti un efektivitāti demokrātiskā iekārtā, kā arī nosaka tai lielāku atbildību pilsoņu priekšā.[38]

Ievērojot šo argumentāciju, Padomes Regulā (EK) Nr. 1290/2005 par kopējās lauksaimniecības politikas finansēšanu un Komisijas Regulā (EK) Nr. 259/2008, ar ko nosaka minētās Padomes regulas piemērošanas noteikumus, ir prasīts publicēt informāciju par noteiktu ES lauksaimniecības nozares fondu līdzekļu saņēmējiem un par summām, ko saņem katrs atbalsta saņēmējs.[39] Publikācijai ir jāveicina sabiedrības kontrole pār to, lai administrācija pienācīgi izmantotu publisko fondu līdzekļus. Šīs publikācijas samērīgumu apstrīdēja vairāki atbalsta saņēmēji.

Piemērs: Lietā *Volker un Markus Schecke GbR un Hartmut Eifert pret Land Hessen*[40] Tiesai bija jāizspriež, vai ir bijis samērīgs pasākums publicēt, kā tas paredzēts ES tiesību aktos, ES lauksaimniecības subsīdiju saņēmēju vārdus un viņu saņemtās summas.

Tiesa, norādot, ka tiesības uz datu aizsardzību nav absolūtas, iebilda, ka datu, kuros nosaukti divu ES lauksaimniecības atbalsta fondu līdzekļu saņēmēju vārdi un precīzas saņemtās summas, publicēšana tīmeklī ir privātās dzīves neaizskaramības pārkāpums vispār un personas datu aizsardzības pārkāpums konkrēti.

Tiesa uzskatīja, ka tāds Hartas 7. un 8. pantā paredzēto tiesību aizskārums bija paredzēts tiesību aktos un atbilda ES atzītam vispārējas nozīmes mērķim, proti, arī pastiprināt Kopienas fondu izmantošanas caurskatāmību. Tomēr Tiesa uzskatīja, ka fizisku personu – kas ir ES lauksaimniecības atbalsta no abiem minētajiem fondiem saņēmējas – vārdu un precīzu saņemto summu publicēšana bija nesamērīgs pasākums, un nebija attaisnots, ievērojot Hartas 52. panta 1. punktu. Tādējādi Tiesa atzina par daļēji nederīgiem ES tiesību aktus par informācijas publicēšanu par Eiropas lauksaimniecības fondu līdzekļu saņēmējiem.

38 Tiesas 2003. gada 6. marta spriedums lietā C-41/00 P *Interporc Im- und Export GmbH pret Eiropas Kopienu Komisija*, 39. punkts; un Tiesas 2010. gada 29. jūnija spriedums lietā C-28/08 P, *Eiropas Komisija pret The Bavarian Lager Co. Ltd.*, 54. punkts.

39 Padomes 2005. gada 21. jūnija Regula (EK) Nr. 1290/2005 par kopējās lauksaimniecības politikas finansēšanu, OV 2005 L 209; un 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.

40 Tiesas 2010. gada 9. novembra spriedums apvienotajās lietās C-92/09 un C-93/09 *Volker un Markus Schecke GbR un Hartmut Eifert pret Land Hessen*, 47.–52., 58., 66.–67., 75., 86. un 92. punkts.

1.2.3. Brīvība mākslās un zinātnēs

Vēl vienas tiesības uz līdzsvaru starp tiesībām uz privātās dzīves neaizskaramību un uz datu aizsardzību ir brīvība mākslās un zinātnēs, kas konkrēti aizsargāta Hartas 13. pantā. Šīs tiesības izriet pirmkārt no tiesībām uz domas un izpausmes brīvību, un tās ir jāīsteno, ievērojot Hartas 1. pantu (Cilvēka cieņa). ECT uzskata, ka brīvība mākslās ir aizsargāta ar ECK 10. pantu.[41] Uz Hartas 13. pantā garantētajām tiesībām var attiekties arī ierobežojumi, kas atļauti ar ECK 10. pantu.[42]

Piemērs: Lietā *Vereinigung bildender Künstler pret Austriju*[43] Austrijas tiesas aizliedza asociācijai-prasītājai turpināt eksponēt gleznojumu, kurā bija ietvertas dažādu publisku figūru galvu fotogrāfijas, seksuālās pozās. Kāds Austrijas parlamentārietis, kura fotogrāfija bija izmantota gleznojumā, cēla prasību pret asociāciju-prasītāju, lūdzot noteikt aizliegumu eksponēt gleznojumu. Valsts tiesa, apmierinot viņa prasību, izdeva aizliegumu. ECT atkārtoti uzsvēra, ka ECK 10. pants ir piemērojams tādu ideju komunicēšanai, kas aizvaino, šokē vai aizskar valsti vai jebkuru sabiedrības daļu. Tie, kuri radīja, izpildīja, izplatīja vai eksponēja mākslas darbus, veicināja ideju un viedokļu apmaiņu, un valstij bija pienākums nepienācīgi netraucēt viņu vārda brīvībai. Tā kā gleznojums bija kolāža, un tika izmantotas tikai cilvēku galvu fotogrāfijas, bet viņu ķermeņi bija uzgleznoti nereālā un pārspīlētā manierē, ar ko acīmredzami nebija izvirzīts mērķis atspoguļot vai pat dot mājienu uz realitāti, ECT turpmāk apgalvoja, ka „diez vai gleznojumu var uzskatīt par tādu, kas skar [uzgleznotās personas] privātās dzīves detaļas, bet drīzāk tas attiecās uz viņa kā politiķa reputāciju" un ka „šajā statusā [uzgleznotajai personai] bija jāizrāda lielāka iecietība pret kritiku". Izsverot dažādās iesaistītās intereses, ECT konstatēja, ka neierobežots aizliegums turpināt eksponēt gleznojumu ir nesamērīgs. Tiesa secināja, ka ir bijis ECK 10. panta prasību pārkāpums.

Saistībā ar zinātni Eiropas tiesību akti datu aizsardzības jomā atzīst īpašu zinātnes vērtību sabiedrībai. Tāpēc vispārīgie personas datu izmantošanas ierobežojumi tiek samazināti. Gan datu aizsardzības direktīvā, gan 108. konvencijā ir atļauts saglabāt datus zinātniskajai izpētei, kad tie vairs nav vajadzīgi sākotnējam nolūkam, kuram tos vāca. Turklāt datu vēlāku izmantošanu zinātniskajai izpētei neuzskata par

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

42 Paskaidrojumi saistībā ar Pamattiesību Hartu, OV 2007 C 303.

43 ECT 2007. gada 25. janvāra spriedums lietā *Vereinigung bildender Künstler pret Austriju*, prasības pieteikums Nr. 68345/01, jo īpaši sk. 26. un 34. punktu.

nesaderīgu nolūku. Valsts tiesību aktos ir jāizstrādā sīkāki noteikumi, tostarp vajadzīgās garantijas, lai saskaņotu interesi par zinātnisko izpēti ar tiesībām uz datu aizsardzību (sk. arī 3.3.3 un 8.4 iedaļu).

1.2.4. Īpašuma aizsardzība

Tiesības uz īpašuma aizsardzību ir nostiprinātas ECK Pirmā protokola 1. pantā un Hartas 17. panta 1. punktā. Viens svarīgs īpašuma tiesību aspekts ir intelektuālā īpašuma aizsardzība, kas konkrēti pausts Hartas 17. panta 2. punktā. ES tiesību sistēmā ir atrodamas vairākas direktīvas, kuru mērķis ir intelektuālā īpašuma, jo īpaši autortiesību, efektīva aizsardzība. Intelektuālais īpašums ietver ne tikai literāro un mākslas īpašumu, bet arī patentu, preču zīmju un saistītās tiesības.

Kā skaidri izriet no Tiesas prakses, pamattiesības uz īpašumu aizsardzību ir jālīdzsvaro ar citu pamattiesību aizsardzību, jo īpaši, ar tiesībām uz datu aizsardzību.[44] Ir bijuši gadījumi, kad autortiesību aizsardzības iestādes ir prasījušas, lai interneta [pakalpojumu] sniedzēji atklātu interneta datņu koplietošanas platformu lietotāju identitāti. Tādas platformas bieži vien ļauj interneta lietotājiem par brīvu lejupielādēt mūzikas darbus, lai gan minētie darbi ir aizsargāti ar autortiesībām.

Piemērs: Lieta *Promusicae pret Telefónica de España*[45] attiecās uz Spānijas interneta piekļuves sniedzēja *Telefónica* atteikumu atklāt *Promusicae*, bezpeļņas asociācijai, kas apvieno mūzikas ierakstu, kā arī audiovizuālo ierakstu producentus un izdevējus, atsevišķu personu, kam tā sniedza pakalpojumus piekļuvei internetam, personas datus. Promusicae lūdza sniegt minēto informāciju, lai varētu uzsākt civilo tiesvedību pret attiecīgajām personām, kuras, kā apgalvoja Promusicae, izmanto arhīvu apmaiņas programmu, kas ļauj piekļūt fonogrammām, kuru izmantošanas īpašumtiesības ir Promusicae biedriem.

Spānijas tiesa lūdza Tiesai sniegt prejudiciālu nolēmumu, jautājot, vai tādi personas dati ir jāpaziņo, saskaņā ar Kopienas tiesību aktiem, civilā tiesvedībā, lai nodrošinātu autortiesību efektīvu aizsardzību. Tā atsaucās uz Direktīvu 2000/31, Direktīvu 2001/29 un Direktīvu 2004/48, tās lasot arī kopsakarā ar Hartas 17. un 47. pantu. Tiesa secināja, ka minētās trīs direktīvas, kā arī

44 ECT 2013. gada 10. janvāra spriedums lietā *Ashby Donald un citi pret Franciju*, prasības pieteikums Nr. 36769/08.

45 Tiesas 2008. gada 29. janvāra spriedums lietā C-275/06, *Productores de Música de España (Promusicae) pret Telefónica de España SAU*, 54. un 60. punkts.

e-privātuma direktīva (Direktīva 2002/58) neizslēdz iespēju dalībvalstīm paredzēt pienākumu civilā tiesvedībā izpaust personas datus, lai nodrošinātu autortiesību efektīvu aizsardzību.

Tiesa 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.

Tiesa 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 nepamatotos uz tādu šo direktīvu interpretāciju, kas nonāk konfliktā ar šīm pamattiesībām vai citiem Kopienu tiesību vispārējiem principiem – tādiem kā samērīguma princips”.[46]

46 Turpat, 65. un 68. punkts; sk. arī Tiesas 2012. gada 16. februāra spriedumu lietā C-360/10, *SABAM pret Netlog N.V.*

2 Datu aizsardzības terminoloģija

ES	Aplūkotie jautājumi	EP
Personas dati		
Datu aizsardzības direktīva, 2. panta a) punkts Tiesas 2010. gada 9. novembra spriedums apvienotajās lietās C-92/09 un C-93/09 *Volker un Markus Schecke GbR un Hartmut Eifert pret Land Hessen* Tiesas 2008. gada 29. janvāra spriedums lietā C-275/06 *Productores de Música de España (Promusicae)/Telefónica de España SAU*	**Juridiskā definīcija**	108. konvencija, 2. panta a) punkts ECT 2013. gada 14. marta spriedums lietā *Bernh Larsen Holding AS un citi pret Norvēģiju*, prasības pieteikums Nr. 24117/08
Datu aizsardzības direktīva, 8. panta 1. punkts Tiesas 2003. gada 6. novembra spriedums lietā C-101/01 *Bodil Lindqvist*	**Īpašas personas datu kategorijas (sensitīvi dati)**	108. konvencija, 6. pants
Datu aizsardzības direktīva, 6. panta 1. punkta e) apakšpunkts	**Anonimizēti un pseidonimizēti dati**	108. konvencija, 5. panta e) punkts 108. konvencija, Paskaidrojuma ziņojuma 42. pants
Datu apstrāde		
Datu aizsardzības direktīva, 2. panta b) punkts Tiesas 2003. gada 6. novembra spriedums lietā C-101/01 *Bodil Lindqvist*	**Definīcijas**	108. konvencija, 2. panta c) punkts

ES	Aplūkotie jautājumi	EP
Datu lietotāji		
Datu aizsardzības direktīva, 2. panta d) punkts	**Pārzinis**	108. konvencija, 2. panta d) punkts Ieteikums par profilēšanu, 1. panta g) punkts *
Datu aizsardzības direktīva, 2. panta e) punkts Tiesas 2003. gada 6. novembra spriedums lietā C-101/01 *Bodil Lindqvist*	**Personas datu operators**	Ieteikums par profilēšanu, 1. panta h) punkts
Datu aizsardzības direktīva, 2. panta g) punkts	**Saņēmējs**	108. konvencija, papildprotokola 2. panta 1. punkts
Datu aizsardzības direktīva, 2. panta f) punkts	**Trešā persona**	
Piekrišana		
Datu aizsardzības direktīva, 2. panta h) punkts Tiesas 2011. gada 5. maija spriedums lietā C-543/09 *Deutsche Telekom AG pret Bundesrepublik Deutschland*	**Derīgas piekrišanas definīcija un prasības**	Ieteikums par medicīniskajiem datiem, 6. pants, un dažādi turpmāki ieteikumi

Piezīme: * *Eiropas Padome, Ministru komiteja (2010), Ieteikums Nr. Rec(2010)13 dalībvalstīm par fizisko personu aizsardzību attiecībā uz personas datu automātisku apstrādi datu profilu veidošanas [profilēšanas] kontekstā (Ieteikums par profilēšanu), 2010. gada 23. novembrī.*

2.1. Personas dati

Galvenie punkti

- Dati ir personas dati, ja tie attiecas uz identificētu vai vismaz identificējamu personu, datu subjektu.
- Persona ir identificējama, ja bez nesaprātīgām pūlēm ir iespējams iegūt papildu informāciju, kas ļauj identificēt datu subjektu.
- Autentifikācija nozīmē pierādīt, ka konkrētai personai piemīt konkrēta identitāte, un/vai ka tai ir atļauja veikt konkrētas darbības.
- Ir īpašas datu kategorijas, tā dēvētie „sensitīvie dati", kas uzskaitīti 108. konvencijā un datu aizsardzības direktīvā, un kam vajadzīga pastiprināta aizsardzība un tātad tie ir pakļauti īpašam tiesiskajam režīmam.

- Dati ir anonimizēti, ja tajos vairs nav identifikatoru; tie ir pseidonimizēti, ja identifikatori ir šifrēti.
- Pretēji anonimizētiem datiem, pseidonimizēti dati ir personas dati.

2.1.1. „Personas datu" jēdziena galvenie aspekti

Saskaņā ar ES tiesību aktiem, tāpat kā saskaņā ar **EP tiesību aktiem**, „personas dati" tiek definēti kā informācija, kas attiecas uz identificētu vai identificējamu fizisku personu,[47] proti, informācija par personu, kuras identitāte ir vai nu nepārprotami skaidra vai arī to var vismaz noteikt, iegūstot papildu informāciju.

Ja datus par kādu personu apstrādā, šo personu sauc par „datu subjektu".

Persona

Tiesības uz datu aizsardzību tika izstrādātas no tiesībām uz privātās dzīves neaizskaramību. „Privātās dzīves" jēdziens attiecas uz cilvēkiem. Tādējādi fiziskās personas ir primārās labuma guvējas no datu aizsardzības. Vēl, atbilstīgi 29. panta darba grupas atzinumam, tikai *dzīva būtne* ir aizsargāta saskaņā ar Eiropas tiesību aktiem datu aizsardzības jomā.[48]

ECT judikatūra par ECK 8. pantu liecina, ka var būt sarežģīti pilnībā nošķirt privātās un profesionālās dzīves jautājumus.[49]

Piemērs: Lietā *Amann pret Šveici*[50] varas iestādes pārtvēra ar darījumiem saistītu telefona zvanu prasītājam. Pamatojoties uz šo zvanu, varas iestādes veica izmeklēšanu attiecībā uz prasītāju un sagatavoja par prasītāju kartīti valsts drošības kartotēkai. Lai gan pārtveršana attiecās uz telefona sarunu par darījumiem, ECT uzskatīja, ka datu uzglabāšana par šo zvanu ir saistīta ar prasītāja privāto dzīvi. Tā norādīja, ka terminu „privātā dzīve" nedrīkst interpretēt ierobežo-

47 Datu aizsardzības direktīva, 2. panta a) punkts; 108. konvencija, 2. panta a) punkts.

48 29. panta darba grupa (2007), *Atzinums 4/2007 par „personas datu" jēdzienu,* WP 136, 2007. gada 20. jūnijā, 22. lpp.

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

50 ECT 2000. gada 16. februāra spriedums lietā *Amann pret Šveici*, prasības pieteikums Nr. 27798/95, 65. punkts.

joši, jo īpaši tāpēc, ka tiesības uz privātās dzīves neaizskaramību ietver tiesības izveidot un attīstīt attiecības ar citiem cilvēkiem. Turklāt pamatā netika pieļauta iespēja profesionāla vai darījumu rakstura darbību izslēgt no „privātās dzīves" jēdziena. Tāda plaša interpretācija atbilda 108. konvencijas interpretācijai. Vēl ECT konstatēja, ka prasītāja gadījumā iejaukšanās nebija notikusi saskaņā ar tiesību aktiem, jo valsts tiesību aktos nebija specifisku un detalizētu noteikumu par informācijas vākšanu, reģistrēšanu un uzglabāšanu. Tādējādi tā secināja, ka ir bijis ECK 8. panta prasību pārkāpums.

Turklāt, ja arī profesionālās dzīves jautājumi var būt datu aizsardzības priekšmets, šķiet apšaubāmi, ka aizsardzība būtu jāpiešķir tikai fiziskām personām. Tiesības atbilstīgi ECK ir garantētas ne tikai fiziskām personām, bet ikvienam.

Pastāv ECT judikatūra, kurā ir pieņemti spriedumi par juridisko personu prasībām, kurās apgalvots, ka ir pārkāptas to tiesības uz aizsardzību pret attiecīgo personu datu izmantošanu atbilstīgi ECK 8. pantam. Tiesa tomēr šo lietu izskatīja saskaņā ar tiesībām uz dzīvokļa un korespondences, nevis privātās dzīves, neaizskaramību.

Piemērs: Lieta *Bernh Larsen Holding AS un citi pret Norvēģiju*[51] attiecās uz trīs Norvēģijas uzņēmumu iesniegtu sūdzību par nodokļu iestādes lēmumu, kurā tiem bija noteikts iesniegt nodokļu revidentiem visu datora serverī, ko trīs uzņēmumi izmantoja kopīgi, esošo datu kopiju.

ECT konstatēja, ka tāds prasītāju uzņēmumu pienākums bija to tiesību uz „dzīvokļa" un „korespondences" neaizskaramību aizskārums ECK 8. panta nolūkā. Tomēr Tiesa konstatēja, ka nodokļu iestādēm ir efektīvas un pienācīgas garantijas pret ļaunprātīgu izmantošanu: prasītāji uzņēmumi savlaicīgi bija informēti, bija klāt un varēja iesniegt materiālus pārbaudes uz vietas laikā; un materiāls pēc nodokļu pārskatīšanas bija jāiznīcina. Tādos apstākļos bija nodrošināts atbilstošs līdzsvars starp prasītāju uzņēmumu tiesībām uz „dzīvokļa" un „korespondences" neaizskaramību un viņu interesēm aizsargāt savu darbinieku privātumu, no vienas puses, un sabiedrības interesi nodrošināt efektīvu inspekciju nodokļu novērtēšanas nolūkiem, no otras puses. Tiesa uzskatīja, ka tāpēc nav bijis 8. panta prasību pārkāpuma.

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

Atbilstoši 108. konvencijai datu aizsardzība, pirmkārt, ir fizisku personu aizsardzība, tomēr līgumslēdzējas puses var savas valsts tiesību aktos paplašināt aizsardzību un attiecināt to arī uz juridiskām personām, piemēram, uzņēmējsabiedrībām un asociācijām. **ES datu aizsardzības tiesību akti** parasti neattiecas uz juridisko personu aizsardzību attiecībā uz datu, kas uz tiem attiecas, apstrādi. Valstu regulatori var brīvi regulēt šo jautājumu.[52]

Piemērs: Lietā *Volker un Markus Schecke GbR un Hartmut Eifert pret Land Hessen*[53] Tiesa, atsaucoties uz personas datu publicēšanu saistībā ar 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 [...]".[54]

Personas identificējamība

Saskaņā ar ES tiesību aktiem, kā arī saskaņā ar **EP tiesību aktiem** informācija satur datus par personu, ja:

- šajā informācijā ir identificēta persona, vai
- ja persona, lai gan nav identificēta, ir šajā informācijā aprakstīta tā, ka, veicot turpmāku izpēti, ir iespējams atklāt, kas ir datu subjekts.

Abus informācijas veidus vienādi aizsargā Eiropas tiesību akti datu aizsardzības jomā. ECT ir atkārtoti apgalvojusi, ka „personas datu" jēdziens atbilstoši ECK ir tāds pats kā 108. konvencijā, jo īpaši attiecībā uz nosacījumu par saistību ar identificētām vai identificējamām personām.[55]

52 Datu aizsardzības direktīva, preambulas 24. apsvērums.

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

54 Turpat, 52. punkts.

55 Sk. ECT 2000. gada 16. februāra spriedumu lietā *Amann pret Šveici* [GC], prasības pieteikums Nr. 27798/95, 65. un nākamie punkti.

Personas datu juridiskās definīcijas tālāk nepaskaidro, kad personu uzskata par identificētu.[56] Acīmredzot identifikācija prasa elementus, kuri apraksta personu tādā veidā, ka viņš vai viņa ir atšķirams(-a) no visām citām personām un atpazīstama kā indivīds. Personas vārds ir pirmais tādu apraksta elementu piemērs. Izņēmuma gadījumos citiem identifikatoriem var būt līdzīga ietekme kā vārdam. Piemēram, publiskām personām var būt pietiekami norādīt tikai personas amatu, piemēram, Eiropas Komisijas priekšsēdētājs.

Piemērs: Lietā *Promusicae*[57] Tiesa apgalvoja, ka „netiek apstrīdēts, ka *Promusicae* lūgtā noteiktu [zināmas tīmekļa 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 2. panta a) punktā esošo definīciju [..]. Šī tās informācijas sniegšana, ko, kā norāda *Promusicae*, uzkrājusi *Telefónica*, – un ko pēdējā minētā nenoliedz – ir personas datu apstrāde Direktīvas 2002/58 2. panta pirmās daļas izpratnē, aplūkojot to kopskatā ar Direktīvas 95/46 2. panta b) punktu".

Tā kā daudzi vārdi/uzvārdi nav unikāli, personas identitātes noteikšanai var vajadzēt papildu identifikatorus, lai nodrošinātu, ka vienu personu nesajauc ar kādu citu. Bieži izmanto dzimšanas datumu un vietu. Papildus, dažās valstīs ir ieviesti personalizēti numuri, lai labāk nošķirtu pilsoņus. Tehnoloģiskajā laikmetā personu identificēšanai arvien svarīgāki kļūst biometriskie dati, kā pirkstu nospiedumi, digitālās fotogrāfijas vai acu varavīksnenes skenēšana.

Tomēr, lai piemērotu Eiropas tiesību aktus datu aizsardzības jomā, nav vajadzīga datu subjekta kvalitatīva identifikācija; pietiek, ka attiecīgā persona ir identificējama. Personu uzskata par identificējamu, ja informācijā ir identifikācijas elementi, ar kuriem personu tieši vai netieši var identificēt.[58] Atbilstoši datu aizsardzības direktīvas preambulas 26. apsvērumam etalons ir tas, vai ir ticams, ka paredzamajiem informācijas lietotājiem būs pieejami saprātīgi identificēšanas līdzekļi, ko viņi pārvaldīs; te ietilpst trešās personas-saņēmēji (sk. 2.3.2 iedaļu).

56 Sk. arī ECT 2003. gada 13. februāra spriedumu lietā *Odièvre pret Franciju* [GC], prasības pieteikums Nr. 42326/98; un ECT 2012. gada 25. septembra spriedumu lietā *Godelli pret Itāliju*, prasības pieteikums Nr. 33783/09.

57 Tiesas 2008. gada 29. janvāra spriedums lietā C-275/06 *Productores de Música de España (Promusicae)/Telefónica de España SAU*, 45. punkts.

58 Datu aizsardzības direktīva, 2. panta a) punkts.

Piemērs: Kāda vietējā varas iestāde [pašvaldība] nolemj ievākt datus par ātri braucošām mašīnām vietējās ielās. Tā fotografē mašīnas, automātiski reģistrējot laiku un vietu, lai tālāk nodotu datus kompetentajai iestādei un tā var uzlikt sodu tiem, kuri ir pārkāpuši atļauto ātrumu. Datu subjekts iesniedz sūdzību, apgalvojot, ka vietējai varas iestādei atbilstīgi datu aizsardzības tiesību aktiem nav likumīga pamata šādai datu vākšanai. Vietējā varas iestāde apgalvo, ka tā nevāc personas datus. Tā apgalvo, ka valsts reģistrācijas numura zīmes ir dati par anonīmām personām. Vietējai varas iestādei nebija likumīgu pilnvaru piekļūt vispārējam transportlīdzekļu reģistram, lai uzzinātu mašīnas īpašnieka vai šofera identitāti.

Šī argumentācija nav saskaņā ar datu aizsardzības direktīvas preambulas 26. apsvērumu. Ievērojot, ka datu vākšanas nolūks acīmredzami ir identificēt un sodīt ātruma pārkāpējus, ir paredzams, ka notiks centieni veikt identifikāciju. Lai gan vietējām varas iestādēm nav tām tieši pieejamu identifikācijas līdzekļu, tās tālāk nodos datus kompetentajai iestādei, policijai, kurai tādi līdzekļi ir. Preambulas 26. apsvērumā ir konkrēti ietverts scenārijs, kurā ir paredzams, ka nākamie datu saņēmēji, kas nav tiešais datu lietotājs, var censties identificēt personu. Ņemot vērā 26. apsvērumu, vietējās varas iestādes rīcība ir vienāda ar datu vākšanu par identificējamām personām, un tāpēc tai ir vajadzīgs tiesisks pamats atbilstīgi datu aizsardzības tiesību aktiem.

Saskaņā ar EP tiesību aktiem identificējamību saprot līdzīgi. Ieteikuma par maksāšanas datiem[59] 1. panta 2. punktā, piemēram, ir noteikts, ka personu nevar uzskatīt par „identificējamu", ja identifikācijai vajag nesamērīgi ilgu laiku, lielas izmaksas vai daudz darbaspēka.

Autentifikācija

Ar šo procedūru persona spēj pierādīt, ka viņam vai viņai ir noteikta identitāte un/vai pilnvaras darīt noteiktas lietas, piemēram, ieiet drošības zonā vai izņemt naudu no bankas konta. Autentifikāciju var veikt, salīdzinot biometriskos datus, piemēram, fotogrāfiju vai pirkstu nospiedumus pasē ar tās personas datiem, kura ir ieradusies, piemēram, imigrācijas kontroles punktā; vai prasot informāciju, kura būtu jāzina tikai personai ar noteiktu identitāti vai pilnvarām, piemēram, personas identifikācijas numuru (PIN) vai paroli, vai prasot uzrādīt īpašu marķieri, kam jābūt tikai pie

59 EP, Ministru komiteja (1990), Ieteikums Nr. R Rec(90) 19 par personas datu aizsardzību, ko izmanto maksājumiem un citām saistītajām darbībām, 1990. gada 13. septembrī.

personas ar noteiktu identitāti vai pilnvarām, piemēram, īpašu mikroshēmas karti vai atslēgu no bankas seifa. Papildus parolēm vai mikroshēmas kartēm, dažreiz kopā ar PIN, elektroniskie paraksti ir instrumenti, kas īpaši spēj identificēt un autentificēt personu elektroniskajā komunikācijā.

Datu raksturojums

Jebkura veida informācija var būt personas dati, ja vien tā attiecas uz kādu personu.

Piemērs: Priekšnieka veikts darbinieka darba snieguma novērtējums, kas tiek glabāts darbinieka personīgajā lietā, ir personas dati par darbinieku, lai gan tie var vienkārši atspoguļot – pilnībā vai daļēji – priekšnieka personīgo viedokli, piemēram: „darbinieks nevelta sevi pilnībā darbam", un nevis stingri fakti, piemēram: „darbinieks pēdējo sešu mēnešu laikā nav bijis darbā piecas nedēļas".

Personas dati attiecas uz informāciju par personas privāto dzīvi, kā arī informāciju par viņa vai viņas profesionālo vai sabiedrisko dzīvi.

Lietā *Amann case*[60] ECT interpretēja jēdzienu „personas dati" kā tādu, kas nav ierobežots tikai līdz personas privātajai dzīvei (sk. 2.1.1 iedaļu). Šī termina „personas dati" nozīme ir būtiska arī datu aizsardzības direktīvai:

Piemērs: Lietā *Volker un Markus Schecke GbR un Hartmut Eifert pret Land Hessen*[61] Tiesa apgalvoja, ka „[š]ajā sakarā nav nozīmes faktam, ka publicētās ziņas attiecas uz profesionālo darbību [..].Saistībā ar ECPAK 8. panta interpretāciju Eiropas Cilvēktiesību tiesa šajā sakarā ir nospriedusi, ka jēdziens „privātā dzīve" nav tulkojams sašaurināti un ka pamatā netiek pieļauta iespēja profesionālo darbību „izņemt no privātās dzīves" jēdziena [..].

Dati attiecas uz personām arī tad, ja informācijas saturs netieši atklāj datus par personu. Dažos gadījumos, kad ir cieša saikne starp kādu priekšmetu vai notikumu – piemēram, mobilo tālruni, mašīnu, avāriju –, no vienas puses, un personu – piemēram, tā(tās) īpašnieku, lietotāju, upuri –, no otras puses, informācija par priekšmetu vai par notikumu arī ir uzskatāma par personas datiem.

60 Sk. ECT 2000. gada 16. februāra spriedumu lietā *Amann pret Šveici*, prasības pieteikums Nr. 27798/95, 65. punkts.

61 Tiesas 2010. gada 9. novembra spriedums apvienotajās lietās C-92/09 un C-93/09 *Volker un Markus Schecke GbR un Hartmut Eifert pret Land Hessen*, 59. punkts.

Piemērs: Lietā *Uzun pret Vāciju*[62] prasītājs un vēl kāds vīrietis tika uzraudzīti ar šā otra vīrieša mašīnā ievietotas globālās pozicionēšanas sistēmas (GPS) ierīces starpniecību, jo bija aizdomas, ka viņi ir iesaistīti spridzināšanās. Šajā lietā ECT uzskatīja, ka prasītāja novērošana ar GPS starpniecību aizskāra viņa tiesības uz privātās dzīves neaizskaramību, ko aizsargā ECK 8. pants. Tomēr GPS uzraudzība bija notikusi saskaņā ar tiesību aktiem, kā arī samērīga ar likumīgo mērķi – izmeklēt vairākus slepkavību mēģinājumu gadījumus, un tātad nepieciešama demokrātiskā sabiedrībā. Tiesa uzskatīja, ka nav bijis ECK 8. panta prasību pārkāpuma.

Kādā formā dati var būt

Forma, kādā personas datus uzglabā vai izmanto, nav svarīga datu aizsardzības tiesību aktu piemērošanas nolūkiem. Personas datus var saturēt rakstiska vai mutiska komunikācija, kā arī attēli,[63] tostarp slēgtā kontūra televīzijas (*CCTV*) ieraksts[64] vai skaņa.[65] Elektroniski reģistrēta informācija, kā arī informācija uz papīra var būt personas dati; pat cilvēka audu šūnu paraugi var būt personas dati, jo tie reģistrē personas DNS.

2.1.2. Īpašas personas datu kategorijas

Saskaņā ar ES tiesību aktiem, kā arī **EP tiesību aktiem**, ir īpašas personas datu kategorijas, kuras savu īpašību dēļ apstrādes gadījumā var radīt risku datu subjektiem, un tās ir jāsargā pastiprināti. Tāpēc šādu īpašo datu kategoriju („sensitīvo datu") apstrāde ir jāatļauj tikai ar īpašām garantijām.

Definējot sensitīvus datus, gan 108. konvencija (6. pants), gan datu aizsardzības direktīva (8. pants) nosauc šādas kategorijas:

- personas dati, kas atklāj rasi vai etnisko izcelsmi,

62 ECT 2010. gada 2. septembra spriedums lietā *Uzun pret Vāciju*, prasības pieteikums Nr. 35623/05.

63 ECT 2004. gada 24. jūnija spriedums lietā *Von Hannover pret Vāciju*, prasības pieteikums Nr. 59320/00; ECT 2005. gada 11. janvāra spriedums lietā *Sciacca pret Itāliju*, prasības pieteikums Nr. 50774/99.

64 ECT 2003. gada 28. janvāra spriedums lietā *Peck pret Apvienoto Karalisti*, prasības pieteikums Nr. 44647/98; ECT 2010. gada 5. oktobra spriedums lietā *Köpke pret Vāciju*, prasības pieteikums Nr. 420/07.

65 Datu aizsardzības direktīva, preambulas 16. un 17. apsvērums; ECT 2011. gada 25. decembra spriedums lietā *P.G. un J.H. pret Apvienoto Karalisti*, prasības pieteikums Nr. 44787/98, 59. un 60. punkts; ECT 2005. gada 20. septembra spriedums lietā *Wisse pret Franciju*, prasības pieteikums Nr. 71611/01.

- personas dati, kas atklāj politiskos uzskatus, reliģisko vai citu pārliecību, un
- personas dati par veselību vai seksuālo dzīvi.

> Piemērs: Lietā *Bodil Lindqvist*[66] Tiesa apgalvoja, ka „norāde uz faktu, ka persona ir guvusi pēdas savainojumu un atrodas daļējā slimības atvaļinājumā, ir personas dati par veselības stāvokli Direktīvas 95/46 8. panta 1. punkta izpratnē".

Datu aizsardzības direktīva vēl papildus uzskaita „dalību arodbiedrībā" kā sensitīvus datus, jo šī informācija var tuvu norādīt uz politiskajiem uzskatiem vai pārliecību.

108. konvencija uzskata par sensitīviem arī personas datus par kriminālu sodāmību.

Datu aizsardzības direktīvas 8. panta 7. punktā ir dots uzdevums ES dalībvalstīm „paredzēt nosacījumus, ar kādiem var apstrādāt attiecīgās valsts reģistrācijas numuru vai jebkuru citu vispārēja pielietojuma identifikatoru".

2.1.3. Anonimizēti un pseidonimizēti dati

Atbilstoši datu ierobežotas uzglabāšanas principam, kas ietverts gan datu aizsardzības direktīvā, gan 108. konvencijā (un sīkāk apspriests 3. nodaļā), datiem jābūt saglabātiem „veidā, kas pieļauj datu subjektu identifikāciju ne ilgāk, kā tas nepieciešams nolūkiem, kuriem datus vāca vai kuriem tos turpmāk apstrādā".[67] Līdz ar to dati ir jāanonimizē, ja pārzinis vēlas tos saglabāt pēc tam, kad to derīguma termiņš ir beidzies un tie vairs nekalpo savam sākotnējam nolūkam.

Anonimizēti dati

Dati ir anonimizēti, ja no personas datu kopuma ir izņemti visi identificējošie elementi. Informācijā nedrīkst atstāt nevienu elementu, kas, pieliekot saprātīgas pūles, var noderēt attiecīgās(-o) personas(-u) atkārtotai identificēšanai.[68] Kad dati ir veiksmīgi anonimizēti, tie vairs nav personas dati.

Ja personas dati vairs nekalpo savam sākotnējam nolūkam, bet tos vēlas saglabāt personalizētā formā izmantošanai vēsturiskiem, statistiskiem vai zinātniskiem

66 Tiesas 2003. gada 6. novembra spriedums lietā C-101/01 *Bodil Lindqvist*, 51. punkts.

67 Datu aizsardzības direktīva, 6. panta 1. punkta e) apakšpunkts; un 108. konvencija, 5. panta e) punkts.

68 Turpat, preambulas 26. apsvērums.

mērķiem, datu aizsardzības direktīvā un 108. konvencijā ir atļauta šāda iespēja, ar nosacījumu, ka piemēro pienācīgas garantijas pret ļaunprātīgu izmantošanu.[69]

Pseidonimizēti dati

Personas informācijā ir ietverti identifikatori, kā vārds/uzvārds, dzimšanas datums, dzimums un adrese. Kad personas informāciju pseidonimizē, identifikatorus aizstāj ar vienu pseidonīmu. Pseidonimizāciju panāk, piemēram, šifrējot identifikatorus personas datos.

Pseidonimizēti dati nav konkrēti pieminēti ne 108. konvencijas, ne datu aizsardzības direktīvas juridiskajās definīcijās. Tomēr 108. konvencijas Paskaidrojuma ziņojuma 42. pantā ir noteikts, ka „[p]rasība [..] par datu saglabāšanas ar vārdu saistītā formā termiņi nenozīmē, ka dati pēc kāda laika neatgriezeniski jānošķir no personas, uz kuru tie attiecas, vārda/uzvārda, bet nozīmē tikai to, ka nav jābūt iespējamam tūlīt sasaistīt datus un identifikatorus". Šādas sekas var sasniegt, pseidonimizējot datus. Nevienam, kura rīcībā nav atšifrēšanas atslēgas, pseidonimizēti dati nav identificējami bez grūtībām. Saikne ar identitāti joprojām pastāv pseidonīma un atšifrēšanas atslēgas formā. Tie, kuri drīkst izmantot atšifrēšanas atslēgu, bez grūtībām spēj veikt atkārtotu identifikāciju. Ir īpaši jāraugās, lai nepilnvarotas personas nevarētu izmantot atšifrēšanas atslēgas.

Tā kā datu pseidonimizācija ir viens no svarīgākajiem līdzekļiem, lai plašā mērogā nodrošinātu datu aizsardzību, ja nav iespējams pilnībā atturēties no personas datu lietošanas, ir sīkāk jāpaskaidro šīs darbības loģika un sekas.

Piemērs: Teikumu „Čārlzs Spensers, dzimis 1967. gada 3. aprīlī, ir četru bērnu – divu zēnu un divu meiteņu – ģimenes tēvs" var, piemēram, pseidonimizēt šādi:

„Č.S. 1967 ir četru bērnu – divu zēnu un divu meiteņu – ģimenes tēvs"; vai

„324 ir četru bērnu – divu zēnu un divu meiteņu – ģimenes tēvs"; vai

„YESz320l ir četru bērnu – divu zēnu un divu meiteņu – ģimenes tēvs".

69 Turpat, 6. panta 1. punkta e) apakšpunkts, un 108. konvencija, 5. panta e) punkts.

Lietotāji, kuri piekļūst šiem pseidonimizētajiem datiem, parasti nespēs identificēt „Čārlzu Spenseru, dzimušu 1967. gada 3. aprīlī" no „324" vai „YESz3201". Pseidonimizēti dati tādējādi drīzāk būs droši pret ļaunprātīgu izmantošanu.

Pirmais piemērs tomēr ir mazāk drošs. Ja teikums „Č.S. 1967 ir četru bērnu – divu zēnu un divu meiteņu – ģimenes tēvs" tiek lietots mazā ciematā, kurā dzīvo Čārlzs Spensers, Spensera k–gs var būt viegli atpazīstams. Pseidonimizācijas metode skar datu aizsardzības efektivitāti.

Personas dati ar šifrētiem identifikatoriem tiek izmantoti daudzos kontekstos kā līdzeklis, lai paturētu slepenībā personu identitāti. Tas ir jo īpaši noderīgi tad, kad pārziņiem ir jānodrošina, ka viņi aplūko vienus un tos pašus datu subjektus, bet viņiem nevajag vai arī viņi nedrīkst zināt datu subjektu reālās identitātes. Tāds gadījums, piemēram, ir, kad kāds pētnieks pēta tādu pacientu slimības gaitu, kuru identitāte ir zināma tikai slimnīcai, kur viņus ārstē un no kuras pētnieks saņem pseidonimizētās slimības vēstures. Tāpēc pseidonimizācija ir spēcīga saikne privātumu stiprinošas tehnoloģijas arsenālā. Tā var darboties kā svarīgs elements, kad īsteno integrētu privātuma aizsardzību. Tas nozīmē, ka datu aizsardzība ir jāiestrādā progresīvo datu apstrādes sistēmu struktūrā.

2.2. Datu apstrāde

Galvenie punkti

- Termins „apstrāde" attiecas pirmkārt uz automatizētu apstrādi.
- Saskaņā ar ES tiesību aktiem „apstrāde" papildus attiecas uz manuālu apstrādi strukturētās personas datu apstrādes sistēmās.
- Saskaņā ar EP tiesību aktiem „apstrādes" nozīmi var ar valsts tiesību aktiem paplašināt un attiecināt arī uz manuālu apstrādi.

Datu aizsardzība atbilstoši 108. konvencijai un datu aizsardzības direktīvai ir galvenokārt koncentrēta uz automatizētu datu apstrādi.

Saskaņā ar EP tiesību aktiem automatizētas apstrādes definīcija tomēr atzīst, ka starp automatizētām darbībām var būt nepieciešami daži personas datu manuālas apstrādes posmi. Līdzīgi, saskaņā ar ES tiesību aktiem automatizēta datu apstrāde

ir definēta kā „darbības, ko veic ar personas datiem pilnībā vai daļēji ar automatizētiem līdzekļiem".[70]

Piemērs: Lietā *Bodil Lindqvist*[71] Tiesa uzskatīja, ka:

„darbība, kuras ietvaros interneta mājas lapā 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 3. panta 1. punkta izpratnē."

Manuālai datu apstrādei arī vajag datu aizsardzību.

Datu aizsardzība **saskaņā ar ES tiesību aktiem** nekādā veidā nav ierobežota līdz automatizētai datu apstrādei. Attiecīgi, saskaņā ar ES tiesību aktiem datu aizsardzība attiecas uz personas datu apstrādi manuālā personas datu apstrādes sistēmā, tas ir, īpaši strukturētā papīra kartotēkā.[72] Šīs datu aizsardzības paplašināšanas iemesls ir tāds, ka:

- papīra kartotēkas var būt strukturētas tā, lai informāciju varētu atrast ātri un viegli; un

- uzglabājot personas datus strukturētās papīra kartotēkās, ir viegli apiet ierobežojumus, kas tiesību aktos noteikti attiecībā uz automatizētu datu apstrādi.[73]

Saskaņā ar EP tiesību aktiem 108. konvencija galvenokārt regulē datu apstrādi automatizētu datu datnēs.[74] Tā tomēr paredz arī iespēju valsts tiesību aktos paplašināt aizsardzību un attiecināt to arī uz manuālu apstrādi. Daudzas 108. konvencijas Līgumslēdzējas Puses ir izmantojušas šo iespēju un iesniegušas šajā sakarā deklarācijas EP ģenerālsekretāram.[75] Datu aizsardzības paplašinājumam uz šādas

70 108. konvencija, 2. panta c) punkts; un Datu aizsardzības direktīva, 2. panta b) punkts un 3. panta 1. punkts.

71 Tiesas 2003. gada 6. novembra spriedums lietā C-101/01 *Bodil Lindqvist*, 27. punkts.

72 Datu aizsardzības direktīva, 3. panta 1. punkts.

73 Turpat, preambulas 27. apsvērums.

74 108. konvencija, 2. panta b) punkts.

75 Sk. paziņojumus, kas izdarīti saskaņā ar 108. konvencijas 3. panta 2. punkta c) apakšpunktu.

deklarācijas pamata ir jāattiecas uz visu manuālo datu apstrādi, un to nevar ierobežot līdz apstrādei manuālās personas datu apstrādes sistēmās.[76]

Kas attiecas uz ietverto apstrādes darbību raksturu, apstrādes jēdziens ir visaptverošs **gan saskaņā ar ES, gan saskaņā ar EP tiesību aktiem**: „„personas datu apstrāde" [..] ir jebkura ar personas datiem veikta darbība [..] kā vākšana, reģistrēšana, organizēšana, uzglabāšana, piemērošana vai pārveidošana, izgūšana, konsultēšana, izmantošana, atklāšana, pielietojot pārsūtīšanu [nodošanu], izplatīšanu vai darot tos pieejamus citādā veidā, grupēšana vai savienošana, piekļuves noslēgšana [bloķēšana], dzēšana vai iznīcināšana"[77]. Termins „apstrāde" ietver arī darbības, ar kurām dati tiek izņemti no viena pārziņa atbildības un nodoti cita pārziņa atbildībai.

Piemērs: Darba devēji savāc un apstrādā datus par saviem darbiniekiem, tostarp informāciju par viņu algām. Tiesiskais pamats, lai to varētu likumīgi darīt, ir darba līgums.

Darba devējiem būs jānodod sava personāla algas dati nodokļu iestādēm. Šī datu nodošana arī būs „apstrāde" saskaņā ar šā jēdziena nozīmi 108. konvencijā un direktīvā. Tomēr tiesiskais pamats tādai atklāšanai nav darba līgums. Ir jābūt papildu tiesiskajam pamatam apstrādes darbībām, kuru rezultātā darba devējs nodod algas datus nodokļu iestādēm. Šis tiesiskais pamats parasti ir ietverts valsts nodokļu tiesību aktu noteikumos. Bez šādiem noteikumiem datu nodošana būtu nelikumīga apstrāde.

2.3. Personas datu lietotāji

Galvenie punkti

- Ikviens, kurš nolemj apstrādāt citu personu [personas] datus, ir „pārzinis" saskaņā ar datu aizsardzības tiesību aktiem; ja vairākas personas kopīgi pieņem šo lēmumu, tās var būt „kopīgi pārziņi".
- „Personas datu operators" ir juridiski nošķirta vienība, kas apstrādā personas datus pārziņa vārdā.

76 Sk. 108. konvencijas 3. panta 2. punkta formulējumu.

77 Datu aizsardzības direktīva, 2. panta b) punkts. Tāpat sk. arī 108. konvencijas 2. panta c) punktu.

- Personas datu operators kļūst par pārzini, ja viņš vai viņa lieto datus saviem nolūkiem, neievērojot pārziņa instrukcijas.
- Jebkurš, kurš saņem datus no pārziņa, ir „saņēmējs".
- „Trešā persona" ir fiziska vai juridiska persona, kura nerīkojas atbilstoši pārziņa instrukcijām (un nav datu subjekts).
- „Trešā persona-saņēmējs" ir persona vai vienība, kas ir juridiski nošķirta no pārziņa, bet saņem no pārziņa personas datus.

2.3.1. Pārziņi un personas datu operatori

Svarīgākais pārziņa vai personas datu operatora statusa [iegūšanas] rezultāts ir juridiskā atbildība par atbilstību attiecīgajiem pienākumiem saskaņā ar datu aizsardzības tiesību aktiem. Tāpēc šos posteņus drīkst ieņemt tikai tie, kurus var uzskatīt par atbildīgiem saskaņā ar piemērojamajiem tiesību aktiem. Privātajā sektorā tā parasti ir kāda fiziska vai juridiska persona; publiskajā sektorā tā parasti ir kāda iestāde. Citas vienības, piemēram, struktūras vai iestādes bez juridiskas personības, var būt pārziņi vai personas datu operatori tikai tad, ja to paredz īpaši juridiski noteikumi.

Piemērs: Kad *Sunshine* uzņēmuma tirgvedības nodaļa plāno apstrādāt datus tirgus izpētei, *Sunshine* uzņēmums, un nevis tirgvedības nodaļa būs šādas apstrādes pārzinis. Tirgvedības nodaļa nevar būt pārzinis, jo tai nav atsevišķas juridiskas identitātes.

Uzņēmumu grupās mātes uzņēmums un katra filiāle, kas ir atsevišķas juridiskas personas, ir uzskatāmi par atsevišķiem pārziņiem vai personas datu operatoriem. Šā juridiski nošķirtā statusa sekas ir tādas, ka datu nodošanai uzņēmumu grupas biedru starpā vajadzēs īpašu tiesisko pamatu. Nav nekādu privilēģiju, kas ļauj veikt personas datu apmaiņu kā tādu vienas uzņēmumu grupas atsevišķu juridisko personu starpā.

Šajā saistībā jāpiemin privāto personu loma. **Saskaņā ar ES tiesību aktiem** uz privātām personām, kad tās apstrādā datus par citiem tīri personīgā nolūkā vai mājsaimniecības apstākļos, neattiecas datu aizsardzības direktīvas normas; šādas personas nav uzskatāmas par pārziņiem.[78]

78 Datu aizsardzības direktīva, preambulas 12. apsvērums un 3. panta 2. punkta pēdējais ievilkums.

Taču judikatūrā ir atklāts, ka datu aizsardzības tiesību akti tomēr ir jāpiemēro, ja privātā persona, lietojot internetu, publicē datus par citiem.

Piemērs: Tiesa lietā *Bodil Lindqvist*[79] uzskatīja, ka:

„darbība, kuras ietvaros interneta mājas lapā 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" Direktīvas 95/46 3. panta 1. punkta izpratnē".[80]

Tāda personas datu apstrāde attiecas ne tikai uz personiska vai sadzīves rakstura darbībām un ir ārpus datu aizsardzības direktīvas darbības jomas, jo šis izņēmums „ir 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".[81]

Pārzinis

Saskaņā ar ES tiesību aktiem pārzinis ir persona (iestāde, aģentūra, institūcija), kura „viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus".[82] Pārziņa lēmums nosaka, kāpēc un kā dati tiks apstrādāti. **Saskaņā ar EP tiesību aktiem** „pārziņa" definīcijā ir papildus minēts, ka pārzinis nolemj, kuras personas datu kategorijas ir jāuzglabā.[83]

108. konvencijas „pārziņa" definīcijā ir norāde uz turpmāku datu apstrādes kontroles aspektu, kurš ir jāaplūko. Šī definīcija norāda uz jautājumu par to, kurš var likumīgi apstrādāt noteiktus datus definētam nolūkam. Tomēr, ja notiek domājami nelikumīgas apstrādes darbības, un ir jāatrod atbildīgais pārzinis, par pārzini uzskatīs to personu vai vienību, piemēram, uzņēmumu vai iestādi, kas nolēma, ka dati

79 Tiesas 2003. gada 6. novembra spriedums lietā C-101/01 *Bodil Lindqvist*.

80 Turpat, 27. punkts.

81 Turpat, 47. punkts.

82 Datu aizsardzības direktīva, 2. panta d) punkts.

83 108. konvencija, 2. panta d) punkts.

ir jāapstrādā, neatkarīgi no tā, vai tai/tam bija juridiskas pilnvaras to darīt vai nē[84]. Dzēšanas pieprasījums vienmēr jāadresē „faktiskajam" pārzinim.

Pārziņu veikta vienota datu apstrādes kontrole

„Pārziņa" definīcija datu aizsardzības direktīvā paredz, ka var būt arī vairākas juridiski nošķirtas vienības, kuras kopā vai kopīgi ar citiem rīkojas kā pārzinis. Tas nozīmē, ka tās kopīgi nolemj apstrādāt datus kopīgam nolūkam.[85] Tomēr tas ir juridiski iespējams tikai gadījumos, kad īpašs tiesiskais pamats atļauj kopīgi apstrādāt datus kopīgam nolūkam.

Piemērs: Datu bāze, kuru par saviem klientiem-parādniekiem kopīgi pārvalda vairākas kredītiestādes, ir tipisks pārziņu veiktas vienotas datu apstrādes kontroles piemērs. Kad kāds iesniedz pieteikumu par kredītlīnijas atvēršanu bankā, kura ir viens no kopīgajiem pārziņiem, bankas pārbauda datu bāzes, lai palīdzētu tiem pieņemt informētus lēmumus par pieteikuma iesniedzēja kredītspēju.

Regulās nav konkrēti noteikts, vai pārziņu veiktai vienotas datu apstrādes kontrolei vajag, lai kopīgais nolūks būtu vienāds visiem pārziņiem, un vai ir pietiekami, ja viņu nolūki pārklājas tikai daļēji. Tomēr Eiropas mērogā vēl nav pieejama attiecīga judikatūra, un nav skaidrības par sekām attiecībā uz atbildību. 29. panta darba grupa aktīvi aizstāv plašāku šādas pārziņu veiktas vienotas datu apstrādes kontroles jēdziena interpretāciju, lai pieļautu zināmu elastīgumu, kas ņemtu vērā aizvien pieaugošo pašreizējās datu apstrādes realitātes komplicētību.[86] Kāda lieta, kurā ir iesaistīta Vispasaules Starpbanku finanšu telekomunikāciju sabiedrība (SWIFT), atspoguļo darba grupas nostāju.

Piemērs: Tā dēvētajā SWIFT lietā Eiropas banku iestādes izmantoja SWIFT, sākotnēji kā personas datu operatoru, lai nodotu datus banku darījumu laikā. SWIFT, nesaņēmusi no Eiropas banku iestādēm – savām darba devējām – konkrētu rīkojumu par šīs darbības veikšanu, atklāja ASV Valsts kases departamentam šādus banku darījumu datus, kuri tika uzglabāti kādā datošanas

84 Sk. arī 29. panta darba grupas (2010), *Atzinumu 1/2010 par „apstrādātāja" [„pārziņa"] un „personas datu apstrādātāja" [„personas datu operatora"] jēdzienu,* WP 169, Briselē, 2010. gada 16. februārī, 15. lpp.

85 Datu aizsardzības direktīva, 2. panta d) punkts.

86 29. panta darba grupa (2010), *Atzinums 1/2010 par „apstrādātāja" [„pārziņa"] un „personas datu apstrādātāja" [„personas datu operatora"] jēdzienu,* WP 169, Briselē, 2010. gada 16. februārī, 19. lpp.

pakalpojumu centrā Amerikas Savienotajās Valstīs. 29. panta darba grupa, izvērtējot šīs situācijas likumību, secināja, ka Eiropas banku iestādes, kuras nodarbināja SWIFT, tāpat kā pati SWIFT, ir uzskatāmas par kopīgiem pārziņiem, kas bija atbildīgi Eiropas klientu priekšā par viņu datu atklāšanu ASV iestādēm.[87] SWIFT, nolēmusi par atklāšanu, uzņēmās – nelikumīgi – pārziņa lomu; banku iestādes acīmredzami nebija izpildījušas savu pienākumu uzraudzīt savu personas datu operatoru un tāpēc nevarēja tikt pilnībā atbrīvotas no savas pārziņa atbildības. Šāda situācija rada pārziņu veiktu vienotu datu apstrādes kontroli.

Personas datu operators

Personas datu operators **saskaņā ar ES tiesību aktiem** ir definēts kā persona, kas apstrādā personas datus pārziņa vārdā.[88] Personas datu operatoram uzticētās darbības var būt ierobežotas līdz ļoti konkrētam uzdevumam vai būt samērā vispārīgas un visaptverošas.

Saskaņā ar EP tiesību aktiem „personas datu operatora" nozīme ir tāda pati kā saskaņā ar ES tiesību aktiem.

Personas datu operatori, papildus datu apstrādei citu personu labā, arī paši būs datu pārziņi saistībā ar apstrādi, ko tie veic saviem nolūkiem, piemēram, savu darbinieku, pārdoto preču un pārskatu pārvaldībai.

Piemēri: *Everready* uzņēmuma specializācija ir datu apstrāde citu uzņēmumu cilvēkresursu datu pārvaldībai. Šajā funkcijā *Everready* ir personas datu operators.

Kad *Everready* apstrādā savu darbinieku datus, tas tomēr ir datu apstrādes darbību pārzinis, lai izpildītu sava kā darba devēja uzdevumu.

Attiecības starp pārzini un personas datu operatoru

Kā mēs redzējām, pārzini definē kā personu, kas nosaka apstrādes nolūkus un līdzekļus.

87 29. panta darba grupa (2006), *Atzinums 10/2006 par personas datu apstrādi, ko veic Society for Worldwide Interbank Financial Telecommunications (SWIFT)*, WP 128, Briselē, 2006. gada 22. novembrī.

88 Datu aizsardzības direktīva, 2. panta e) punkts.

Piemērs: *Sunshine* uzņēmuma direktors nolemj, ka *Moonlight* uzņēmumam, tirgus analīzes speciālistam, jāveic *Sunshine* klientu datu tirgus analīze. Lai gan uzdevums noteikt apstrādes līdzekļus tādējādi tiks deleģēts uzņēmumam *Moonlight*, *Sunshine* uzņēmums paliek pārzinis, un *Moonlight* ir tikai personas datu operators, jo saskaņā ar līgumu *Moonlight* var izmantot *Sunshine* uzņēmuma klientu datus tikai *Sunshine* noteiktajiem nolūkiem.

Ja pilnvaras noteikt apstrādes līdzekļus deleģē personas datu operatoram, pārzinim tomēr jāspēj ietekmēt personas datu operatora lēmumus par apstrādes līdzekļiem. Vispārējā atbildība joprojām ir uzlikta pārzinim, kuram jāuzrauga personas datu operatori, lai nodrošinātu, ka viņu lēmumi atbilst datu aizsardzības tiesību aktiem. Tāpēc līgums, kas aizliedz pārzinim ietekmēt personas datu operatora lēmumus, iespējams, jāinterpretē kā tāds, kura rezultātā iestājas pārziņu veikta vienota datu apstrādes kontrole, kur abas līgumslēdzējas puses kopīgi īsteno pārziņa pienākumus.

Turpmāk, ja personas datu operators neievēro pārziņa noteiktos datu izmantošanas ierobežojumus, personas datu operators būs kļuvis par pārzini vismaz tiktāl, ciktāl tas ir pārkāpis pārziņa instrukcijas. Tas visdrīzāk padarīs personas datu operatoru par pārzini, kurš rīkojas nelikumīgi. Savukārt sākotnējam pārzinim būs jāpaskaidro, kā personas datu operatoram bija iespējams pārsniegt savas pilnvaras. 29. panta darba grupai šādos gadījumos ir tendence prezumēt pārziņu veiktu vienotu datu apstrādes kontroli, jo tādējādi vislabāk tiek aizsargātas datu subjektu intereses.[89] Svarīgam pārziņu veiktas vienotas datu apstrādes kontroles rezultātam jābūt solidārai atbildībai par kaitējumiem, jo tāda atbildība piešķir datu subjektiem plašāku tiesiskās aizsardzības līdzekļu klāstu.

Var rasties problēmas arī ar atbildības sadali, ja pārzinis ir mazs uzņēmums, bet personas datu operators – liels korporatīvs uzņēmums, kuram ir iespēja diktēt savu pakalpojumu nosacījumus. Šādos apstākļos tomēr 29. panta darba grupa uzskata, ka atbildības standartu nedrīkst pazemināt, pamatojoties uz ekonomiskā līdzsvara trūkumu, un ka ir jāsaglabā izpratne par pārziņa jēdzienu.[90]

89 29. panta darba grupa (2010), *Atzinums 1/2010 par „apstrādātāja" [„pārziņa"] un „personas datu apstrādātāja" [„personas datu operatora"] jēdzienu,* WP 169, Briselē, 2010. gada 16. februārī, 25. lpp.; un 29. panta darba grupa (2006), *Atzinums 10/2006 par personas datu apstrādi, ko veic Society for Worldwide Interbank Financial Telecommunications (SWIFT)*, WP 128, Briselē, 2006. gada 22. novembrī.

90 29. panta darba grupa (2010), *Atzinums 1/2010 par „apstrādātāja" [„pārziņa"] un „personas datu apstrādātāja" [„personas datu operatora"] jēdzienu,* WP 169, Briselē, 2010. gada 16. februārī, 26. lpp.

Skaidrības un caurskatāmības labad sīka informācija par attiecībām starp pārzini un personas datu operatoru ir jāreģistrē rakstiskā līgumā.[91] Ja tāda līguma nav, tad nav ievērots pārziņa pienākums nodrošināt rakstisku dokumentāciju par savstarpējiem pienākumiem, un var tikt noteikts sods.[92]

Personas datu operatori var vēlēties deleģēt noteiktus uzdevumus papildu personas datu apakšoperatoriem. Tas ir juridiski pieļaujams un būs sīkāk atkarīgs no pārziņa un personas datu operatora līguma noteikumiem, tostarp par to, vai pārziņa atļauja ir nepieciešama katrā atsevišķā gadījumā un vai pietiek tikai ar informēšanu.

Saskaņā ar EP tiesību aktiem iepriekš paskaidroto pārziņa un personas datu operatora jēdzienu interpretācija ir piemērojama pilnībā, kā to pierāda atbilstoši 108. konvencijai izstrādātie ieteikumi.[93]

2.3.2. Saņēmēji un trešās personas

Atšķirības pamatā starp šīm abām personu vai vienību kategorijām, ko ieviesa ar datu aizsardzības direktīvu, galvenokārt ir viņu attiecības ar pārzini un, līdz ar to, viņu pilnvaras piekļūt pārziņa rīcībā esošajiem datiem.

„Trešā persona" ir kāds, kas ir juridiski nošķirts no pārziņa. Tāpēc datu atklāšanai trešām personām vienmēr vajadzēs specifisku tiesisko pamatu. Atbilstoši datu aizsardzības direktīvas 2. panta f) punktam trešā persona ir „jebkura fiziska vai juridiska persona, valsts iestāde, aģentūra vai jebkura cita struktūra, kura nav datu subjekts, personas datu apstrādātājs [pārzinis], apstrādātājs [personas datu operators] un personas, kuras ir pilnvarotas apstrādāt datus personas datu apstrādātāja [pārziņa] vai apstrādātāja [personas datu operatora] tiešā vadībā". Tas nozīmē, ka personas, kuras strādā no pārziņa juridiski nošķirtas organizācijas labā – pat ja šī organizācija pieder tai pašai uzņēmumu grupai vai holdingam – būs „trešā persona" (vai „trešai personai" piederīga). No otras puses, banku filiāles, kuras apstrādā klientu kontus sava centrālā biroja tiešā vadībā, nebūs „trešās personas".[94]

91 Datu aizsardzības direktīva, 17. panta 3. un 4. punkts.

92 29. panta darba grupa (2010), *Atzinums 1/2010 par „apstrādātāja" [„pārziņa"] un „personas datu apstrādātāja" [„personas datu operatora"] jēdzienu,* WP 169, Briselē, 2010. gada 16. februārī, 27. lpp.

93 Sk., piemēram, Ieteikumu par profilēšanu, 1. pants.

94 29. panta darba grupa (2010), *Atzinums 1/2010 par „apstrādātāja" [„pārziņa"] un „personas datu apstrādātāja" [„personas datu operatora"] jēdzienu,* WP 169, Briselē, 2010. gada 16. februārī, 31. lpp.

„Saņēmējs" ir plašāks termins nekā „trešā persona". Datu aizsardzības direktīvas 2. panta g) punkta nozīmē saņēmējs ir „fiziska vai juridiska persona, valsts iestāde, aģentūra vai jebkura cita struktūra, kurai tiek atklāti dati, vai tās ir trešās personas vai nav". Šis saņēmējs var būt persona ārpus pārziņa vai personas datu operatora struktūras – tad tā būtu trešā persona – vai kāds pārziņa vai personas datu operatora struktūrā, kā darbinieks vai cita nodaļa tajā pašā uzņēmumā vai iestādē.

Nošķiršana starp saņēmējiem un trešām personām ir svarīga tikai likumīgas datu atklāšanas nosacījumu dēļ. Pārziņa vai personas datu operatora darbinieki var bez turpmākām juridiskām prasībām būt personas datu saņēmēji, ja viņi ir iesaistīti pārziņa vai personas datu operatora apstrādes darbībās. No otras puses, trešā persona, kas ir juridiski nošķirta no pārziņa vai personas datu operatora, nav pilnvarota izmantot pārziņa apstrādātos personas datus, izņemot speciālus gadījumus, kad tam ir speciāls juridiskais pamats. Tāpēc datu „trešām personām-saņēmējām" vienmēr vajadzēs tiesisku pamatu, lai likumīgi saņemtu personas datus.

Piemērs: Personas datu operatora darbinieks, kas izmanto personas datus saistībā ar uzdevumu, ko darba devējs viņam vai viņai uzticējis, ir datu saņēmējs, bet ne trešā persona, jo viņš vai viņa izmanto datus personas datu operatora vārdā un ievērojot viņa instrukcijas.

Tomēr, ja tas pats darbinieks nolemj izmantot datus, kuriem viņš vai viņa spēj piekļūt kā personas datu operatora darbinieks, saviem nolūkiem un pārdod tos citam uzņēmumam, tad darbinieks ir rīkojies kā trešā persona. Viņš vai viņa vairs neievēro personas datu operatora (darba devēja) rīkojumus. Kā trešai personai, darbiniekam vajadzēs tiesisku pamatu datu iegūšanai un pārdošanai. Šajā piemērā darba devējam, protams, nav tāda tiesiska pamata, tāpēc minētās darbības ir nelikumīgas.

2.4. Piekrišana

Galvenie punkti

- Piekrišanai kā tiesiskam pamatam personas datu apstrādei ir jābūt brīvai, informētai un konkrētai.
- Piekrišanai jābūt nepārprotami dotai. Piekrišana var tikt dota konkrēti vai noklusēti, rīkojoties tā, ka nav šaubu, ka datu subjekts piekrīt savu datu apstrādei.

- Sensitīvu datu apstrādei uz piekrišanas pamata vajag skaidri paustu piekrišanu.
- Piekrišanu var atsaukt jebkurā laikā.

Piekrišana ir „jebkurš labprātīgi sniegts datu subjekta vēlmju konkrēts un paziņots norādījums".[95] Daudzos gadījumos tā ir tiesiskais pamats likumīgai datu apstrādei (sk. 4.1 iedaļu).

2.4.1. Derīgas piekrišanas elementi

ES tiesības izklāsta trīs elementus, kuriem jāpastāv, lai piekrišana būtu derīga, un kuru mērķis ir garantēt, lai datu subjekti tiešām būtu gribējuši piekrist savu datu izmantošanai:

- uz datu subjektu, viņam dodot piekrišanu, nedrīkst būt izdarīts spiediens;
- datu subjektam jābūt pienācīgi informētam par piekrišanas priekšmetu un sekām; un
- piekrišanas tvērumam jābūt saprātīgi konkrētam.

Tikai visu minēto prasību izpildes gadījumā piekrišana būs derīga datu aizsardzības tiesību aktu nozīmē.

108. konvencijā nav piekrišanas definīcijas – tas ir atstāts valsts tiesību aktu ziņā. Tomēr **saskaņā ar EP tiesību aktiem** derīgas piekrišanas elementi atbilst tiem, kas paskaidroti iepriekš, kā to paredz ieteikumi, kas ir izstrādāti atbilstoši 108. konvencijai.[96] Piekrišanas prasības ir tās pašas kas attiecībā uz derīgu nodomu deklarāciju atbilstoši Eiropas civiltiesību aktiem.

Protams, ka derīgai piekrišanai saistībā ar datu aizsardzību piemēro arī papildu prasības atbilstoši civiltiesību aktiem, piemēram, par tiesību un rīcības spēju, jo šādas prasības ir juridiski pamata priekšnoteikumi. Nederīga personu, kam nav tiesību un rīcības spējas, piekrišana nozīmē, ka nebūs tiesiska pamata šādu personu datu apstrādei.

95 Datu aizsardzības direktīva, 2. panta h) punkts.

96 Sk., piemēram, 108. konvenciju, Ieteikuma par statistikas datiem 6. punktu.

Piekrišanu var dot konkrēti[97] vai noklusēti. Pirmajā gadījumā nav šaubu par datu subjekta nodomiem, un šādu konkrētu piekrišanu var dot mutiski vai rakstiski; otrajā gadījumā piekrišanu secina no apstākļiem. Ikvienai piekrišanai jābūt dotai nepārprotami.[98] Tas nozīmē, ka nav jāpastāv pamatotām šaubām par to, ka datu subjekts ir vēlējies paziņot savu piekrišanu savu datu apstrādei. Secinājums par piekrišanu bezdarbības gadījumā piemēram, nespēj sniegt nepārprotamu piekrišanu. Ja apstrādājamie dati ir sensitīvi, skaidri pausta piekrišana ir obligāta un tai jābūt nepārprotamai.

Brīva piekrišana

Brīva piekrišana var būt derīga tikai tad, "kad datu subjektam ir reālas izvēles iespējas bez maldināšanas, iebiedēšanas, piespiešanas vai ievērojamu negatīvu seku riska, ja persona nepiekrīt datu apstrādei".[99]

Piemērs: Daudzās lidostās pasažieriem, lai nokļūtu iekāpšanas zonā, ir jāiet cauri [ķermeņa] drošības skeneriem.[100] Tā kā skenēšanas laikā tiek apstrādāti pasažieru personas dati, apstrādei jāatbilst kādam no datu aizsardzības direktīvas 7. pantā minētajiem tiesiskajiem pamatiem (sk. 4.1.1 iedaļu). Dažreiz pasažierus informē, ka iešana cauri drošības skeneriem ir brīvprātīga, lai datu apstrādi varētu pamatot ar viņu piekrišanu. Pasažieri tomēr var bīties, ka viņu atteikums iet cauri drošības skeneriem radīs aizdomas vai kļūs par papildu kontroles pasākumu, piemēram, personas fiziskas pārmeklēšanas, iemeslu, Daudzi pasažieri piekrīt skenēšanai, jo tādējādi viņi izvairās no potenciāliem sarežģījumiem vai kavēšanās. Šāda piekrišana, domājams, nav pietiekami brīva.

Tādējādi derīgs likumīgs pamats var būt rodams tikai likumdevēja aktā, kura pamatā ir datu aizsardzības direktīvas 7. panta e) punkts, kas nosaka, ka pasažierim ir pienākums sadarboties svarīgāku sabiedrības interešu vārdā. Šādā tiesību aktā varētu paredzēt arī izvēles iespēju starp skenēšanu un fizisku pārmeklēšanu, bet tikai kā robežkontroles papildu pasākumu daļu, kas vajadzīgi īpašos

97 Datu aizsardzības direktīva, 8. panta 2. punkts.

98 Turpat, 7. panta a) punkts un 26. panta 1. punkts.

99 Sk. arī 29. panta darba grupas (2011) *Atzinumu 15/2011 par jēdziena „piekrišana" definīciju*, WP 187, Briselē, 2011. gada 13. jūlijā, 12. lpp.

100 Šis piemērs ir ņemts no „Turpat, 15. lpp."

apstākļos. Tieši to Eiropas Komisija 2011. gadā ir izklāstījusi divās regulās par drošības skeneriem.[101]

Brīva piekrišana var būt apdraudēta arī subordinācijas gadījumos, kad pastāv nozīmīgs ekonomiskā vai cita līdzsvara trūkums starp pārzini, kas nodrošina piekrišanu, un datu subjektu, kas sniedz piekrišanu.[102]

Piemērs: Liels uzņēmums plāno izveidot direktoriju [katalogu], kurā ievietot visu darbinieku vārdus/uzvārdus, viņu funkciju uzņēmumā un viņu darījumu adreses, ar vienīgo nolūku uzlabot uzņēmuma iekšējo komunikāciju. Personāla daļas vadītājs ierosina pievienot direktorijā katra darbinieka fotogrāfiju, lai, piemēram, būtu vieglāk atpazīt kolēģus sanāksmēs. Darbinieku pārstāvji pieprasa, lai tas tiktu darīts tikai ar katra individuāla darbinieka piekrišanu.

Šādā situācijā darbinieka piekrišana ir jāatzīst par tiesisku pamatu fotogrāfiju apstrādei direktorijā, jo ir skaidrs, ka fotogrāfijas publicēšanai direktorijā pašai par sevi nav negatīvu seku, un turklāt ir ticami, ka darbiniekam nebūs jāsaskaras ar negatīvu darba devēja attieksmi, ja viņš vai viņa nepiekritīs savas fotogrāfijas publicēšanai direktorijā.

Tas tomēr nenozīmē, ka piekrišana nekad nevar būt derīga apstākļos, kur nepiekrišanai būtu negatīvas sekas. Ja, piemēram, nepiekrītot saņemt lielveikala klienta karti, vienīgās sekas būs atlaižu nesaņemšana no noteiktu preču cenas, tad piekrišana joprojām ir derīgs tiesiskais pamats to klientu personas datu apstrādei, kuri piekrita saņemt tādu karti. Uzņēmuma un klienta starpā nav subordinācijas situācijas, un nepiekrišanas sekas nav pietiekami nopietnas datu subjektam, lai kavētu brīvu izvēli.

No otras puses, ikreiz, kad pietiekami svarīgas preces vai pakalpojumus var saņemt tikai un vienīgi, ja trešām pusēm tiek atklāti noteikti personas dati, datu subjekta

101 Komisijas 2011. gada 10. novembra Regula (ES) Nr. 1141/2011 par grozījumiem Regulā (EK) Nr. 272/2009, ar ko papildina vispārējos civilās aviācijas drošības pamatstandartus, attiecībā uz drošības skeneru izmantošanu ES lidostās, OV 2011 L 293, un Komisijas 2011. gada 11. novembra Īstenošanas regula (ES) Nr. 1147/2011 par grozījumiem Regulā (ES) Nr. 185/2010, ar ko īsteno kopīgus pamatstandartus civilās aviācijas drošības jomā, attiecībā uz drošības skeneru izmantošanu ES lidostās, OV 2011 L 294.

102 Sk. arī 29. panta darba grupa (2001), *Atzinums 8/2001 par personas datu apstrādi nodarbinātības [nodarbināšanas] jomā*, WP 48, Briselē, 2001. gada 13. septembrī; un 29. panta darba grupa (2005), *Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta vienotu interpretāciju,* WP 114, Briselē, 2005. gada 25. novembrī.

piekrišanu savu datu atklāšanai parasti nevar uzskatīt par brīvu lēmumu un tādējādi tā nav derīga atbilstīgi datu aizsardzības tiesību aktam.

Piemērs: Pasažieru paustu atļauju aviosabiedrībai, lai tā nodod tā sauktos pasažieru datu reģistrus (PDR), proti, datus par viņu identitāti, ēšanas paradumiem vai veselības problēmām konkrētas ārvalsts imigrācijas iestādēm, nevar uzskatīt par derīgu piekrišanu atbilstīgi datu aizsardzības tiesību aktam, jo ceļojošiem pasažieriem nav izvēles, ja viņi vēlas apmeklēt attiecīgo valsti. Lai tādus datus nodotu likumīgi, ir vajadzīgs cits tiesiskais pamats, nevis piekrišana: visdrīzāk īpašs tiesību akts.

Informēta piekrišana

Datu subjektam pirms lēmuma pieņemšanas jābūt pietiekamai informācijai. To, vai sniegtā informācija ir vai nav pietiekama, var nolemt tikai katrā konkrētā gadījumā. Parasti informēta piekrišana ietvers precīzu un viegli saprotamu priekšmeta, kam vajag piekrišanu, aprakstu un – papildus – izklāstu par piekrišanas vai nepiekrišanas sekām. Informācijā lietotajai valodai jābūt pielāgotai paredzamajiem informācijas adresātiem.

Informācijai jābūt arī viegli pieejamai datu subjektam. Informācijas pieejamība un redzamība ir svarīgi elementi. Tiešsaistes vidē slāņaini informācijas paziņojumi var būt labs risinājums, jo papildus konspektīvai informācijas versijai datu subjekts var piekļūt arī plašākai versijai.

Specifiska piekrišana

Lai piekrišana būtu derīga, tai jābūt arī specifiskai. Tas iet roku rokā ar informācijas, kas sniegta par piekrišanas objektu, kvalitāti. Šajā saistībā būtiskas būs vidusmēra datu subjekta pamatotas cerības. Datu subjekta piekrišana atkal ir jālūdz, ja tiks pievienotas vai mainītas apstrādes darbības tādā veidā, ko saprātīgi nevarēja paredzēt, kad tika dota sākotnējā piekrišana.

Piemērs: Lietā *Deutsche Telekom AG*[103] Tiesa skatīja jautājumu par to, vai telekomunikāciju pakalpojumu sniedzējam, kuram bija jānodod tālāk personas dati par abonentiem saskaņā ar *Direktīvas par privāto dzīvi un elektronisko komu-*

103 Tiesas 2011. gada 5. maija spriedums lietā C-543/09 *Deutsche Telekom AG pret Vāciju*; sk. it īpaši 53. un 54. punktu.

nikāciju[104] 12. pantu, bija vajadzīga atjaunota piekrišana no datu subjektiem, jo saņēmēji nebija nosaukti sākumā, kad piekrišana tika dota.

Tiesa uzskatīja, ka atbilstīgi minētajam pantam atjaunota piekrišana pirms datu tālāknodošanas nebija vajadzīga, jo datu subjektiem atbilstīgi šim noteikumam bija iespēja dot piekrišanu tikai apstrādes nolūkā, kas ir viņu datu publicēšana, un nevarēja izvēlēties starp dažādajām direktorijām, kurās šie dati varēja tikt publicēti.

Kā Tiesa uzsvēra, „interpretējot Direktīvas par privāto dzīvi un elektronisko komunikāciju 12. pantu kontekstuāli un sistēmiski, ir jāsecina, ka piekrišana atbilstoši 12. panta 2. punktam attiecas uz personas datu publicēšanas publiskā sarakstā nolūku, nevis uz attiecīgā abonentu saraksta pakalpojumu sniedzēja personu".[105] Turklāt, „personas datu publicēšana abonentu sarakstā, kam ir īpašs nolūks, abonentam pati par sevi rada zaudējumus"[106], un nevis tas, kas ir šīs publikācijas autors.

2.4.2. Tiesības atsaukt piekrišanu jebkurā laikā

Datu aizsardzības direktīva nepiemin vispārējas tiesības jebkurā laikā atsaukt piekrišanu. Tomēr tiek plaši prezumēts, ka tādas tiesības pastāv un ka datu subjektam ir jābūt iespējai tās īstenot pēc sava ieskata. Nedrīkst būt nedz prasības pamatot atsaukumu, nedz negatīvu seku riska ārpus ieguvumu, kuri var izrietēt no iepriekš saskaņotās datu izmantošanas, tvēruma.

Piemērs: Klients piekrīt saņemt reklāmas pastu uz adresi, ko viņš vai viņa norāda datu pārzinim. Ja klients atsauc piekrišanu, pārzinim tūlīt pat jāpārtrauc reklāmas pasta sūtīšana. Tam nedrīkst būt negatīvu seku, piemēram, komisijas naudas iekasēšanas.

Ja klients saņēma 5 % atlaidi no viesnīcas istabas cenas apmaiņā pret piekrišanu, ka viņa vai viņas datus izmanto reklāmas pastam, atsaucot piekrišanu saņemt reklāmas pastu kaut kad vēlāk, minētā atlaide nebūtu jāatmaksā.

104 Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīvā 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*).

105 Tiesas 2011. gada 5. maija spriedums lietā C-543/09 *Deutsche Telekom AG pret Vāciju*; sk. it īpaši 61. punktu.

106 Turpat, sk. it īpaši 62. punktu.

3

Eiropas tiesību aktu datu aizsardzības jomā galvenie principi

ES	Aplūkotie jautājumi	EP
Datu aizsardzības direktīva, 6. panta 1. punkta a) un b) apakšpunkts Tiesas 2008. gada 16. decembra spriedums lietā C-524/06 *Huber pret Vāciju* Tiesas 2010. gada 9. novembra spriedums apvienotajās lietās C-92/09 un C-93/09 *Volker un Markus Schecke GbR un Hartmut Eifert pret Land Hessen*	**Likumīgas datu apstrādes princips**	108. konvencija, 5. panta a) un b) punkts ECT 2000. gada 4. maija spriedums lietā *Rotaru pret Rumāniju*, prasības pieteikums Nr. 28341/95 ECT 2002. gada 22. oktobra spriedums lietā *Taylor-Sabori pret Apvienoto Karalisti*, prasības pieteikums Nr. 47114/99 ECT 2003. gada 28. janvāra spriedums lietā *Peck pret Apvienoto Karalisti*, prasības pieteikums Nr. 44647/98 ECT 2011. gada 18. oktobra spriedums lietā *Khelili pret Šveici*, prasības pieteikums Nr. 16188/07 ECT 1987. gada 26. marta spriedums lietā *Leander pret Zviedriju*, prasības pieteikums Nr. 9248/81
Datu aizsardzības direktīva, 6. panta 1. punkta b) apakšpunkts	**Datu apstrādes mērķa noteikšanas un apstrādes ierobežošanas princips**	108. konvencija, 5. panta b) punkts

ES	Aplūkotie jautājumi	EP
	Datu kvalitātes principi	
Datu aizsardzības direktīva, 6. panta 1. punkta c) apakšpunkts	**Datu būtiskums**	108. konvencija, 5. panta c) punkts
Datu aizsardzības direktīva, 6. panta 1. punkta d) apakšpunkts	**Datu precizitāte**	108. konvencija, 5. panta d) punkts
Datu aizsardzības direktīva, 6. panta 1. punkta e) apakšpunkts	**Datu ierobežota saglabāšana**	108. konvencija, 5. panta e) punkts
Datu aizsardzības direktīva, 6. panta 1. punkta e) apakšpunkts	**Izņēmums zinātniskās izpētes un statistiskiem nolūkiem**	108. konvencija, 9. panta 3. punkts
Datu aizsardzības direktīva, 6. panta 1. punkta a) apakšpunkts	**Godprātīgas apstrādes princips**	108. konvencija, 5. panta a) punkts ECT 2009. gada 27. oktobra spriedums lietā *Haralambie pret Rumāniju*, prasības pieteikums Nr. 21737/03 ECT 2009. gada 6. novembra spriedums lietā *K.H. un citi pret Slovākiju*, prasības pieteikums Nr.32881/04
Datu aizsardzības direktīva, 6. panta 2. punkts	**Atbildības princips**	

108. konvencijas 5. pantā izklāstītie principi nostiprina Eiropas tiesību aktu datu aizsardzības jomā būtību. Tie ir ietverti arī datu aizsardzības direktīvas 6. pantā kā sākuma punkts sīkākiem noteikumiem, kas izklāstīti nākamajos direktīvas pantos. Visiem vēlākajiem tiesību aktiem, ko EP vai ES līmenī pieņem datu aizsardzības jomā, jāatbilst šiem principiem, un tie jāpatur prātā, interpretējot šādus tiesību aktus. Jebkuri šādu pamatprincipu izņēmumi vai ierobežojumi jāparedz valsts līmenī;[107] tie jānosaka tiesību aktos, ar tiem jācenšas sasniegt likumīgs mērķis, un tiem jābūt nepieciešamiem demokrātiskā sabiedrībā. Jābūt izpildītiem visiem trim nosacījumiem.

107 108. konvencija, 9. panta 2. punkts; Datu aizsardzības direktīva, 13. panta 2. punkts.

3.1. Likumīgas datu apstrādes princips

Galvenie punkti

- Lai saprastu likumīgas datu apstrādes principu, ir jāatsaucas uz nosacījumiem, ar kādiem var likumīgi ierobežot tiesības uz datu aizsardzību, ņemot vērā Hartas 52. panta 1. punktu un prasības par pamatotu aizskārumu atbilstoši ECK 8. panta 2. punktam.
- Attiecīgi, personas datu apstrāde ir likumīga tikai tad, ja tā:
  - ir saskaņā ar tiesību aktiem; un
  - cenšas sasniegt likumīgu mērķi; un
  - ir nepieciešama demokrātiskā sabiedrībā, lai sasniegtu likumīgu mērķi.

Saskaņā ar ES un EP datu aizsardzības tiesību aktiem likumīgas datu apstrādes princips ir pirmais nosauktais princips; tas ir izteikts gandrīz identiskos terminos 108. konvencijas 5. pantā un datu aizsardzības direktīvas 6. pantā.

Nevienā no minētajiem noteikumiem nav ietverta definīcija, kas ir „likumīga datu apstrāde". Lai saprastu šo juridisko terminu, ir jāatsaucas uz attaisnotu aizskārumu saskaņā ar ECK, kas interpretēta ECT judikatūrā, un uz likumīgas ierobežošanas nosacījumiem atbilstoši Hartas 52. pantam.

3.1.1. Pamatota aizskāruma prasības atbilstoši ECK

Personas datu apstrāde var veidot datu subjekta tiesību uz privātās dzīves neaizskaramību aizskārumu. Tiesības uz privātās dzīves neaizskaramību tomēr nav absolūtas tiesības, bet tās jālīdzsvaro un jāsaskaņo ar citām likumīgām interesēm – vai tās būtu citu personu (privātas intereses) vai sabiedrības kopumā (vispārējās nozīmes jeb publiskas intereses).

Nosacījumi, kuros valsts iejaukšanās ir pamatota, ir šādi:

Saskaņā ar tiesību aktiem

Atbilstīgi 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".[108] Norma ir paredzama, „tā ir formulēta pietiekami precīzi, lai dotu iespēju ikvienai personai – attiecīgā gadījumā saņemot atbilstošu padomu – regulēt savu rīcību".[109] „Attiecībā uz „tiesību aktu" prasītā precizitātes pakāpe šajā saistībā būs atkarīga no konkrētā temata."[110]

Piemērs: lietā *Rotaru pret Rumāniju*[111] ECT konstatēja ECK 8. panta prasību pārkāpumu, jo Rumānijas tiesību akti atļāva vākt, reģistrēt un arhivēt slepenās datnēs informāciju, kas skar valsts drošību, nenosakot minēto pilnvaru īstenošanas robežas, kas palika iestāžu ziņā. Piemēram, valsts tiesību aktos nebija definēts apstrādājamas informācijas veids, cilvēku kategorijas, attiecībā uz kuriem 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 atbilstīgi ECK 8. pantam un ka ir bijis minētā panta prasību pārkāpums.

Piemērs: Lietā *Taylor-Sabori pret Apvienoto Karalisti*[112] prasītājs bija kļuvis par policijas uzraudzības mērķi. Izmantojot „klonu" uz prasītāja peidžera, policija spēja pārtvert viņam sūtītos ziņojumus. Tad prasītāju apcietināja un izvirzīja pret viņu apsūdzību 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

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

109 ECT 2000. gada 16. februāra spriedums lietā *Amann pret Šveici* [GC], prasības pieteikums Nr. 27798/95, 56. punkts; sk. arī ECT 1985. gada 26. aprīļa spriedumu lietā *Malone pret Apvienoto Karalisti*, prasības pieteikums Nr. 8691/79, 66. punkts; ECT 1983. gada 25. marta spriedumu lietā *Silver un citi pret Apvienoto Karalisti*, prasības pieteikumi Nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 88. punkts.

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

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

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

aktos netika regulēta privātā telekomunikāciju sistēmā pārraidītu komunikāciju pārtveršana. Viņa tiesību aizskārums tātad nebija noticis „saskaņā ar tiesību aktiem". ECT secināja, ka ir bijis ECK 8. panta prasību pārkāpums.

Tiekšanās pēc likumīga mērķa sasniegšanas

Likumīgs mērķis var būt vai nu kāda no nosauktajām vispārējām interesēm vai citu tiesības un brīvības.

Piemērs: Lietā *Peck pret Apvienoto Karalisti*[113] prasītājs uz ielas centās izdarīt pašnāvību, pārgriežot sev vēnas, nezinādams, ka šā mēģinājuma laikā viņu bija nofilmējusi videonovērošanas (*CCTV*) kamera. Pēc tam, kad policija, kura vēroja *CCTV* kameras, viņu izglāba, policijas iestāde tālāk nodeva *CCTV* kameras ierakstu 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. Tiesa secināja, ka ir bijis ECK 8. panta prasību pārkāpums.

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".[114]

Piemērs: Lietā *Khelili pret Šveici*[115] policijas pārbaudes laikā policija atklāja, ka prasītājai bija līdzi zvanāmās kartes ar uzrakstu: „Pievilcīga sieviete, 30+, 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

113 ECT 2003. gada 28. janvāra spriedums lietā *Peck pret Apvienoto Karalisti*, prasības pieteikums Nr. 44647/98, jo īpaši 85. punkts.

114 ECT 1985. gada 11. jūlija spriedums lietā *Leander pret Zviedriju*, prasības pieteikums Nr. 9248/81, 58. punkts.

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

gadījumā apgalvojums par nelikumīgu prostitūciju šķita pārāk netiešs un vispārīgs, to nepamatoja konkrēti fakti, jo prasītāja nekad nebija tikusi notiesāta par nodarbošanos ar nelikumīgu prostitūciju, un tāpēc nevarēja uzskatīt, ka tā atbilst „akūtai sociālai vajadzībai" ECK 8. panta izpratnē. Uzskatot to par iestāžu uzdevumu pierādīt par prasītāju uzglabāto datu precizitāti, un skatot prasītājas tiesību aizskāruma nopietnību, Tiesa izsprieda, ka vārda „prostitūta" gadiem ilgā saglabāšana policijas kartotēkās nav bijusi vajadzīga demokrātiskā sabiedrībā. Tiesa secināja, ka ir bijis ECK 8. panta prasību pārkāpums.

Piemērs: Lietā *Leander pret Zviedriju*[116] ECT izsprieda, ka personu, kuras piesakās darbam svarīgos amatos valsts drošības sistēmā, slepena sīka 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 ECK 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 secināja, ka nav bijis ECK 8. panta prasību pārkāpuma.

3.1.2. Likumīgu ierobežojumu nosacījumi saskaņā ar ES Hartu

Hartas struktūra un formulējums ir atšķirīgi no ECK struktūras un formulējuma. Harta nerunā par garantēto tiesību aizskārumiem, bet satur noteikumu par ierobežojumu(-iem) Hartā atzīto tiesību un brīvību īstenošanā.

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

- ir paredzēti tiesību aktos; un
- respektē tiesību uz datu aizsardzību būtību; un
- ir vajadzīgi, ievērojot samērīguma principu; un

116 ECT 1985. gada 11. jūlija spriedums lietā *Leander pret Zviedriju*, prasības pieteikums Nr. 9248/81, 59. un 67. punkts.

- atbilst Savienībā atzītiem vispārējo interešu kritērijiem vai vajadzībai aizsargāt citu tiesības un brīvības.

Piemēri: Lietā *Volker un Markus Schecke GbR un Hartmut Eifert pret Land Hessen*[117] Tiesa secināja, ka, nosakot [pienākumu] publicēt visu [noteiktu lauksaimniecības fondu atbalsta] saņēmēju – fizisku personu personas datus, nenošķirot tos atbilstoši tādiem pienācīgiem kritērijiem kā laikposmi, kuros viņi ir saņēmuši šādu atbalstu, tā biežums vai arī tā veids un apmērs, Padome un Komisija ir pārkāpušas robežas, kuras nosaka samērīguma principa ievērošana.

Tāpēc Tiesa secināja, ka ir jāpaziņo par spēkā neesošiem daži Padomes Regulas (EK) Nr. 1290/2005 noteikumi un jāpaziņo Regula Nr. 259/2008 par spēkā neesošu kopumā.[118]

Neraugoties uz atšķirīgo formulējumu, Hartas 52. panta 1. punktā paredzētie nosacījumi likumīgai datu apstrādei atgādina ECK 8. panta 2. punkta nosacījumus. Hartas 52. panta 3. punktā uzskaitītie nosacījumi jāaplūko kā tādi, kuri atbilst ECK 8. panta 2. punktā minētajiem nosacījumiem, jo Hartas 52. panta 3. punkta pirmajā teikumā ir noteikts, ka „[c]iktāl 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, ievērojot 52. panta 3. punkta pēdējo teikumu, „[š]is noteikums neliedz Savienības tiesībās paredzēt plašāku aizsardzību". Salīdzinot ar ECK 8. panta 2. punktu un 52. panta 3. punkta pirmo teikumu, tas var nozīmēt tikai to, ka nosacījumi attaisnotiem aizskārumiem atbilstoši ECK 8. panta 2. punktam ir prasību minimums likumīgiem tiesību uz datu aizsardzību ierobežojumiem saskaņā ar Hartu. Līdz ar to likumīga personas datu apstrāde prasa saskaņā ar ES tiesību aktiem, lai būtu izpildīti vismaz ECK 8. panta 2. punkta nosacījumi; ES tiesību aktos tomēr konkrētos gadījumos var noteikt papildu prasības.

117 Tiesas 2010. gada 9. novembra spriedums apvienotajās lietās C-92/09 un C-93/09 *Volker un Markus Schecke GbR un Hartmut Eifert pret Land Hessen*, 89. un 86. punkts.

118 Padomes 2005. gada 21. jūnija Regula (EK) Nr. 1290/2005 par kopējās lauksaimniecības politikas finansēšanu, OV 2005 L 209; Komisijas 2008. gada 18. 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.

Saskaņā ar ES tiesību aktiem likumīgas datu apstrādes principa atbilstību attiecīgajiem ECK noteikumiem turpmāk veicina LES 6. panta 3. punkts, kurā ir noteikts, ka „[p]amattiesības, kas garantētas Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijā [...], ir Savienības tiesību vispārīgo principu pamats".

3.2. Datu apstrādes mērķa noteikšanas un apstrādes ierobežošanas princips

Galvenie punkti

- Datu apstrādes nolūkam jābūt redzami definētam pirms apstrādes sākuma.
- Saskaņā ar ES tiesību aktiem apstrādes nolūkam ir jābūt skaidri definētam; saskaņā ar EP tiesību aktiem šis jautājums ir atstāts valsts tiesību aktu ziņā.
- Apstrāde nedefinētiem nolūkiem neatbilst datu aizsardzības tiesību aktiem.
- Lai turpmāk izmantotu datus citam nolūkam, ir vajadzīgs papildu tiesiskais pamats, ja jaunais apstrādes nolūks nav saderīgs ar sākotnējo nolūku.
- Datu nodošana trešām personām ir jauns nolūks, kam vajag papildu tiesisko pamatu.

Būtībā, datu apstrādes mērķa noteikšanas un apstrādes ierobežošanas princips nozīmē, ka personas datu apstrādes likumība būs atkarīga no apstrādes mērķa [nolūka].[119] Nolūkam jābūt noteiktam, un pārzinim skaidri jādara tas zināms pirms datu apstrādes sākuma.[120] **Saskaņā ar ES tiesību aktiem** tas jādara vai nu ar deklarāciju, citiem vārdiem, paziņojumu, attiecīgajai uzraudzības iestādei vai vismaz ar iekšēju dokumentāciju, kas pārzinim jādara pieejama uzraudzības iestāžu pārbaudei un datu subjekta piekļuvei.

Personas datu apstrāde nenoteiktiem un/vai neierobežotiem nolūkiem ir nelikumīga.

Katram jaunam datu apstrādes nolūkam jābūt savam konkrētam tiesiskajam pamatam, un tā nevar balstīties uz faktu, ka dati sākotnēji tika iegūti vai apstrādāti citam likumīgam nolūkam. Savukārt likumīga apstrāde ir ierobežota līdz tās sākotnēji

119 108. konvencija, 5. panta b) punkts; Datu aizsardzības direktīva, 6. panta 1. punkta b) apakšpunkts.

120 Sk. arī 29. panta darba grupas (2013) *Atzinumu 03/2013 par nolūka ierobežošanu*, WP 203, Briselē, 2013. gada 2. aprīlī.

noteiktajam nolūkam, un jebkuram jaunam apstrādes nolūkam vajadzēs atsevišķu jaunu tiesisko pamatu. Datu atklāšana trešām personām būs jāapsver īpaši rūpīgi, jo atklāšana parasti veido jaunu nolūku un tāpēc prasa tiesisko pamatu, kas atšķiras no datu vākšanas tiesiskā pamata.

Piemērs: Aviokompānija savāc datus no saviem pasažieriem rezervācijas veikšanai, lai pienācīgi pārvaldītu reisu. Aviokompānijai vajadzēs datus par: pasažieru sēdvietu numuriem, īpašiem fiziskiem ierobežojumiem, piemēram, vajadzību pēc ratiņkrēsla, un īpašām pārtikas prasībām, kā *kosher* vai *halal* ēdiens. Ja aviokompānijām prasa nodot pasažieru datu reģistrā iekļautus datus ielidošanas lidostas imigrācijas iestādēm, šos datus pēc tam izmanto imigrācijas kontroles nolūkiem, kas atšķiras no sākotnējā datu vākšanas nolūka. Tāpēc šo datu nodošanai imigrācijas iestādei vajadzēs jauns un atsevišķs tiesiskais pamats.

Apsverot konkrēta nolūka tvērumu un robežas, 108. konvencija un datu aizsardzības direktīva izmanto savienojamības [saderības] jēdzienu: datu izmantošana saderīgiem nolūkiem ir atļauta uz sākotnējā tiesiskā pamata bāzes. Tomēr nav noteikts, ko nozīmē „saderīgs", un šis jēdziens paliek atvērts interpretācijai katrā konkrētā gadījumā.

Piemērs: *Sunshine* uzņēmuma klientu datu, ko tas ieguvis klientu attiecību pārvaldības (*CRM*) laikā, pārdošana tiešās tirgvedības uzņēmumam, *Moonlight* uzņēmumam, kurš vēlas izmantot šos datus, lai atbalstītu trešo uzņēmumu tirgvedības kampaņas, ir jauns nolūks, kas nav saderīgs ar *CRM – Sunshine* uzņēmuma klientu datu vākšanas sākotnējo nolūku. Tāpēc datu pārdošanai *Moonlight* uzņēmumam vajadzēs savu tiesisko pamatu.

Savukārt tas, ka *Sunshine* uzņēmums izmanto *CRM* datus saviem tirgvedības nolūkiem, proti, nosūta saviem klientiem tirgvedības sūtījumus par saviem izstrādājumiem, parasti tiek pieņemts kā saderīgs nolūks.

Datu aizsardzības direktīvā ir skaidri paziņots, ka „turpmākā [personu] datu apstrāde vēsturiskiem, statistiskiem vai zinātniskiem nolūkiem [vispārēji] netiek uzskatīta par nesavienojamu [ar nolūkiem, kādiem dati iepriekš tikuši vākti], ar noteikumu, ka dalībvalstis sniedz piemērotas garantijas".[121]

121 Tādu valsts noteikumu piemērs ir Austrijas Datu aizsardzības akts (*Datenschutzgesetz*), *Fed. Law Gazette I* Nr. 165/1999, 46. punkts, pieejams angļu valodā tīmekļa vietnē: www.dsk.gv.at/DocView.axd?CobId=41936.

Piemēri: *Sunshine* uzņēmums ir savācis un uzglabājis *CRM* datus par saviem klientiem. *Sunshine* uzņēmums drīkst turpmāk izmantot šos datus, lai veiktu savu klientu pirkšanas paradumu statistisko analīzi, jo statistika ir saderīgs nolūks. Nav vajadzīgs papildu tiesiskais pamats, piemēram, datu subjektu piekrišana.

Ja tos pašus datus gribētu tālāk nodot trešai personai, *Starlight* uzņēmumam, tikai statistikas nolūkiem, tālāknodošana būtu pieļaujama bez papildu tiesiskā pamata, bet tikai ar nosacījumu, ka ir ieviestas atbilstošas garantijas, piemēram, datu subjektu identitātes maskēšana, jo statistikas nolūkiem identitātes parasti nav vajadzīgas.

3.3. Datu kvalitātes principi

Galvenie punkti

- Datu kvalitātes principi pārzinim jāīsteno visās apstrādes darbībās.
- Datu ierobežotas saglabāšanas princips prasa dzēst datus, tiklīdz tie vairs nav vajadzīgi nolūkiem, kuriem tos savāca.
- Izņēmumiem no ierobežotas saglabāšanas principa jābūt noteiktiem tiesību aktos, un tiem vajag īpašas garantijas datu subjektu aizsardzībai.

3.3.1. Datu būtiskuma princips

Var apstrādāt tikai tādus datus, kas ir „adekvāti, attiecīgi un ne pārmērīgā apjomā attiecībā uz nolūkiem, kādiem tie ievākti un/vai tālāk apstrādāti”.[122] Apstrādei izvēlēto datu kategorijām jābūt nepieciešamām, lai sasniegtu apstrādes darbību paziņoto vispārējo mērķi, un pārzinim ir stingri jāierobežo datu vākšana līdz tādai informācijai, kas ir tieši būtiska konkrētajam apstrādes nolūkam.

Mūsdienu sabiedrībā datu būtiskuma principam ir vēl viens arguments: izmantojot īpašas privātumu veicinošas tehnoloģijas, dažreiz ir iespējams vispār novērst personas datu izmantošanu vai izmantot pseidonimizētus datus, kā rezultātā iegūst privātumam draudzīgu risinājumu. Tas ir īpaši piemēroti plašākās apstrādes sistēmās.

122 108. konvencija, 5. panta c) punkts; un Datu aizsardzības direktīva, 6. panta 1. punkta c) apakšpunkts.

Piemērs: Pilsētas dome par zināmu samaksu piedāvā regulārajiem pilsētas sabiedriskā transporta lietotājiem karti ar mikroshēmu. Uz kartes ir norādīts lietotāja vārds/uzvārds – gan rakstiski uz kartes virsmas, gan elektroniskā formā mikroshēmā. Ikreiz, kad cilvēks iekāpj autobusā vai tramvajā, karte ar mikroshēmu ir jāpietuvina lasītājiekārtām, kuras ir uzstādītas, piemēram, autobusos un tramvajos. Ierīces nolasītos datus elektroniski pārbauda datu bāzē, kurā ir iekļauti cilvēku, kuri ir nopirkuši braukšanas karti, vārdi/uzvārdi.

Šī sistēma nav optimāli pielāgota būtiskuma principam: pārbaudīt, vai personai ir tiesības izmantot transporta līdzekļus, var arī nesalīdzinot personas datus kartes mikroshēmā ar datu bāzi. Būtu pietiekami, piemēram, ierīkot kartes mikroshēmā īpašu elektronisku attēlu, piemēram, svītrkodu, kas, pietuvināts lasītājierīcei, apstiprinātu, vai karte ir derīga vai nē. Tāda sistēma nereģistrētu datus par to, kurš, kurā laikā un kādu transporta līdzekli ir izmantojis. Netiktu ievākti personas dati, kas ir optimālais risinājums būtiskuma principa ziņā, jo šis princips paredz pienākumu pēc iespējas mazināt datu vākšanu.

3.3.2. Datu precizitātes princips

Pārzinis, kuram ir informācija par personām, neizmanto šo informāciju, pirms nav veicis vajadzīgos pasākumus, lai ar saprātīgu noteiktību nodrošinātu, ka dati ir precīzi un atjaunināti.

Pienākums nodrošināt datu precizitāti ir jāaplūko saistībā ar datu apstrādes nolūku.

Piemērs: Mēbeļu tirdzniecības uzņēmums savāca klientu identitātes un adrešu datus, lai nosūtītu viņam vai viņai rēķinu. Sešus mēnešus vēlāk tas pats uzņēmums vēlas sākt mārketinga kampaņu un vēlas sazināties ar bijušajiem klientiem. Lai sasniegtu klientus, uzņēmums vēlas piekļūt valsts pastāvīgo iedzīvotāju reģistram, kur visdrīzāk būs atjaunināti adrešu dati, jo pastāvīgajiem iedzīvotājiem ir pienākums informēt reģistru par savu pašreizējo dzīvesvietu. Piekļuve datiem šajā reģistrā ir ierobežota – piekļūt var tikai personas un vienības, kuras var sniegt pamatojošu iemeslu.

Šajā situācijā uzņēmums nevar izmantot argumentu, ka dati ir jāuztur precīzi un atjaunināti, lai apgalvotu, ka tam ir tiesības vākt no pastāvīgo iedzīvotāju reģistra jaunus adrešu datus par visiem saviem bijušajiem klientiem. Dati tika vākti rēķinu izrakstīšanas laikā; šim nolūkam būtiska ir adrese pārdošanas darījuma

laikā. Nav tiesiska pamata jaunu adrešu datu vākšanai, jo tirgvedība nav interese, kura būtu svarīgāka par tiesībām uz datu aizsardzību, un tāpēc nevar attaisnot piekļuvi reģistra datiem.

Var būt arī tādi gadījumi, kad uzglabāto datu atjaunināšana ir aizliegta tiesību aktos, jo datu uzglabāšanas nolūks galvenokārt ir dokumentēt notikumus.

Piemērs: Medicīnas operācijas protokolu nedrīkst grozīt, citiem vārdiem, „atjaunināt", pat ja vēlāk izrādās, ka protokolā ietvertie konstatējumi ir nepareizi. Šādos apstākļos drīkst izdarīt tikai papildinājumus protokola piezīmēm, ciktāl tos skaidri atzīmē kā ierakstus, kas izdarīti vēlākā posmā.

No otras puses, ir situācijas, kurās regulāra datu precizitātes pārbaude, tostarp atjaunināšana, ir absolūti nepieciešama iespējamā kaitējuma dēļ, kas var rasties datu subjektam, ja dati paliktu neprecīzi.

Piemērs: Ja kāds vēlas noslēgt līgumu ar banku iestādi, banka parasti pārbaudīs sava potenciālā klienta kredītspēju. Šajā nolūkā pastāv īpašas datu bāzes, kurās ir dati par privātu personu kredītvēsturi. Ja tāda datu bāze sniedz nepareizus vai novecojušus datus par kādu personu, šī persona var saskarties ar nopietnām problēmām. Tāpēc šādu datu bāžu pārziņiem ir jāpieliek īpaši pūliņi, lai ievērotu precizitātes principu.

Tālāk, datus, kuri attiecas nevis uz faktiem, bet uz aizdomām, piemēram, kriminālizmeklēšanas, drīkst vākt un uzglabāt tik ilgi, kamēr pārzinim ir tiesisks pamats tādas informācijas vākšanai un pietiekams attaisnojums tam, ka viņam ir radušās šādas aizdomas.

3.3.3. Ierobežotas datu saglabāšanas princips

Datu aizsardzības direktīvas 6. panta 1. punkta e) apakšpunktā un, līdzīgi, 108. konvencijas 5. panta e) punktā ir prasīts, lai dalībvalstis nodrošina, ka personas datiem jābūt „saglabātiem veidā, kas pieļauj datu subjektu identifikāciju ne ilgāk, kā tas nepieciešams nolūkiem, kuriem datus vāca vai kuriem tos turpmāk apstrādā". Tāpēc dati ir jādzēš pēc tam, kad šie nolūki ir izpildīti.

Lietā *S.* un *Marper* ECT secināja, ka attiecīgo Eiropas Padomes instrumentu pamatprincipi un pārējo Līgumslēdzēju Pušu tiesību akti un prakse prasīja, lai datu

uzglabāšana būtu samērīga attiecībā pret vākšanas mērķi un ierobežota laikā, jo īpaši policijas jomā.[123]

Personas datu glabāšanas laika ierobežojums tomēr attiecas tikai uz datiem, kurus tur tādā formā, kas dod iespēju identificēt datu subjektu. Tāpēc vairs nevajadzīgus datus var likumīgi uzglabāt, tos anonimizējot vai pseidonimizējot.

Uz datu glabāšanu turpmākiem zinātniskiem, vēsturiskiem vai statistiskiem nolūkiem datu aizsardzības direktīvā paredzētais ierobežotas datu uzglabāšanas princips neattiecas.[124] Šai ilgstošai personas datu glabāšanai un izmantošanai tomēr jāparedz īpašas garantijas valsts tiesību aktos.

3.4. Godprātīgas apstrādes princips

Galvenie punkti

- Godprātīga apstrāde nozīmē apstrādes caurskatāmību, jo īpaši *vis-à-vis* datu subjektiem.
- Pārziņiem ir jāinformē datu subjekti pirms viņu datu apstrādes, vismaz par apstrādes nolūku un par pārziņa identitāti un adresi.
- Ja vien tas nav konkrēti atļauts tiesību aktos, nedrīkst notikt slepena un slēpta personas datu apstrāde.
- Datu subjektiem ir tiesības uz piekļuvi saviem datiem ikvienā vietā, kur tos apstrādā.

Godprātīgas apstrādes princips regulē galvenokārt attiecības starp pārzini un datu subjektu.

3.4.1. Caurskatāmība

Šis princips nosaka pārzinim pienākumu turēt datu subjektus informētus par to, kā izmanto viņu datus.

123 ECT 2008. gada 4. decembra spriedums lietā *S. un Marper pret Apvienoto Karalisti*, prasības pieteikumi Nr. 30562/04 un Nr. 30566/04; sk. arī, piemēram, ECT 2012. gada 13. novembra spriedums lietā *M.M. pret Apvienoto Karalisti*, prasības pieteikums Nr. 24029/07.

124 Datu aizsardzības direktīva, 6. panta 1. punkta e) apakšpunkts.

Piemērs: Lietā *Haralambie pret Rumāniju*[125] prasītājs prasīja piekļuvi kartotēkai, kuru par viņu bija sagatavojusi slepenā dienesta organizācija, bet viņa prasību apmierināja tikai piecus gadus vēlāk. ECT uzsvēra, ka personām, par kurām valsts varas iestādes ir turējušas personas kartotēku, ir būtiski svarīgi spēt piekļūt tai. Iestādēm ir pienākums nodrošināt efektīvu procedūru, lai saņemtu piekļuvi tādai informācijai. ECT uzskatīja, ka ne nodoto kartotēku skaits, ne trūkumi arhīva sistēmā neattaisno piecu gadu kavēšanos, lai piešķirtu prasītājam atļauju piekļūt savai kartotēkai. Iestādes nebija nodrošinājušas prasītājam efektīvu un pieejamu procedūru, lai dotu viņam iespēju saprātīgā laikā piekļūt kartotēkai ar saviem datiem. Tiesa secināja, ka ir bijis ECK 8. panta prasību pārkāpums.

Apstrādes darbības ir jāpaskaidro datu subjektiem viegli saprotamā veidā, kas nodrošina, ka viņi/viņas saprot, kas ar viņu datiem notiks. Datu subjektam ir arī tiesības pēc pieprasījuma saņemt informāciju no pārziņa par to, vai viņa/viņas datus apstrādā, un, ja jā, tad kurus.

3.4.2. Uzticības veidošana

Pārziņiem ir dokumentāri jāapstiprina – gan datu subjektiem, gan plašai sabiedrībai –, ka viņi apstrādās datus likumīgi un caurskatāmi. Apstrādes darbības nedrīkst veikt slepeni, un tām nedrīkst būt neparedzamu negatīvu seku. Pārziņiem jānodrošina, ka patērētāji, klienti vai pilsoņi ir informēti par to, kā viņu datus izmanto. Vēl pārziņiem, cik vien tas iespējams, ir jārīkojas veidā, kas tūlīt atbilst datu subjekta vēlmēm, jo īpaši, ja viņa vai viņas piekrišana ir datu apstrādes tiesiskais pamats.

Piemērs: Lietā *K.H. un citi pret Slovākiju*[126] prasītājas bija astoņas romu etniskās izcelsmes sievietes, kuras bija bijušas divu Austrumslovākijas slimnīcu pacientes grūtniecības un dzemdību laikā. Pēc tam neviena no viņām vairs nespēja ieņemt bērnu, lai gan bija notikuši atkārtoti mēģinājumi. Valsts tiesas lika slimnīcām atļaut prasītājām un viņu pārstāvjiem iepazīties ar medicīnas kartēm un ar roku izrakstīt informāciju, bet noraidīja prasību sagatavot dokumentu fotokopijas, it kā tāpēc, lai novērstu to ļaunprātīgu izmantošanu. Valstu pozitīvie pienākumi saskaņā ar ECK 8. pantu katrā ziņā ietvēra pienākumu darīt datu subjektam pieejamas viņa vai viņas datu kartotēkas kopijas. Valsts ziņā bija noteikt

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

126 ECT 2009. gada 6. novembra spriedums lietā *K.H. un citi pret Slovākiju*, prasības pieteikums Nr. 32881/04.

kārtību, kādā kopēt personas datu kartotēku, vai, attiecīgā gadījumā, norādīt pārliecinošus iemeslus prasības noraidīšanai. Prasītāju gadījumā valsts tiesas pamatoja aizliegumu kopēt medicīnas kartes galvenokārt ar vajadzību nepieļaut būtiskas informācijas ļaunprātīgu izmantošanu. Tomēr ECT nesaskatīja, kā prasītājas, kurām pat bija atļauts piekļūt visām savām medicīnas kartotēkām, būtu varējušas ļaunprātīgi izmantot informāciju par viņām pašām. Turklāt tādas ļaunprātīgas izmantošanas risku varēja novērst ar citiem līdzekļiem, nevis liedzot prasītājām kartotēku kopijas – to varēja panākt, piemēram, ierobežojot to personu loku, kurām ir tiesības piekļūt kartotēkām. Valsts nepierādīja pietiekami pārliecinošu iemeslu pastāvēšanu, lai liegtu prasītājām efektīvi piekļūt informācijai par savu veselību. Tiesa secināja, ka ir bijis 8. panta prasību pārkāpums.

Attiecībā uz interneta pakalpojumiem datu apstrādes sistēmas īpašībām jābūt tādām, lai datu subjektiem būtu iespējams reāli saprast, kas notiek ar viņu datiem.

Godprātīga apstrāde nozīmē arī to, ka pārziņi ir gatavi pakalpojumā datu subjektam pārsniegt prasību obligāto juridisko minimumu, ja to prasa datu subjekta likumīgās intereses.

3.5. Atbildības princips

Galvenie punkti

- Atbildības princips prasa, lai pārziņi aktīvi īstenotu pasākumus, lai savās [datu] apstrādes darbībās veicinātu un garantētu datu aizsardzību.
- Pārziņi atbild par savu apstrādes darbību atbilstību datu aizsardzības tiesību aktiem.
- Pārziņiem jāspēj katrā laikā pierādīt datu aizsardzības noteikumu atbilstību datu subjektiem, plašai sabiedrībai un uzraudzības iestādēm.

Ekonomiskā sadarbības un attīstības organizācija (ESAO) 2013. gadā pieņēma pamatnostādnes par privātumu, kurās uzsvēra, ka pārziņiem ir liela nozīme, lai datu aizsardzība darbotos praksē. Pamatnostādnes izstrādā atbildības principu, lai „datu pārzinis būtu atbildīgs par atbilstību pasākumiem, kuri īsteno iepriekš minētos [materiālos] principus”.[127]

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

Kamēr 108. konvencijā nav norādes uz pārziņa atbildības principu, pamatā atstājot to valsts tiesību aktu ziņā, datu aizsardzības direktīvas 6. panta 2. punktā ir noteikts, ka pārzinim jānodrošina atbilstība 1. punktā minētajiem datu kvalitātes principiem.

Piemērs: Leģislatīvs piemērs atbildības principa uzsvēršanai ir 2009. gada grozījums[128] e-privātuma direktīvā 2002/58/EK. Atbilstoši 4. pantam tā grozītajā redakcijā direktīva nosaka pienākumu īstenot drošības politiku, proti, „nodrošina, ka tiek īstenota drošības politika saistībā ar personas datu apstrādi". Tādējādi, ciktāl runa ir par minētās direktīvas drošības noteikumiem, likumdevējs nolēma, ka ir nepieciešams ieviest skaidru prasību par vajadzīgo drošības politiku, kā arī īstenot to.

Atbilstoši 29. panta darba grupas atzinumam[129] atbildības principa būtība ir pārziņa pienākums:

- īstenot pasākumus, kuri parastajos apstākļos garantētu, ka datu aizsardzības normas ir ievērotas saistībā ar apstrādes darbībām; un

- turēt gatavībā dokumentus, kuri pierāda datu subjektiem un uzraudzības iestādēm, kādi pasākumi ir veikti, lai panāktu atbilstību datu aizsardzības normām.

Tādējādi atbildības princips prasa, lai pārziņi aktīvi pierādītu atbilstību, nevis tikai gaidītu, līdz datu subjekti vai uzraudzības iestādes norādīs uz trūkumiem.

128 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.

129 29. panta darba grupas *Atzinums 3/2010 par atbildības principu*, WP 173, Briselē, 2010. gada 13. jūlijā.

4

Eiropas tiesību aktu normas datu aizsardzības jomā

ES	Aplūkotie jautājumi	EP
Normas likumīgai nesensitīvu datu apstrādei		
Datu aizsardzības direktīva, 7. panta a) punkts	Piekrišana	Ieteikums par profilēšanu, 3.4. punkta b) apakšpunkts un 3.6. punkts
Datu aizsardzības direktīva, 7. panta b) punkts	(Pirms)līgumiskās attiecības	Ieteikums par profilēšanu, 3.4. punkta b) apakšpunkts
Datu aizsardzības direktīva, 7. panta c) punkts	Pārziņa juridiskas saistības	Ieteikums par profilēšanu, 3.4. punkta a) apakšpunkts
Datu aizsardzības direktīva, 7. panta d) punkts	Datu subjekta būtiskas intereses	Ieteikums par profilēšanu, 3.4. punkta b) apakšpunkts
Datu aizsardzības direktīva, 7. panta e) punkts un 8. panta 4. punkts Tiesas 2008. gada 16. decembra spriedums lietā C-524/06 *Huber pret Vācijas Federatīvo Republiku*	Sabiedrības intereses un oficiālu pilnvaru realizācija	Ieteikums par profilēšanu, 3.4. punkta b) apakšpunkts
Datu aizsardzības direktīva, 7 (f). pants, 8. panta 2. un 3. punkts Tiesas 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*	Citu likumīgas intereses	Ieteikums par profilēšanu, 3.4. punkta b) apakšpunkts
Normas likumīgai sensitīvu datu apstrādei		
Datu aizsardzības direktīva, 8. panta 1. punkts	Vispārīgs apstrādes aizliegums	108. konvencija, 6. pants

ES	Aplūkotie jautājumi	EP
Datu aizsardzības direktīva, 8. panta 2.–4. punkts	Izņēmumi no vispārīgā aizlieguma	108. konvencija, 6. pants
Datu aizsardzības direktīva, 8. panta 5. punkts	Datu par (kriminālo) notiesāšanām apstrāde	108. konvencija, 6. pants
Datu aizsardzības direktīva, 8. panta 7. punkts	Identifikācijas numuru apstrāde	
Drošas apstrādes normas		
Datu aizsardzības direktīva, 17. pants	Pienākums nodrošināt drošu apstrādi	108. konvencija, 7. pants
		ECT 2008. gada 17. jūlija spriedums lietā *I. pret Somiju*, prasības pieteikums Nr. 20511/03
E-privātuma direktīva, 4. panta 2. punkts	Paziņojums par datu aizsardzības pārkāpumiem	
Datu aizsardzības direktīva, 16. pants	Konfidencialitātes pienākums	
Apstrādes caurskatāmības normas		
	Caurskatāmība vispār	108. konvencija, 8. panta a) punkts
Datu aizsardzības direktīva, 10. un 11. pants	Informācija	108. konvencija, 8. panta a) punkts
Datu aizsardzības direktīva, 10. un 11. pants	Izņēmumi no informēšanas pienākuma	108. konvencija, 9. pants
Datu aizsardzības direktīva, 18. un 19. pants	Paziņošana	Ieteikums par profilēšanu, 9.2. punkta a) apakšpunkts
Atbilstības veicināšanas normas		
Datu aizsardzības direktīva, 20. pants	Iepriekšēja pārbaude	
Datu aizsardzības direktīva, 18. panta 2. punkts	Personas datu aizsardzības speciālisti	Ieteikums par profilēšanu, 8.3. punkts
Datu aizsardzības direktīva, 27. pants	Rīcības kodeksi	

Principi katrā ziņā ir vispārīgas dabas. Piemērojot tos konkrētām situācijām, paliek zināma rīcības brīvība to interpretācijā un līdzekļu izvēlē. Saskaņā ar EP tiesību aktiem 108. konvencijas līgumslēdzēju pušu ziņā ir izskaidrot šo interpretācijas iespēju savos valsts tiesību aktos. Situācija **ES tiesību aktos** ir atšķirīga: lai izveidotu

datu aizsardzību iekšējā tirgū, tika uzskatīts par nepieciešamu jau ES mērogā pieņemt sīkāk izstrādātus noteikumus, lai saskaņotu dalībvalstu tiesību aktos paredzēto datu aizsardzības līmeni. Datu aizsardzības direktīvā atbilstoši tās 6. pantā izklāstītajiem principiem ir noteikts sīki izstrādātu normu slānis, kas uzticami jāīsteno valstu tiesību aktos. Tāpēc nākamās piezīmes par sīki izstrādātām datu aizsardzības normām Eiropas mērogā attiecas galvenokārt uz ES tiesībām.

4.1. Normas par likumīgu datu apstrādi

Galvenie punkti

- Personas datus drīkst likumīgi apstrādāt, ja:
  - apstrādes pamatā ir datu subjekta piekrišana; vai
  - datu subjektu būtiskas intereses prasa viņu datu apstrādi; vai
  - apstrādes iemesls ir citu likumīgas intereses, bet tikai tiktāl, ciktāl tās netiek atceltas ar interesēm saistībā ar datu subjektu pamattiesību aizsardzību.
- Likumīga sensitīvu personas datu apstrāde ir pakļauta īpašam, stingrākam režīmam.

Datu aizsardzības direktīvā ir ietverti divi dažādi likumīgas datu apstrādes normu kopumi: viens 7. pantā – attiecībā uz nesensitīviem datiem, un otrs 8. pantā – attiecībā uz sensitīviem datiem.

4.1.1. Likumīga nesensitīvu datu apstrāde

Direktīvas 95/46 II nodaļā ar virsrakstu „Vispārīgie noteikumi personas datu apstrādes atzīšanai par likumīgu" ir paredzēts, ka, ievērojot 13. pantā paredzētos izņēmumus, visai personas datu apstrādei jāatbilst, pirmkārt, datu aizsardzības 6. pantā izklāstītajiem datu kvalitātes principiem un, otrkārt, kādam no 7. pantā uzskaitītajiem kritērijiem, lai datu apstrādi atzītu par likumīgu.[130] Tas paskaidro gadījumus, kuros nesensitīvu personas datu apstrāde tiek atzīta par likumīgu.

130 Tiesas 2003. gada 20. maija spriedums apvienotajās lietās C-465/00, C-138/01 un C-139/01 *Österreichischer Rundfunk un citi*, 65. punkts; Tiesas 2008. gada 16. decembra spriedums lietā C-524/06 *Huber pret Vāciju*, 48. punkts. Tiesas 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.

Piekrišana

Saskaņā ar EP tiesību aktiem piekrišana nav pieminēta ECK 8. pantā vai 108. konvencijā. Tā tomēr ir minēta ECT judikatūrā un vairākos EP Ieteikumos. **Saskaņā ar ES tiesību aktiem** piekrišana kā pamats likumīgai datu apstrādei ir stingri noteikta datu aizsardzības direktīvas 7. panta a) punktā, kā arī ir skaidri pieminēta Hartas 8. pantā.

Līgumiskas attiecības

Cits pamats personas datu likumīgai apstrādei **saskaņā ar ES tiesību aktiem**, kas uzskaitīts datu aizsardzības direktīvas 7. panta b) punktā, ir tad, ja tā ir „vajadzīga līguma, kurā datu subjekts ir līgumslēdzēja puse, izpildei". Šis noteikums attiecas arī uz pirmslīguma attiecībām. Piemēram, viena puse plāno noslēgt līgumu, bet vēl nav to izdarījusi – iespējams, tāpēc, ka vēl ir jāpabeidz dažas pārbaudes. Ja vienai pusei ir jāapstrādā dati šim nolūkam, tāda apstrāde ir likumīga, kamēr vien tā ir „pasākumu veikšanai pēc datu subjekta pieprasījuma pirms līguma noslēgšanas".

Kas attiecas uz EP tiesību aktiem, ECK 8. panta 2. punktā „lai aizstāvētu citu tiesības un brīvības" ir minēts kā tiesību uz datu aizsardzību likumīga aizskāruma iemesls.

Pārziņa juridiskās saistības

ES tiesību aktos tad ir konkrēti minēti citi kritēriji, kuri padara datu apstrādi par likumīgu, proti, ja tā ir „vajadzīga, lai izpildītu uz personas datu apstrādātāju [pārzini] attiecināmas juridiskas saistības" (datu aizsardzības direktīvas 7. panta c) punkts). Šis noteikums attiecas uz pārziņiem, kuri darbojas privātajā sektorā, uz publiskā sektora datu pārziņu juridiskajām saistībām attiecas direktīvas 7. panta e) punkts. Ir daudzi gadījumi, kuros privātā sektora pārziņiem ir tiesību aktos noteikts pienākums apstrādāt datus par citiem; piemēram, ārstiem un slimnīcām ir juridisks pienākums vairākus gadus uzglabāt datus par pacientu ārstēšanu, darba devējiem ir jāapstrādā dati par saviem darbiniekiem sociālās nodrošināšanas un aplikšanas ar nodokļiem nolūkos, un uzņēmumiem jāapstrādā dati par saviem klientiem aplikšanas ar nodokļiem nolūkos.

Saistībā ar to, ka aviosabiedrībām ir obligāti jānodod pasažieru dati ārvalstu imigrācijas kontroles iestādēm, radās jautājums par to, vai juridiskās saistības atbilstīgi *ārvalstu* tiesību aktiem var veidot likumīgu pamatu, lai apstrādātu datus saskaņā ar ES tiesību aktiem (šis jautājums ir sīkāk aplūkots 2.3.2 iedaļā).

Pārziņa juridiskās saistības var būt par pamatu likumīgai datu apstrādei arī **atbilstīgi EP tiesību aktiem**. Kā norādīts iepriekš, privātā sektora pārziņa juridiskās saistības ir tikai viens speciāls citu likumīgo interešu gadījums, kā minēts ECK 8. panta 2. punktā. Tāpēc iepriekš minētais piemērs arī ir svarīgs EP tiesību aktiem.

Datu subjekta būtiskas intereses

Saskaņā ar ES tiesību aktiem, datu aizsardzības direktīvas 7. panta d) punktā ir paredzēts, ka personas datu apstrāde ir likumīga, ja tā ir „vajadzīga, lai aizsargātu datu subjekta būtiskas intereses". Tādas intereses, kas ir cieši saistītas ar datu subjekta izdzīvošanu, var būt par pamatu, piemēram, likumīgai veselības datu vai datu par pazudušām personām izmantošanai.

Saskaņā ar EP tiesību aktiem datu subjekta būtiskas intereses nav minētas ECK 8. pantā kā tiesību uz datu aizsardzību likumīga aizskāruma iemesls. Tomēr dažos EP ieteikumos, kas papildina 108. konvenciju īpašās jomās, datu subjekta būtiskas intereses ir konkrēti minētas kā likumīgas datu apstrādes pamats.[131] Datu subjekta būtiskas intereses acīmredzot uzskata par noklusēti ietvertām to iemeslu kopumā, kuras attaisno datu apstrādi: pamattiesību aizsardzība nekad nedrīkst apdraudēt aizsargātās personas būtiskas intereses.

Sabiedrības intereses un oficiālu pilnvaru realizācija

Ņemot vērā daudzos veidus, kādos var organizēt valsts darbu, datu **aizsardzības direktīvas** 7. panta e) punktā ir paredzēts, ka personas datus var likumīgi apstrādāt, ja „apstrāde vajadzīga sabiedrības interesēs realizējama uzdevuma izpildei vai personas datu apstrādātājam [pārzinim] vai treša[ja]i personai, kurai dati tiek atklāti, piešķirto oficiālo pilnvaru realizācijai [...]".[132]

Piemērs: Lietā *Huber pret Vāciju*[133] Hūbera k–gs, Austrijas pilsonis ar dzīvesvietu Vācijā, lūdza Federālajai migrācijas un bēgļu pārvaldei dzēst Ārvalstnieku centrālajā reģistrā ("*AZR*") par viņu iekļautos datus. Šo reģistru, kurā ir ietverti dati par ES pilsoņiem, kuri nav Vācijas valsts piederīgie un ilgāk nekā trīs mēnešus pastāvīgi dzīvo Vācijā, izmanto statistikas nolūkiem, un vēl to izmanto tiesībaizsardzības iestādes un tiesu iestādes, izmeklējot noziedzīgas darbības vai tādas

131 Ieteikums par profilēšanu, 3.4. punkta b) apakšpunkts.

132 Sk. arī Datu aizsardzības direktīvas preambulas 32. apsvērumu.

133 Tiesas 2008. gada 16. decembra spriedums lietā C-524/06 *Huber pret Vāciju*.

darbības, kas apdraud sabiedrisko drošību, un saucot pie atbildības par tām. Iesniedzējtiesa jautāja, vai personas datu apstrāde tādā reģistrā, kā Ārvalstnieku centrālais reģistrs, kuram piekļuve ir sniegta tikai valsts [varas] iestādēm, ir saderīga ar ES tiesībām, ņemot vērā, ka par Vācijas pilsoņiem tāda reģistra nav.

Tiesa uzskata, pirmkārt, ka saskaņā ar direktīvas 7. panta e) punktu personas datu apstrāde ir likumīga tikai tad, ja tā ir vajadzīga sabiedrības interesēs realizējama uzdevuma izpildei vai piešķirto oficiālo pilnvaru realizācijai.

Pēc Tiesas domām, „ņemot vērā mērķi visās dalībvalstīs nodrošināt vienādu aizsardzības līmeni, vajadzības jēdzienam, kas izriet no Direktīvas 95/46 7. panta e) punkta, [..], nevar būt atšķirīgs saturs atkarībā no dalībvalsts. Tādējādi tas ir autonoms Kopienu tiesību jēdziens, kas ir jāinterpretē tā, lai tas pilnībā atbilstu šīs direktīvas mērķim, kas ir noteikts tās 1. panta 1. punktā".[134]

Tiesa norāda, ka Savienības pilsoņa tiesības pārvietoties tādas dalībvalsts teritorijā, kuras valstspiederīgais viņš vai viņa nav, nav beznosacījuma, un Līgumā, kā arī tā piemērošanai pieņemtajās tiesību normās šīm tiesībām var būt noteikti ierobežojumi un nosacījumi. Tāpēc, ja tāda reģistra kā *AZR* izmantošana, lai palīdzētu iestādēm, kurām uzticēts piemērot uzturēšanās tiesības regulējošu tiesisko regulējumu, principā dalībvalstij ir leģitīma, tādā reģistrā tomēr var iekļaut tikai tādu informāciju, kas ir vajadzīga šim konkrētajam mērķim. Tiesa nospriež, ka šāda personas datu apstrādes sistēma atbilst ES tiesībām, ja tajā ir tikai tādi dati, kas vajadzīgi, lai minētās iestādes varētu piemērot šo regulējumu, un ja tās centralizētais raksturs veicina šī regulējuma efektīvāku piemērošanu. Valsts tiesai ir jānoskaidro, vai šajā konkrētajā gadījumā minētie nosacījumi ir izpildīti. Ja nē, katrā ziņā par vajadzīgu Direktīvas 95/46/EK 7. panta e) punkta izpratnē nevar uzskatīt personas datu glabāšanu un apstrādi tādā reģistrā kā *AZR* statistikas mērķiem.[135]

Visbeidzot, attiecībā uz jautājumu par reģistrā iekļauto datu izmantošanu noziedzības apkarošanas nolūkiem, Tiesa uzskata, ka šis mērķis „obligāti nozīmē, ka ir jāizmeklē izdarītie noziegumi un kriminālpārkāpumi neatkarīgi no to izdarītāju pilsonības". Konkrētajā reģistrā nav ietverti personas dati par attiecīgās dalībvalsts valstspiederīgajiem, un šī atšķirīgā attieksme ir diskriminācija, kas aizliegta ar LESD 18. pantu. Tādējādi šis noteikums, atbilstoši Tiesas interpretācijai,

134 Turpat, 52. punkts.

135 Turpat, 54., 58., 59., 66.68. punkts.

„liedz dalībvalstij, lai cīnītos pret noziedzību, izveidot personas datu apstrādes sistēmu, kas attiecas tikai uz tiem Savienības pilsoņiem, kas nav šīs dalībvalsts valstspiederīgie".[136]

Uz personas datu izmantošanu, ko veic iestādes, kuras darbojas publiskajā telpā, arī attiecas **ECK** 8. pants.

Pārziņa vai trešās personas likumīgo interešu ievērošana

Datu subjekts nav vienīgā persona ar likumīgām interesēm. Datu **aizsardzības direktīvas** 7. panta f) punktā ir paredzēts, ka datu apstrāde ir likumīga, ja tā „vajadzīga personas datu apstrādātāja [pārziņa] vai trešo personu, kurām dati tiek atklāti, likumīgo interešu ievērošanai, izņemot, ja šīs intereses ignorē, ņemot vērā datu subjekta pamattiesību un brīvību intereses, kurām nepieciešama aizsardzība [...]".

Nākamajā spriedumā Tiesa skaidri izsprieda par direktīvas 7. panta f) punktu:

Piemērs: Lietā *ASNEF* un *FECEMD*[137] Tiesa paskaidroja, ka nav atļauts valsts tiesību aktos pievienot nosacījumus papildus tiem, kuri minēti datu apstrādes direktīvas 7. panta f) punktā attiecībā uz likumīgu datu apstrādi. Tas attiecās uz situāciju, kurā Spānijas datu aizsardzības tiesību aktos bija ietverts noteikums, ar kuru citas privātas personas varēja pieprasīt ievērot savas likumīgas intereses personas datu apstrādē tikai tad, ja informācija jau bija parādījusies publiski pieejamos avotos.

Tiesa vispirms norādīja, ka ar Direktīvu 95/46 ir paredzēts visās dalībvalstīs nodrošināt vienādu personu tiesību un brīvību aizsardzību saistībā ar personas datu apstrādi. Attiecīgajā jomā piemērojamo valstu tiesību aktu tuvināšana nedrīkst vājināt to sniegto aizsardzību. Tai jācenšas nodrošināt augstu aizsardzības līmeni Savienībā.[138] Tāpēc Tiesa uzskatīja, ka „no mērķa nodrošināt vienādu aizsardzības līmeni visās dalībvalstīs izriet, ka Direktīvas 95/46 7. pants paredz plašu un pilnīgu tādu situāciju sarakstu, kurās var uzskatīt, ka ir notikusi likumīga personas datu apstrāde". Turklāt „dalībvalstis nedrīkst ne pievienot

136 Turpat, 78. un 81. punkts.

137 Tiesas 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*.

138 Turpat, 28. punkts. Sk. Datu aizsardzības direktīvas preambulas 8. un 10. apsvērumu.

Direktīvas 95/46 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".[139] Tiesa atzina, ka „[a]ttiecībā uz nepieciešamo izvērtējumu atbilstoši Direktīvas 95/46 7. panta f) punktam ir iespējams ņemt vērā, ka minētās datu apstrādes izraisīta attiecīgās personas pamattiesību pārkāpuma smagums var atšķirties atkarībā no tā, vai attiecīgie dati jau ir vai vēl nav ietverti publiski pieejamos avotos".

Tomēr „šīs 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 minētos apsvērumus, Tiesa secināja, ka „Direktīvas 95/46 7. panta f) punkts ir jāinterpretē tādējādi, ka tam ir pretrunā tāds valsts tiesiskais regulējums, ar kuru gadījumā, ja nav attiecīgās personas [datu subjekta] piekrišanas, un lai atļautu šo personas datu apstrādi, kura ir vajadzīga personas datu apstrādātāja [pārziņa] 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".[140]

Līdzīgus formulējumus var atrast **EP ieteikumos**. Ieteikumā par profilēšanu personas datu apstrāde profilēšanas mērķiem ir atzīta par likumīgu, ja tas nepieciešams citu personu likumīgās interesēs, „izņemot, ja šīs intereses ignorē, ņemot vērā datu subjekta pamattiesību un brīvību intereses".[141]

4.1.2. Likumīga sensitīvu datu apstrāde

EP tiesību akti atstāj valsts tiesību aktu ziņā noteikt atbilstošu aizsardzību sensitīvu datu izmantošanai, savukārt **ES tiesību akti** – datu aizsardzības direktīvas 8. pants ietver detalizētu režīmu tādu kategoriju datu apstrādei, kuri atklāj: rasi vai etnisko izcelsmi, politiskos uzskatus, reliģisko vai filozofisko pārliecību, dalību arodbiedrībās,

139 Tiesas 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*, 30. un 32. punkts.

140 Turpat, 40., 44., 48. un 49. punkts.

141 Ieteikums par profilēšanu, 3.4. punkta b) apakšpunkts.

kā arī uz veselību vai seksuālo dzīvi attiecināmus datus. Sensitīvu datu apstrāde ir principā aizliegta.[142] Tomēr ir pilnīgs uzskaitītu šā aizlieguma izņēmumu saraksts, ko var atrast direktīvas 8. panta 2. un 3. punktā. Šie izņēmumi ietver datu subjekta skaidri paustu piekrišanu, datu subjekta būtiskas intereses, citu likumīgas intereses un sabiedrības intereses.

Atšķirībā no nesensitīvu datu apstrādes gadījuma, līgumiskas attiecības ar datu subjektu netiek uzlūkotas kā vispārīgs pamats likumīgai sensitīvu datu apstrādei. Tāpēc, ja sensitīvi dati ir jāapstrādā saistībā ar līgumu ar datu subjektu, šo datu izmantošanai vajag atsevišķu, skaidri paustu datu subjekta piekrišanu, kas papildina piekrišanu slēgt līgumu. Datu subjekta skaidri pausts pieprasījums pēc precēm vai pakalpojumiem, kuros katrā ziņā ir jāatklāj sensitīvi dati, tomēr ir jāuzskata par tikpat ticamu kā skaidri pausta piekrišana.

Piemērs: Ja aviokompānijas pasažieris, rezervējot lidojumu, prasa, lai aviokompānija viņam nodrošinātu ratiņkrēslu un *kosher* ēdienu, aviokompānija drīkst izmantot šos datus, pat ja pasažieris nav parakstījis papildu punktu par piekrišanu ar apgalvojumu, ka viņš vai viņa piekrīt, ka tiek izmantoti viņa/viņas dati, kuri atklāj informāciju par šīs personas veselību un reliģiskajiem uzskatiem.

Datu subjekta skaidri pausta piekrišana

Pirmais jebkuru datu likumīgas apstrādes nosacījums – neatkarīgi no tā, vai dati ir vai nav sensitīvi –, ir datu subjekta piekrišana. Sensitīvu datu gadījumā tādai piekrišanai jābūt skaidri paustai. Valsts tiesību aktos tomēr var paredzēt, ka piekrišana sensitīvu datu izmantošanai nav pietiekams tiesiskais pamats, lai atļautu to apstrādi,[143] piemēram, ja ārkārtas gadījumos apstrāde ietver neparastus riskus datu subjektam.

Vienā īpašā gadījumā, pat noklusētu piekrišanu atzīst par tiesisku pamatu sensitīvu datu apstrādei: direktīvas 8. panta 2. punktā ir paredzēts, ka apstrāde nav aizliegta, ja tā attiecas uz datiem, kurus datu subjekts publiski darījis zināmus atklātībai. Šajā noteikumā ir acīmredzami prezumēts, ka datu subjekta rīcība, darot savus datus zināmus atklātībai, ir jāinterpretē kā datu subjekta noklusēta piekrišana minēto datu izmantošanai.

142 Datu aizsardzības direktīva, 8. panta 1. punkts.

143 Turpat, 8. panta 2. punkta a) apakšpunkts.

Datu subjekta būtiskās intereses

Tāpat kā nesensitīvu datu gadījumā, sensitīvus datus drīkst apstrādāt datu subjekta būtisku interešu dēļ.[144]

Lai sensitīvu datu apstrāde uz šā pamata būtu likumīga, ir jābūt bijis neiespējamam iesniegt jautājumu izlemšanai datu subjektam, piemēram, tāpēc, ka datu subjekts bija bezsamaņā vai nebija klāt, un ar viņu nevarēja sazināties.

Citu likumīgās intereses

Tāpat kā nesensitīvo datu gadījumā, citu likumīgās intereses var būt par pamatu sensitīvu datu apstrādei. Attiecībā uz sensitīviem datiem, un atbilstoši datu aizsardzības direktīvas 8. panta 2. punktam, tas tomēr attiecas tikai uz šādiem gadījumiem:

- ja apstrāde vajadzīga, lai aizsargātu citas personas būtiskas intereses,[145] ja datu subjekts ir fiziski vai tiesiski nespējīgs dot savu piekrišanu;

- ja sensitīvi dati ir būtiski nodarbināšanas tiesību aktu jomā, piemēram, veselības dati saistībā ar īpaši bīstamu darbavietu, vai dati par reliģiskajiem uzskatiem – piemēram, saistībā ar brīvdienām;[146]

- ja fonds, apvienība vai jebkura cita bezpeļņas institūcija, kam ir politisks, filozofisks, reliģisks vai arodbiedrību darbības mērķis, apstrādā datus par saviem biedriem vai sponsoriem vai citām ieinteresētajām personām (šādi dati ir sensitīvi, jo tie visdrīzāk atklās attiecīgo personu reliģisko vai politisko pārliecību);[147]

- ja sensitīvus datus izmanto saistībā ar tiesvedību tiesā vai administratīvā iestādē, lai celtu, realizētu vai aizstāvētu juridisku prasību.[148]

- Turklāt atbilstoši datu aizsardzības direktīvas 8. panta 3. punktam, ja veselības datus izmanto medicīnas izmeklēšanām un ārstēšanai, ko veic veselības aprūpes pakalpojumu sniedzēji, uz šādu pakalpojumu pārvaldību attiecas minētais

144 Turpat, 8. panta 2. punkta c) apakšpunkts.

145 Turpat.

146 Turpat, 8. panta 2. punkta b) apakšpunkts.

147 Turpat, 8. panta 2. punkta d) apakšpunkts.

148 Turpat, 8. panta 2. punkta e) apakšpunkts.

izņēmums. Īpaša garantija ir tā, kas personas atzīst par „veselības aprūpes pakalpojumu sniedzējiem" tikai tad, ja uz tām attiecas īpaši profesionālie konfidencialitātes pienākumi.

Sabiedrības intereses

Papildus, atbilstoši datu aizsardzības direktīvas 8. panta 4. punktam, dalībvalstis var ieviest turpmākus nolūkus, kuriem drīkst apstrādāt sensitīvus datus, kamēr vien:

- datu apstrāde notiek, pamatojoties uz būtiskām sabiedrības interesēm; un
- tas ir paredzēts vai nu attiecīgās valsts tiesību aktos vai ar uzraudzības iestādes lēmumu; un
- valsts tiesību aktos vai uzraudzības iestādes lēmumā ir paredzētas vajadzīgās garantijas, lai efektīvi aizsargātu datu subjektu intereses.[149]

Redzams piemērs ir elektronisko veselības datņu sistēmas, kas tiks izveidotas daudzās dalībvalstīs. Šādas sistēmas dod iespēju padarīt veselības datus, ko veselības aprūpes pakalpojumu sniedzēji savākuši pacienta ārstēšanas gaitā, pieejamus citiem šā pacienta veselības aprūpes pakalpojumu sniedzējiem, parasti valsts mērogā.

29. panta darba grupa secināja, ka šādu sistēmu izveide nevarēja notikt saskaņā ar juridiskajām normām, kas ir spēkā attiecībā uz pacientu datu apstrādi uz datu aizsardzības direktīvas 8. panta 3. punkta pamata. Tomēr, pieņemot, ka šādu elektronisko veselības datņu pastāvēšana veido būtiskas sabiedrības intereses, to var pamatot uz direktīvas 8. panta 4. punktu, kas prasa konkrētu tiesisku pamatu to izveidei un ietver arī vajadzīgās garantijas, lai nodrošinātu tādas sistēmas drošu vadību.[150]

149 Turpat, 8. panta 4. punkts.

150 29. panta darba grupa (2007), *Darba dokuments par personas ar veselību saistīto datu apstrādi elektroniskajās pacienta veselības kartēs,* WP 131, Briselē, 2007. gada 15. februārī.

4.2. Normas par apstrādes drošību

Galvenie punkti

- Normas par apstrādes drošību ietver nosacījumu, ka pārzinim un personas datu operatoram ir pienākums veikt atbilstošus tehniskus un organizatoriskus pasākumus, lai novērstu jebkuru nesankcionētu iejaukšanos datu apstrādes darbībās.
- Vajadzīgo datu drošības līmeni nosaka:
  - drošības iezīmes, kas tirgū pieejamas jebkuram apstrādes veidam; un
  - izmaksas; un
  - apstrādāto datu sensitivitāte.
- Datu drošu apstrādi turpmāk garantē vispārīgās visu personu, pārziņu vai personas datu operatoru saistības nodrošināt, ka dati paliek konfidenciāli.

Tāpēc pārziņu un personas datu operatoru pienākums veikt pienācīgus pasākumus datu drošības garantēšanai ir noteikts **EP datu aizsardzības tiesību aktos,** kā arī **EU datu aizsardzības tiesību aktos**.

4.2.1. Datu drošības elementi

Atbilstoši attiecīgajiem **ES tiesību** noteikumiem:

> *„Dalībvalstis paredz to, ka personas datu apstrādātājam [pārzinim] jāīsteno atbilstoši tehniski un organizatoriski pasākumi, lai aizsargātu personas datus pret nejaušu vai nelikumīgu iznīcināšanu vai nejaušu pazaudēšanu, pārveidošanu, nesankcionētu atklāšanu vai piekļuvi, īpaši, ja apstrāde ietver datu pārraidi [nodošanu] pa elektronisko sakaru tīklu, un pret visām citām nelikumīgām apstrādes formām".*[151]

Līdzīgs noteikums pastāv saskaņā ar EP tiesību aktiem:

> *„Veic atbilstošus drošības pasākumus, lai nodrošinātu, ka automatizētu datu datnēs uzglabātus personas datus efektīvi aizsargā no nejaušas*

151 Datu aizsardzības direktīva, 17. panta 1. punkts.

vai neatļautas iznīcināšanas vai nejaušas zaudēšanas, kā arī neatļautas piekļuves, pārveidošanas un izpaušanas."[152]

Bieži vien pastāv arī rūpnieciski, valstu un starptautiski standarti, izstrādāti drošai datu apstrādei. Eiropas privātuma zīmogs (*EuroPriSe*), piemēram, ir ES *eTEN* (Eiropas telekomunikāciju tīkli) projekts, kurā ir izpētītas iespējas sertificēt izstrādājumus, jo īpaši programmatūru, kā atbilstīgus Eiropas tiesību aktiem datu aizsardzības jomā. Tika izveidota Eiropas Tīklu un informācijas drošības aģentūra (*ENISA*), lai pastiprinātu ES, ES dalībvalstu un tātad uzņēmēju sabiedrības spēju novērst un risināt tīklu un informācijas drošības problēmas, un reaģēt uz tām.[153] *ENISA* regulāri publicē pašreizējās situācijas apdraudējumu analīzi un padomus, kā tos risināt.

Datu drošību nevar sasniegti, tikai ieviešot pareizo aprīkojumu – datoraparatūru un programmatūru. Ir vajadzīgas arī pienācīgas iekšējās organizācijas normas. Ideālā situācijā tādas iekšējās normas regulē šādus jautājumus:

- regulāra informācijas sniegšana visiem darbiniekiem par datu drošības normām un viņu pienākumiem atbilstoši datu aizsardzības tiesību aktiem, jo īpaši attiecībā uz viņu pienākumu ievērot konfidencialitāti;

- skaidra atbildības sadale un skaidrs kompetenču izklāsts datu apstrādes jautājumos, jo īpaši attiecībā uz lēmumiem apstrādāt personas datus un nodot datus trešām personām;

- personas datu izmantošana tikai atbilstoši kompetentās personas instrukcijām vai atbilstoši vispārīgi noteiktām normām;

- piekļuves pārziņa vai personas datu operatora telpām un datoraparatūrai un programmatūrai aizsardzība, tostarp piekļuves sankcionēšanas pārbaudes;

- nodrošināšana, ka atļaujas piekļūt personas datiem piešķir kompetenta persona, un ka šādām atļaujām prasa atbilstošu dokumentāciju;

- automatizēti protokoli, lai piekļūtu personas datiem ar elektroniskiem līdzekļiem, un regulāras šādu protokolu pārbaudes, ko veic iekšējais uzraudzības dienests;

152 108. konvencija, 7. pants.

153 Eiropas Parlamenta un Padomes 2004. gada 10. marta Regula (EK) Nr. 460/2004, ar ko izveido Eiropas Tīklu un informācijas drošības aģentūru, OV 2004 L 77.

- rūpīga citu atklāšanas formu – kas nav automatizēta piekļuve datiem – dokumentācija, lai būtu iespējams pierādīt, ka nav notikusi nelikumīga datu nodošana.

Pienācīgu datu drošības mācību un izglītošanas piedāvājums personālam arī ir svarīgs efektīvu drošības piesardzības pasākumu elements. Jāīsteno arī verifikācijas procedūras, lai nodrošinātu, ka šādi atbilstoši pasākumi nepaliek tikai uz papīra, bet tiek īstenoti un darbojas praksē (piemēram, iekšējās vai ārējās revīzijas).

Pārziņa vēlas, lai personas datu operatora veiktie pasākumi drošības līmeņa uzlabošanai ietver tādus instrumentus kā personas datu aizsardzības speciālisti, darbinieku izglītošana drošības jomā, regulāras revīzijas, ielaušanās testēšana un kvalitātes zīmogi.

Piemērs: Lietā *I. pret Somiju*[154] prasītāja nespēja pierādīt, ka citi slimnīcas, kurā viņi strādāja, darbinieki bija nelikumīgi piekļuvuši viņas medicīnas kartei. Tāpēc valsts tiesas noraidīja viņas prasību par viņas tiesību uz datu aizsardzību aizskārumu. ECT secināja, ka ir bijis ECK 8. panta prasību pārkāpums, jo slimnīcas veselības dokumentācijas reģistrācijas sistēma „bija tāda, ka nebija iespējams ar atpakaļejošu datumu noskaidrot pacientu medicīnas karšu izmantošanu, jo tā uzrādīja tikai piecas nesenākās konsultācijas, un šī informācija tika dzēsta pēc datnes ievietošanas atpakaļ arhīvā". Tiesai izšķirīgi bija tas, ka slimnīcā ieviestā reģistrācijas sistēma skaidri nebija atbildusi valsts tiesību aktos ietvertajām juridiskajām prasībām – šim faktam valsts tiesas nebija piešķīrušas pienācīgu svaru.

Paziņojums par datu aizsardzības pārkāpumiem

Vairāku Eiropas valstu datu aizsardzības tiesību aktos ir ieviests jauns instruments, ar kuru cīnīties pret datu drošības pārkāpumiem: pienākums elektronisko komunikācijas pakalpojumu sniedzējiem paziņot iespējamiem cietušajiem un uzraudzības iestādēm par datu drošības pārkāpumiem. Telekomunikāciju sniedzējiem tas ir obligāti saskaņā ar ES tiesību aktiem.[155] Datu subjektam sniegta paziņojuma par datu aizsar-

154 ECT 2008. gada 17. jūlija spriedums lietā *I. pret Somiju*, prasības pieteikums Nr. 20511/03.

155 Sk. 4. panta 3. punktu Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīvā 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, kas grozīta ar Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīvu 2009/136/EK, ar ko groza Direktīvu 2002/22/EK par universālo pakalpojumu un lietotāju tiesībām attiecībā uz elektronisko sakaru tīkliem un pakalpojumiem; sk. arī 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.

dzības pārkāpumiem nolūks ir novērst kaitējumu: paziņojumi par datu pārkāpumiem un to iespējamām sekām mazina risku, ka būs negatīva ietekme uz datu subjektiem. Rupjas nolaidības gadījumos pakalpojumu sniedzējiem var uzlikt sodu.

Iepriekšēja iekšējo procedūru izveide efektīvai drošības pārkāpumu pārvaldībai un ziņošanai par tiem būs nepieciešama, jo laika periods, kurā jāizpilda paziņošanas pienākums attiecībā pret datu subjektiem un/vai uzraudzības iestādi, ievērojot valsts tiesību aktus, parasti ir diezgan īss.

4.2.2. Konfidencialitāte

Saskaņā ar ES tiesību aktiem datu drošu apstrādi vēl vairāk garantē vispārējais visu personu – pārziņu vai personas datu operatoru – pienākums nodrošināt, lai dati paliktu slepenībā.

Piemērs: Apdrošināšanas kompānijas darbinieks saņem savā darbavietā tālruņa zvanu no kāda, kurš apgalvo, ka ir klients un prasa informāciju par savu apdrošināšanas līgumu.

Pienākums paturēt klientu datus slepenībā prasa, lai darbinieks pirms personas datu atklāšanas veiktu vismaz minimālus drošības pasākumus. To var izdarīt, piemēram, piedāvājot atzvanīt uz tālruņa numuru, kas ir norādīts klienta personīgajā lietā.

Datu aizsardzības direktīvas 16. pants regulē konfidencialitāti tikai pārziņa–personas datu operatora attiecībās. Tas, vai pārziņiem ir vai nav jāpatur dati slepenībā, tādā ziņā, ka viņi tos nedrīkst atklāt trešām personām, ir skatīts direktīvas 7. un 8. pantā.

Konfidencialitātes pienākums neattiecas uz situācijām, kurās dati kļūst zināmi personai privātas personas, nevis pārziņa vai personas datu operatora darbinieka statusā. Šādā gadījumā datu aizsardzības direktīvas 16. pantu nepiemēro, jo uz to, ka privātas personas izmanto personas datus, direktīvas darbības joma pilnīgi neattiecas, jo tur tāda izmantošana ietilpst tā dēvētā „izņēmuma mājsaimniecības vajadzībām" robežās.[156] Izņēmums mājsaimniecības vajadzībām ir personas datu izmantošana, ko veic „fiziska persona tikai un vienīgi personiska vai mājsaimnieciska pasākuma

156 Datu aizsardzības direktīva, 3. panta 2. punkta otrais ievilkums.

gaitā".[157] Kopš Tiesas sprieduma lietā *Bodil Lindqvist*[158] šis izņēmums tomēr ir jāinterpretē šauri, jo īpaši attiecībā uz datu atklāšanu. Jo īpaši, izņēmums mājsaimniecības vajadzībām neattieksies uz personas datu publicēšanu internetā neierobežotam saņēmēju skaitam (vairāk informācijas par šo lietu sk. 2.1.2, 2.2, 2.3.1 un 6.1 iedaļu).

Saskaņā ar EP tiesību aktiem nosacījums par konfidencialitātes ievērošanas pienākumu ir ietverts datu drošības jēdzienā 108. konvencijas 7. pantā, kas aplūko datu drošību.

Personas datu operatoriem konfidencialitāte nozīmē, ka tie drīkst izmantot tiem pārziņa uzticētos personas datus tikai saskaņā ar pārziņa sniegtajām instrukcijām. Pārziņa vai personas datu operatora darbiniekiem konfidencialitāte prasa, lai viņi izmantotu personas datus tikai atbilstoši viņu kompetento uzraugu instrukcijām.

Konfidencialitātes pienākums ir jāietver jebkurā līgumā starp pārziņiem un viņu personas datu operatoriem. Turpmāk pārziņiem un personas datu operatoriem būs jāveic īpaši pasākumi, lai noteiktu saviem darbiniekiem juridisku konfidencialitātes pienākumu, ko parasti nodrošina, iekļaujot noteikumus par konfidencialitāti darbinieka darba līgumā.

Profesionālo konfidencialitātes pienākumu neievērošana ir sodāma saskaņā ar krimināllikumu daudzās ES dalībvalstīs un 108. konvencijas Līgumslēdzējās Pusēs.

4.3. Apstrādes caurskatāmības normas

Galvenie punkti

- Pirms personas datu apstrādes sākuma pārzinim ir vismaz jāinformē datu subjekti par pārziņa identitāti un datu apstrādes nolūku, izņemot gadījumus, kad datu subjektam jau ir šī informācija.
- Kad datus vāc no trešām personām, informācijas sniegšanas pienākumu nepiemēro šādos gadījumos:
  - datu apstrāde ir paredzēta tiesību aktos; vai

157 Turpat.

158 Tiesas 2003. gada 6. novembra spriedums lietā C-101/01 *Bodil Lindqvist*.

  - informācijas sniegšana izrādās neiespējama vai arī būtu jāpieliek nesamērīgas pūles, lai to izdarītu.
- Pirms personas datu apstrādes sākšanas pārzinim papildus ir:
  - jāpaziņo uzraudzības iestādei par plānotajām apstrādes darbībām; vai
  - jānoorganizē, lai neatkarīgs personas datu aizsardzības speciālists gatavo iekšēju apstrādes dokumentāciju, ja valsts tiesību akti paredz šādu procedūru.

Godprātīgas apstrādes princips prasa apstrādes caurskatāmību. **EP tiesību aktos** šajā nolūkā ir noteikts, ka jebkurai personai jābūt iespējamam uzzināt par datu apstrādes datņu pastāvēšanu, par to nolūku un atbildīgo pārzini.[159] Kā to sasniegt, ir atstāts vietējo tiesību aktu ziņā. **ES tiesību akti** ir specifiskāki un nodrošina caurskatāmību datu subjektam, nosakot pārzinim pienākumu informēt datu subjektu, bet plašai sabiedrībai – ar paziņojumu.

Saskaņā ar abām juridiskajām sistēmām valsts tiesību aktos var noteikt pārziņa caurskatāmības pienākuma izņēmumus un ierobežojumus, ja šāds ierobežojums ir nepieciešams pasākums, lai aizsargātu noteiktas sabiedrības intereses vai aizsargātu datu subjektu vai citu tiesības un brīvības, kamēr vien tas ir nepieciešams demokrātiskā sabiedrībā.[160] Šādi izņēmumi var būt vajadzīgi, piemēram, saistībā ar noziegumu izmeklēšanu, bet var tikt attaisnoti arī citos apstākļos.

4.3.1. Informācija

Atbilstoši EP tiesību aktiem, kā arī ES tiesību aktiem apstrādes darbību pārziņiem ir pienākums iepriekš informēt datu subjektu par plānoto apstrādi.[161] Šis pienākums nav atkarīgs no datu subjekta pieprasījuma, bet pārzinim tas jāveic proaktīvi, neatkarīgi no tā, vai datu subjekts izrāda interesi par informāciju vai nē.

Informācijas saturs

Informācijā jāietver apstrādes nolūks, kā arī pārziņa identitāte un kontaktinformācija.[162] Datu aizsardzības direktīvā ir prasīts sniegt turpmāku informāciju, kad tā „ir vajadzīga, ņemot vērā konkrētos apstākļus, kādos dati ievākti, lai garantētu god-

159 108. konvencija, 8. panta a) punkts.

160 *Turpat,* 9. panta 2. punkts; un Datu aizsardzības direktīva, 13. panta 1. punkts.

161 108. konvencija, 8. panta a) punkts; un Datu aizsardzības direktīva, 10. un 11. pants.

162 108. konvencija, 8. panta a) punkts; un Datu aizsardzības direktīva, 10. panta a) un b) punkts.

prātīgu apstrādi attiecībā uz datu subjektu". Direktīvas 10. un 11. pantā citu aspektu starpā ir izklāstītas apstrādāto datu kategorijas un šādu datu saņēmēji, kā arī datu piekļuves tiesību un tiesību uz datu labošanu pastāvēšana. Ja datus ievāc no datu subjektiem, informācijai jāpaskaidro, vai atbildes uz jautājumiem ir obligātas vai brīvprātīgas, kā arī iespējamās sekas neatbildēšanai.[163]

No **EP tiesību aktu** viedokļa šādas informācijas sniegšanu var uzskatīt par labu praksi saskaņā ar godīgas datu apstrādes principu, un tik lielā mērā tā ir arī EP tiesību aktu daļa.

Godprātīgas apstrādes princips prasa, lai informācija būtu datu subjektiem viegli saprotama. Jāizmanto valoda, kas ir vispiemērotākā adresātam. Izmantotās valodas līmenim un veidam jābūt atšķirīgiem atkarībā no tā, vai plānotā auditorija ir, piemēram, pieaugušie vai bērni, plaša sabiedrība vai kompetenti profesionāļi.

Daži datu subjekti vēlēsies uzzināt tikai vispārīgos vilcienos, kā un kāpēc viņu datus apstrādā, savukārt citi prasīs sīku paskaidrojumu. Kā līdzsvarot šo godīgas informācijas aspektu, ir aplūkots kādā 29. panta darba grupas atzinumā, kas veicina tā dēvēto vairāklīmeņu paziņojumu ideju,[164] kas ļauj datu subjektam nolemt, kuru detalizācijas līmeni viņš vai viņa vēlas.

Informācijas sniegšanas laiks

Datu aizsardzības direktīva satur nedaudz atšķirīgus noteikumus par laiku, kad informācija jāsniedz – atkarībā no tā, vai datus ievāc no datu subjekta (10. pants) vai no trešās personas (11. pants). Ja datus ievāc no datu subjekta, informācija ir jāsniedz vēlākais ievākšanas laikā. Ja datus ievāc no trešām personām, informācija ir jāsniedz vēlākais vai nu laikā, kad pārzinis reģistrē datus, vai pirms tam, kad datus pirmo reizi atklāj trešām personām.

Izņēmumi no informēšanas pienākuma

Saskaņā ar ES tiesību aktiem vispārīgs izņēmums no pienākuma informēt datu subjektu pastāv tad, ja datu subjektam jau ir informācija.[165] Tas attiecas uz situācijām,

163 Datu aizsardzības direktīva, 10. panta c) punkts.

164 29. panta darba grupa (2004), *Atzinums 10/2004 par saskaņotākas informācijas noteikumiem*, WP 100, Briselē, 2004. gada 25. novembrī.

165 Datu aizsardzības direktīva, 10. pants un 11. panta 1. punkts.

kurās datu subjekts atbilstoši lietas apstākļiem jau zinās, ka noteikts pārzinis noteiktam nolūkam apstrādās viņa vai viņas datus.

Direktīvas 11. pantā, kas attiecas uz pienākumu informēt datu subjektu, ja dati nav iegūti no viņa vai viņas ir paredzēts arī, ka šāda pienākuma nebūs, jo īpaši apstrādei statistiskiem nolūkiem vai vēsturiskas vai zinātniskas pētniecības nolūkiem, ja:

- šādas informācijas sniegšana izrādās neiespējama; vai
- tas radītu nesamērīgas pūles; vai
- reģistrēšanu vai atklāšanu konkrēti nosaka attiecīgās valsts tiesības.[166]

Tikai datu aizsardzības direktīvas 11. panta 2. punktā ir noteikts, ka datu subjekti nav jāinformē par apstrādes darbībām, ja tās ir noteiktas tiesību aktos. Ņemot vērā vispārīgo juridisko pieņēmumu, ka personas, uz kurām attiecas tiesību akti, tos zina, var iebilst, ka gadījumos, kad datus no datu subjekta ievāc atbilstoši direktīvas 10. pantam, datu subjektam ir informācija. Tomēr, tā kā zināšanas par tiesību aktiem ir tikai pieņēmums, godprātīgas apstrādes princips prasa saskaņā ar 10. pantu, lai datu subjekts būtu informēts, pat ja apstrāde ir noteikta tiesību aktos, jo īpaši tāpēc, ka datu subjekta informēšana neuzliek pārmērīgu slogu, ja datus ievāc tieši no datu subjekta.

Kas attiecas uz EP tiesību aktiem, 108. konvencijā ir konkrēti paredzēti izņēmumi no tās 8. panta. Arī šeit datu aizsardzības direktīvas 10. un 11. pantā izklāstītie izņēmumi var tikt uzlūkoti kā labas prakses piemēri izņēmumiem saskaņā ar 108. konvencijas 9. pantu.

Dažādi informācijas sniegšanas veidi

Ideālais informācijas sniegšanas veids būtu mutiski vai rakstveidā vērsties pie katra datu subjekta atsevišķi. Ja datus vāc no datu subjekta, informācijas sniegšanai jānotiek vienlaikus ar vākšanu. Tomēr, jo īpaši, ja datus vāc no trešām personām, ņemot vērā acīmredzamās praktiskās grūtības, lai personīgi sasniegtu datu subjektus, informāciju var sniegt arī ar atbilstošu publikāciju.

166 Turpat, preambulas 40. apsvērums un 11. panta 2. punkts.

Viens no efektīvākajiem informācijas sniegšanas veidiem būs norādīt atbilstošus noteikumus par informāciju pārziņa mājas lapā, piemēram, tīmekļa vietnes privātuma politiku. Tomēr ir nozīmīga sabiedrības daļa, kura nelieto internetu, un uzņēmuma vai valsts iestādes informācijas politikā šis aspekts ir jāņem vērā.

4.3.2. Paziņošana

Valsts tiesību aktos var noteikt pārzinim pienākumu paziņot kompetentajai uzraudzības iestādei par savām apstrādes darbībām, lai tās var publicēt. Alternatīvi valsts tiesību aktos var noteikt, ka pārziņi var noalgot personas datu aizsardzības amatpersonu, kura atbild jo īpaši par pārziņa veikto apstrādes darbību reģistra uzturēšanu.[167] Šis iekšējais reģistrs pēc pieprasījuma jādara pieejams sabiedrībai.

Piemērs: Iekšējās personas datu aizsardzības speciālista paziņojumā, kā arī dokumentācijā ir jāapraksta konkrētās datu apstrādes galvenās iezīmes. Tur ietilpst informācija par pārzini, apstrādes nolūks, apstrādes tiesiskais pamats, apstrādāto datu kategorijas, iespējamās trešās personas–saņēmējas un tas, vai ir vai nav plānotas pārrobežu datu plūsmas, un, ja jā, tad kuras.

Uzraudzības iestādei paziņojumi jāpublicē īpašā reģistrā. Lai reģistrs izpildītu savu mērķi, piekļuvei reģistram jābūt vieglai un bezmaksas. Tas pats attiecas uz dokumentāciju, kuru uztur pārziņa personas datu aizsardzības speciālists.

Valsts tiesību aktos var paredzēt izņēmumus no saistībām sniegt paziņojumu kompetentajai uzraudzības iestādei vai nodarbināt iekšēju datu aizsardzības speciālistu attiecībā uz apstrādes darbībām, kuras visdrīzāk nevar radīt specifisku risku datu subjektam; šie izņēmumi ir uzskaitīti datu aizsardzības direktīvas 18. panta 2. punktā.[168]

167 Turpat, 18. panta 2. punkta otrais ievilkums.

168 Turpat, 18. panta 2. punkta pirmais ievilkums.

4.4. Atbilstības veicināšanas normas

Galvenie punkti

- Izstrādājot atbildības principu, datu aizsardzības direktīva piemin vairākus atbilstības veicināšanas instrumentus:
  - valsts uzraudzības iestādes iepriekš veikta plānoto apstrādes darbību pārbaude;
  - personas datu aizsardzības speciālisti, kuri sniedz pārzinim īpašu kompetenci datu aizsardzības jomā;
  - rīcības [profesionālās ētikas] kodeksi, kuros precizētas esošās datu aizsardzības normas piemērošanai sabiedrības, īpaši uzņēmējsabiedrības, filiālē.
- EP tiesību aktos ir ierosināti līdzīgi instrumenti, lai veicinātu atbilstību tās Ieteikumā par profilēšanu.

4.4.1. Iepriekšēja pārbaude

Atbilstoši datu aizsardzības direktīvas 20. pantam uzraudzības iestādei pirms apstrādes sākuma ir jāpārbauda apstrādes darbības, kuras var radīt īpašus riskus datu subjektu tiesībām un brīvībām – vai nu apstrādes nolūka vai apstrādes apstākļu dēļ. Valsts tiesību aktos ir jānosaka, kuras apstrādes darbības ir iepriekš jāpārbauda. Tādas pārbaudes rezultātā apstrādes darbības var aizliegt vai arī var izdot rīkojumu, ka ir jāmaina ierosinātais apstrādes darbību plānojums. Direktīvas 20. panta mērķis ir nodrošināt, lai nevajadzīgi riskanta apstrāde vispār nesāktos, jo uzraudzības iestādei ir pilnvaras aizliegt šādas darbības. Priekšnoteikums šāda mehānisma efektivitātes panākšanai ir tas, ka uzraudzības iestādei ir jābūt informētai. Lai nodrošinātu, ka pārziņi izpilda savu paziņošanas pienākumu, uzraudzības iestādēm vajadzēs piespiedu izpildes pilnvaras, piemēram, iespēju uzlikt pārziņiem sodu.

Piemērs: Ja uzņēmums veic apstrādes darbības, kuras atbilstoši valsts tiesību aktiem ir pakļautas iepriekšējai pārbaudei, šim uzņēmumam ir jāiesniedz uzraudzības iestādei dokumenti par plānotajām apstrādes darbībām. Uzņēmums nedrīkst sākt apstrādes darbības, pirms nav saņēmis apstiprinošu atbildi no uzraudzības iestādes.

Dažās dalībvalstīs valsts tiesību aktos ir paredzēta alternatīva iespēja, ka apstrādes darbības var sākt, ja atbilde no uzraudzības iestādes nepienāk noteiktā laika periodā, piemēram, trīs mēnešos.

4.4.2. Personas datu aizsardzības amatpersonas

Datu aizsardzības direktīvā ir dota iespēja valsts tiesību aktos paredzēt, ka pārziņi var iecelt kādu amatpersonu, kura rīkotos kā personas datu aizsardzības speciālists.[169] Šāda speciālista mērķis ir nodrošināt, ka datu apstrādes darbībām nav iespējams nelabvēlīgi iespaidot datu subjektu tiesības un brīvības.[170]

Piemērs: Vācijā saskaņā ar Vācijas Federatīvā datu aizsardzības likuma (*Bundesdatenschutzgesetz*) 4.f iedaļas 1. apakšiedaļu privātiem uzņēmumiem ir jāieceļ iekšēja personas datu aizsardzības amatpersona, ja tie personas datu automatizētajā apstrādē pastāvīgi nodarbina 10 vai vairāk personu.

Spēja sasniegt šo mērķi prasa speciālista amatam zināmu neatkarību pārziņa organizācijā, kā tas konkrēti norādīts direktīvā. Lai atbalstītu efektīvu šā biroja darbību, būs nepieciešamas arī stingras tiesības nodarbināšanas jomā, lai veiktu piesardzības pasākumus pret negadījumiem, piemēram, nepamatotu atlaišanu.

Lai veicinātu atbilstību valsts datu aizsardzības tiesību aktiem, „iekšēju personas datu aizsardzības amatpersonu [speciālistu]" jēdziens ir pieņemts arī dažos EP Ieteikumos.[171]

4.4.3. Rīcības kodeksi

Lai veicinātu atbilstību, uzņēmējdarbības un citas nozares var izstrādāt detalizētus noteikumus, kas regulētu to raksturīgās apstrādes darbības, kodificējot labāko praksi. Nozares dalībnieku pieredze palīdzēs atrast risinājumus, kas būtu praktiski un līdz ar to visdrīzāk. tiks ievēroti. Attiecīgi dalībvalstis – kā arī Eiropas Komisija – tiek mudinātas atbalstīt tādu profesionālās ētikas [rīcības] kodeksu izstrādi, kas paredzēti, lai veicinātu dalībvalstu saskaņā ar šo direktīvu pieņemto noteikumu atbilstīgu ieviešanu, ņemot vērā dažādo nozaru raksturīgās iezīmes.[172]

169 Turpat, 18. panta 2. punkta otrais ievilkums.

170 Turpat.

171 Sk., piemēram, Ieteikumu par profilēšanu, 8.3. punktu.

172 Sk. datu aizsardzības direktīvu, 27. panta 1. punkts.

Lai nodrošinātu, ka minētie rīcības kodeksi atbilst saskaņā ar datu aizsardzības direktīvu pieņemtajiem attiecīgās valsts noteikumiem, dalībvalstis obligāti paredz procedūru minēto kodeksu izvērtēšanai. Šajā procedūrā parasti ir jāiesaistās valsts [varas] iestādēm, arodbiedrībām un citām struktūrām, kas pārstāv citas pārziņu kategorijas.[173]

Kopienas kodeksu projektus un esošo Kopienas kodeksu grozījumus vai paplašinājumus var iesniegt 29. panta darba grupai. Pēc šīs darba grupas apstiprinājuma Eiropas Komisija var nodrošināt, ka kodeksus attiecīgi dara zināmus atklātībai.[174]

Piemērs: **Eiropas** Tiešā un interaktīvā mārketinga federācija (*FEDMA*) izstrādāja Eiropas rīcības kodeksu personas datu izmantošanai tiešajā tirgvedībā. Kodeksu vēlāk iesniedza 29. panta darba grupai. 2010. gadā kodeksam tika pievienots Pielikums par elektroniskajiem paziņojumiem tiešajā tirdzniecībā [tirgvedībā].[175]

173 Turpat, 27. panta 2. punkts.

174 Turpat, 27. panta 3. punkts.

175 29. panta darba grupa (2010), *Atzinums 4/2010 par FEDMA Eiropas rīcības kodeksu personas datu izmantošanai tiešajā tirdzniecībā [tirgvedībā]*, WP 174, Briselē, 2010. gada 13. jūlijā.

5

Datu subjektu tiesības un to [piespiedu] īstenošana

ES	Aplūkotie jautājumi	EP
Piekļuves tiesības		
Datu aizsardzības direktīva, 12. pants Tiesas 2009. gada 7. maija spriedums lietā C-553/07, *College van burgemeester en wethouders van Rotterdam pret M.E.E. Rijkeboer*	**Piekļuves tiesības personas pašas datiem**	108. konvencija, 8. panta b) punkts
	Datu labošanas, dzēšanas vai bloķēšanas tiesības	108. konvencija, 8. panta c) punkts ECT 2008. gada 18. novembra spriedums lietā *Cemalettin Canli pret Turciju*, prasības pieteikums Nr. 22427/04 ECT 2006. gada 6. jūnija spriedums lietā *Segerstedt-Wiberg un citi pret Zviedriju*, prasības pieteikums Nr. 62332/00 ECT 2010. gada 27. aprīļa spriedums lietā *Ciubotaru pret Moldovu*, prasības pieteikums Nr. 27138/04
Iebilduma tiesības		
Datu aizsardzības direktīva, 14. panta 1. punkta a) apakšpunkts	**Iebilduma tiesības datu subjekta īpašās situācijas dēļ**	Ieteikums par profilēšanu, 5.3. punkts

ES	Aplūkotie jautājumi	EP
Datu aizsardzības direktīva, 14. panta 1. punkta b) apakšpunkts	**Iebilduma tiesības pret turpmāku datu izmantošanu tirgvedības nolūkos**	Ieteikums par tiešo tirdzniecību [tirgvedību], 4.1. punkts
Datu aizsardzības direktīva, 15. pants	**Iebilduma tiesības pret automatizētiem lēmumiem**	Ieteikums par profilēšanu, 5.5. punkts
Neatkarīga uzraudzība		
Harta, 8. panta 3. punkts Datu aizsardzības direktīva, 28. pants ES iestādes, V nodaļa Datu aizsardzības regula Tiesas 2010. gada 9. marta spriedums lietā C-518/07 *Eiropas Komisija pret Vācijas Federatīvo Republiku* Tiesas 2012. gada 16. oktobra spriedums lietā C-614/10 *Eiropas Komisija pret Austrijas Republiku* Tiesas 2014. gada 8. aprīļa spriedums lietā C-288/12 *Eiropas Komisija pret Ungāriju*	**Valsts uzraudzības iestādes**	108. konvencija, papildprotokols, 1. pants
Tiesiskās aizsardzības līdzekļi un sankcijas		
Datu aizsardzības direktīva, 12. pants	**Pieprasījums pārzinim**	108. konvencija, 8. panta b) punkts
Datu aizsardzības direktīva, 28. panta 4. punkts Regula par aizsardzību attiecībā uz personas datu apstrādi ES iestādēs, 32. pants 2. punkts	**Uzraudzības iestādei iesniegtas sūdzības**	108. konvencija, papildprotokols, 1. panta 2. punkta b) apakšpunkts
Harta, 47. pants	**Tiesas (vispār)**	ECK, 13. pants
Datu aizsardzības direktīva, 28. panta 3. punkts	**Valsts tiesas**	108. konvencija, papildprotokols, 1. panta 4. punkts
LESD, 263. panta ceturtā daļa Regula par aizsardzību attiecībā uz personas datu apstrādi ES iestādēs, 32. panta 1. punkts LESD, 267. pants	**Eiropas Savienības Tiesa**	
	Eiropas Cilvēktiesību tiesa	ECK, 34. pants

ES	Aplūkotie jautājumi	EP
Tiesiskās aizsardzības līdzekļi un sankcijas		
Harta, 47. pants Datu aizsardzības direktīva, 22. un 23. pants Tiesas 1984. gada 10. aprīļa spriedums lietā C-14/83 *Sabine von Colson pret Elisabeth Kamann/Land Nordrhein-Westfalen* Tiesas 1986. gada 26. februāra spriedums lietā C-152/84 *M.H. Marshall pret Southampton and South-West Hampshire Area Health Authority*	**Par valsts datu aizsardzības tiesību aktu pārkāpumiem**	ECK, 13. pants (tikai EP dalībvalstīm) 108. konvencija, 10. pants ECT 2008. gada 2. marta spriedums lietā *K.U. pret Somiju*, prasības pieteikums Nr. 2872/02 ECT 2008. gada 25. novembra spriedums lietā *Biriuk pret Lietuvu*, prasības pieteikums Nr. 23373/03
Regula par aizsardzību attiecībā uz personas datu apstrādi ES iestādēs, 34. un 49. pants 2010. gada 29. jūnija spriedums lietā C-28/08 P *Eiropas Komisija pret The Bavarian Lager Co. Ltd.*	**Par ES iestāžu un struktūru izdarītiem ES tiesību pārkāpumiem**	

Tas, cik efektīvas ir juridiskās normas vispārīgi un datu subjektu tiesības konkrēti, lielā mērā ir atkarīgs no to izpildei nepieciešamu atbilstošu mehānismu pastāvēšanas. Eiropas tiesību aktos datu aizsardzības jomā datu subjektiem jābūt valsts tiesību aktos paredzētām pilnvarām aizsargāt savus datus. Valsts tiesību aktos jāizveido arī neatkarīgas uzraudzības iestādes, lai palīdzētu datu subjektiem īstenot savas tiesības un uzraudzīt personas datu apstrādi. Papildus, tiesības uz iedarbīgu tiesiskās aizsardzības līdzekli, kas garantēts atbilstoši ECK un Hartai, prasa, lai šādi līdzekļi būtu pieejami ikvienai personai.

5.1. Datu subjektu tiesības

Galvenie punkti

- Ikvienam ir tiesības saskaņā ar valsts tiesību aktiem lūgt jebkuram pārzinim informāciju par to, vai pārzinis apstrādā viņa vai viņas datus.
- Datu subjektiem saskaņā ar valsts tiesību aktiem ir tiesības:
  - piekļūt saviem datiem no jebkura pārziņa, kurš apstrādā šādus datus;

  - lūgt pārzinim, kurš apstrādā viņu datus, lai datus izlabo (vai attiecīgi bloķē), ja dati ir neprecīzi;
  - lūgt pārzinim attiecīgi dzēst vai bloķēt viņu datus, ja pārzinis viņu datus apstrādā nelikumīgi.
- Vēl datu subjektiem ir iebilduma tiesības pret pārziņiem šādos jautājumos:
  - automatizēti lēmumi (pieņemti, izmantojot personas datus, kuri apstrādāti tikai ar automatizētiem līdzekļiem);
  - viņu datu apstrāde, ja tā rada nesamērīgus rezultātus;
  - viņu datu izmantošana tiešās tirgvedības nolūkos.

5.1.1. Piekļuves tiesības

Saskaņā ar ES tiesību aktiem datu aizsardzības direktīvas 12. pantā ir ietverti datu subjektu piekļuves tiesību elementi, tostarp tiesības saņemt no pārziņa „apstiprinājumu, vai uz viņu attiecināmos datus apstrādā vai neapstrādā, un informāciju vismaz attiecībā uz apstrādes nolūkiem, attiecīgo datu kategorijām un saņēmējiem vai saņēmēju kategorijām, kuriem datus atklāj", kā arī „datu izlabošanu, dzēšanu vai piekļuves noslēgšanu, ja šo datu apstrāde neatbilst šīs direktīvas noteikumiem, īpaši datu nepilnības vai neprecizitātes dēļ".

EP tiesību aktos pastāv šīs pašas tiesības, un tās ir jāparedz valsts tiesību aktos (108. konvencijas 8. pants). Vairākos EP ieteikumos ir izmantots termins „piekļuve", un dažādie piekļuves tiesību aspekti ir aprakstīti un ierosināti īstenošanai valsts tiesību aktos tāpat, kā tas norādīts iepriekšējā punktā.

Atbilstoši 108. konvencijas 9. pantam un datu aizsardzības direktīvas 13. pantam pārziņu pienākumu atbildēt uz datu subjekta piekļuves pieprasījumu var ierobežot, ja pastāv svarīgākas likumīgas citu intereses. Svarīgākas likumīgas intereses var būt vispārējas nozīmes intereses, piemēram, valsts drošība, sabiedriskā drošība un saukšana pie atbildības par noziedzīgiem nodarījumiem, kā arī privātas intereses, kas ir pārliecinošākas nekā datu aizsardzības intereses. Ikvienam izņēmumam un ierobežojumam jābūt nepieciešamam demokrātiskā sabiedrībā, un tiem jābūt samērīgiem ar izvirzīto mērķi. Ārkārtas gadījumos, piemēram, medicīnisko indikāciju dēļ, datu subjekta aizsardzība var prasīt caurskatāmības ierobežošanu; tas jo īpaši attiecas uz katra datu subjekta piekļuves tiesību ierobežošanu.

Ikreiz, kad datus apstrādā tikai zinātnisku pētījumu nolūkiem vai statistikas nolūkiem, datu aizsardzības direktīva atļauj valsts tiesību aktos ierobežot piekļuves tiesības; tomēr jābūt īstenotām pienācīgām juridiskām garantijām. Jo īpaši, ir jānodrošina, ka saistībā ar šādu datu apstrādi netiek veikti pasākumi un netiek pieņemti lēmumi par konkrētu personu un ka „nepārprotami nav nekāda riska pārkāpt datu subjekta privātās dzīves neaizskaramību".[176] Līdzīgi noteikumi ir ietverti 108. konvencijas 9. panta 3. punktā.

Piekļuves tiesības personas pašas datiem

Saskaņā ar EP tiesību aktiem tiesības uz piekļuvi saviem personas datiem ir skaidri atzītas 108. konvencijas 8. pantā. ECT ir vairākkārt apgalvojusi, ka personai pastāv tiesības piekļūt informācijai par citu rīcībā esošiem vai citu izmantotiem attiecīgās personas datiem, un ka šīs tiesības izriet no prasības par privātās dzīves neaizskaramību.[177] Lietā *Leander*[178] ECT secināja, ka tiesības uz piekļuvi valsts iestāžu uzglabātiem personas datiem tomēr noteiktos apstākļos var ierobežot.

Saskaņā ar ES tiesību aktiem tiesības uz piekļuvi saviem personas datiem ir skaidri atzītas datu aizsardzības direktīvas 12. pantā un, kā pamattiesības, Hartas 8. panta 2. punktā.

Direktīvas 12. panta a) punktā ir noteikts, ka dalībvalstīm ir jāgarantē ikvienam datu subjektam piekļuves tiesības saviem personas datiem un informācijai. Jo īpaši, ikvienam datu subjektam ir tiesības saņemt no pārziņa apstiprinājumu par to, vai ar šo datu subjektu saistīti dati tiek apstrādāti vai nē, un informāciju vismaz par šādiem aspektiem:

- apstrādes nolūki;
- attiecīgo datu kategorijas;
- apstrādē esošie dati;

176 Datu aizsardzības direktīva, 13. panta 2. punkts.

177 ECT 1989. gada 7. jūlija spriedums lietā *Gaskin pret Apvienoto Karalisti*, prasības pieteikums Nr. 10454/83; ECT 2003. gada 13. februāra spriedums lietā *Odièvre pret Franciju* [GC], prasības pieteikums Nr. 42326/98; ECT 2009. gada 28. aprīļa spriedums lietā *K.H. un citi pret Slovākiju*, prasības pieteikums Nr. 32881/04; ECT 2012. gada 25. septembra spriedums lietā *Godelli pret Itāliju,* prasības pieteikums Nr. 33783/09.

178 ECT 1985. gada 11. jūlija spriedums lietā *Leander pret Zviedriju*, prasības pieteikums Nr. 9248/81.

- saņēmēji vai saņēmēju kategorijas, kam datus atklāj;
- visa pieejamā informācija par apstrādē esošo datu avotu;
- automatizētu lēmumu gadījumā loģika, kas ievērota ikvienā automatizētā datu apstrādē.

Valsts tiesību aktos var noteikt papildu informāciju, ko sniedz pārzinis, piemēram, citē tiesisko pamatu, kas ļauj veikt datu apstrādi.

Piemērs: Piekļūstot kādas personas datiem, var noteikt, vai dati ir vai nav precīzi. Tāpēc ir nepieciešams, lai datu subjekts būtu informēts par apstrādāto datu kategorijām, kā arī par datu saturu. Tāpēc ir pietiekami, ka pārzinis vienkārši pasaka datu subjektam, ka tas apstrādā šādus datus: viņa vai viņas vārds/uzvārds, adrese, dzimšanas datums un interešu sfēra. Pārzinim ir arī jāatklāj datu subjektam, ka tas apstrādā šādus datus: „vārds/uzvārds: N.N.; adrese: 1040 *Vienna, Schwarzenbergplatz 11, Austria*; dzimšanas datums: 10.10.1974.; un interešu sfēra (atbilstīgi datu subjekta paziņojumam): klasiskā mūzika". Pēdējā postenī papildus ir norādīta informācija par datu avotu.

Paziņojums datu subjektam par apstrādē esošajiem datiem un par jebkuru pieejamu informāciju attiecībā uz to avotu ir jāsniedz saprotamā formā, kas nozīmē, ka pārzinim var nākties sīkāk paskaidrot datu subjektam, ko tas apstrādā. Piemēram, tikai tehnisku saīsinājumu vai medicīnas terminu nosaukšana, atbildot uz piekļuves lūgumu, parasti nebūs pietiekama, pat ja ir uzglabāti tikai tādi saīsinājumi vai termini.

Informācija par pārziņa apstrādāto datu avotu ir jāsniedz, atbildot uz piekļuves lūgumu tiktāl, ciktāl šī informācija ir pieejama. Šis pienākums ir jāsaprot, ņemot vērā godīguma un atbildības principus. Pārzinis nedrīkst nedz iznīcināt informāciju par datu avotu, lai tiktu atbrīvots no pienākuma to atklāt, nedz neņemt vērā parasto standartu un atzītās dokumentācijas vajadzības savas darbības jomā. Neturot dokumentāciju par apstrādāto datu avotu, parasti netiks izpildīti pārziņa pienākumi atbilstoši piekļuves tiesībām.

Ja veic automatizētus novērtējumus, būs jāizskaidro novērtējuma vispārīgā loģika, tostarp īpašie kritēriji, kas ir ņemti vērā datu subjekta novērtējumā.

Direktīvā nav skaidri noteikts, vai tiesības piekļūt informācijai attiecas uz pagātni, un, ja jā, uz kādu periodu pagātnē. Šajā sakarā, kā uzsvērts Tiesas praksē, tiesības uz piekļuvi personas datiem nedrīkst būt nepienācīgi ierobežotas ar termiņiem. Datu subjektiem arī jābūt saprātīgai iespējai iegūt informāciju par agrākām datu apstrādes darbībām.

Piemērs: Lietā *Rijkeboer*[179] Tiesai lūdza noteikt, vai atbilstoši direktīvas 12. panta a) punktam personas piekļuves tiesības informācijai par personas datu saņēmējiem vai saņēmēju kategorijām un par paziņoto datu saturu var ierobežot līdz vienam gadam pirms viņa vai viņas lūguma par piekļuvi.

Lai noteiktu, vai direktīvas 12. panta a) punkts atļauj tādu termiņu, Tiesa nolēma interpretēt minēto pantu, ievērojot direktīvas nolūkus. Tiesa vispirms apgalvoja, ka piekļuves tiesības ir nepieciešamas, lai dotu datu subjektam iespēju īstenot tiesības prasīt pārzinim labot, dzēst vai bloķēt viņa vai viņas datus (12. panta b) punkts), vai paziņot trešām personām, kurām minētie dati ir atklāti, par tādu labošanu, dzēšanu vai bloķēšanu (12. panta c) punkts). Piekļuves tiesības ir nepieciešamas arī tādēļ, lai dotu datu subjektam iespēju īstenot savas iebilduma tiesības attiecībā uz savu datu apstrādi (14. pants) vai savas tiesības rīkoties, ja viņam/viņai tiek nodarīts kaitējums (22. un 23. pants).

Lai nodrošinātu iepriekš minēto noteikumu praktisku iedarbību, Tiesa uzskatīja, 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."

Datu labošanas, dzēšanas un bloķēšanas tiesības

„Jebkurai personai jādod iespēja izmantot piekļuves tiesības apstrādāšanā esošiem datiem, kas attiecas uz šo personu, lai konkrēti pārbaudītu šo datu precizitāti un apstrādes likumību".[180] Saskaņā ar šiem principiem datu subjektiem ir jābūt tiesībām atbilstoši valsts tiesību aktiem pieprasīt pārzinim labot, dzēst vai bloķēt attiecīgo

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

180 Datu aizsardzības direktīva, preambulas 41. apsvērums.

datu subjektu datus, ja viņi domā, ka to apstrāde neatbilst direktīvas noteikumam, jo īpaši datu neprecīzā vai nepilnīgā rakstura dēļ.[181]

Piemērs: Lietā *Cemalettin Canli pret Turciju*[182] ECT nepareizā policijas ziņojumā par kriminālu tiesvedību konstatēja ECK 8. panta prasību pārkāpumu.

Prasītājs divreiz bija ticis iesaistīts kriminālajā tiesvedībā, pamatojoties uz apgalvojumu par viņa dalību nelikumīgās organizācijās, bet nebija ticis notiesāts. Kad prasītāju atkal apcietināja un apsūdzēja par citu noziedzīgu nodarījumu, policija iesniedza krimināltiesai ziņojumu ar virsrakstu „*informācijas veidlapa par papildu pārkāpumiem*", kurā prasītājs bija norādīts kā divu nelikumīgu organizāciju dalībnieks. Prasītāja prasība grozīt ziņojumu un policijas reģistrus tika noraidīta. ECT uzskatīja, ka policijas ziņojumā ietvertā informācija ietilpa ECK 8. panta darbības jomā, jo publiska informācija arī var ietilpt „privātās dzīves" tvērumā, ja šo informāciju [varas] iestādes sistemātiski vāc un uzglabā kartotēkās. Turklāt policijas ziņojums bija nepareizs, un tā sagatavošana un iesniegšana krimināltiesai nebija saskaņā ar tiesību aktiem. Tiesa secināja, ka ir bijis 8. panta prasību pārkāpums.

Piemērs: Lietā *Segerstedt-Wiberg un citi pret Zviedriju*[183] prasītāji bija saistīti ar zināmām liberālām un komunistiskām politiskajām partijām. Viņiem bija aizdomas, ka informācija par viņiem ir iekļauta drošības policijas reģistros. ECT tika apstiprināts, ka konkrēto datu uzglabāšanai bija tiesisks pamats un ka ar to centās sasniegt likumīgu mērķi. Attiecībā uz dažiem prasītājiem ECT konstatēja, ka datu ilgstoša saglabāšana bija nesamērīgs viņu privātās dzīves aizskārums. Piemēram *Schmid* k–ga gadījumā iestādes saglabāja informāciju, ka 1969. gadā viņš domājami bija aicinājis uz vardarbīgu pretošanos policijai demonstrāciju laikā. ECT konstatēja, ka šī informācija nevarēja noderēt būtisku valsts drošības interešu sasniegšanai, jo īpaši ņemot vērā tās vēsturisko raksturu. ECT secināja, ka attiecībā uz četriem no pieciem prasītājiem ir bijis ECK 8. panta prasību pārkāpums.

181 Turpat, 12. panta b) punkts.

182 ECT 2008. gada 18. novembra spriedums lietā *Cemalettin Canli pret Turciju*, prasības pieteikums Nr. 22427/04, 33., 42. un 43. punkts; ECT 2010. gada 2. februāra spriedums lietā *Dalea pret Franciju*, prasības pieteikums Nr. 964/07.

183 ECT 2006. gada 6. jūnija spriedums lietā *Segerstedt-Wiberg un citi pret Zviedriju*, prasības pieteikums Nr. 62332/00, 89. un 90. punkts; sk. arī, piemēram, ECT 2013. gada 18. aprīļa spriedums lietā *M.K. pret Franciju*, prasības pieteikums Nr. 19522/09.

Dažos gadījumos datu subjektam būs pietiekami tikai lūgt labot, piemēram, vārda rakstību, mainīt adresi vai telefona numuru. Ja tomēr tādi lūgumi ir saistīti ar juridiskiem jautājumiem, piemēram, datu subjekta juridisko identitāti vai pareizu dzīvesvietas adresi juridisko dokumentu nogādei, ar labošanas lūgumiem var nepietikt, un pārzinis var būt pilnvarots prasīt apgalvotās neprecizitātes pierādījumu. Tādi pieprasījumi nedrīkst uzlikt datu subjektam nesamērīgu pierādījuma slogu un tādējādi liegt datu subjektiem panākt savu datu labošanu. ECT vairākos gadījumos, kur prasītājs nebija spējis apstrīdēt reģistros glabātās informācijas precizitāti, ir konstatējusi ECK 8. panta prasību pārkāpumus.[184]

Piemērs: Lietā *Ciubotaru pret Moldovu*[185] prasītājs nespēja mainīt oficiālajos reģistros savas etniskās izcelsmes reģistrāciju no moldoviešu uz rumāņu it kā tāpēc, ka viņš nebija pamatojis savu lūgumu. ECT uzskatīja par pieņemamu, ka Valstis, reģistrējot personas etnisko identitāti, prasa objektīvus pierādījumus. Ja tāds lūgums bija gluži subjektīvs un nepamatots, iestādes varēja to noraidīt. Tomēr prasītāja lūgums bija pamatots uz ko vairāk, nekā tikai sava etniskuma subjektīvu uztveri; viņš bija spējis sniegt objektīvi pārbaudāmas saites ar rumāņu etnisko grupu, piemēram, valoda, vārds, empātija un citas. Tomēr saskaņā ar valsts tiesību aktiem prasītājam bija jāiesniedz pierādījumi, ka viņa vecāki bija piederējuši rumāņu etniskajai grupai. Ievērojot vēsturiskos notikumus Moldovā, šāda prasība bija radījusi nepārvaramu šķērsli tādas etniskās identitātes reģistrēšanai, kas atšķiras no Padomju varas iestāžu attiecībā uz viņa vecākiem reģistrētās identitātes. Nedodot iespēju prasītājam panākt, ka viņa prasību izskata, ievērojot objektīvi pārbaudāmus pierādījumus, Valsts nebija spējusi izpildīt savu pozitīvo pienākumu nodrošināt prasītājam efektīvu viņa privātās dzīves neaizskaramību. Tiesa secināja, ka ir bijis ECK 8. panta pārkāpums.

Civilās tiesvedības vai procedūras laikā valsts iestādē, lai nolemtu, vai dati ir pareizi vai nav, datu subjekts var lūgt ierakstīt savu datu datnē ierakstu vai piezīmi, ka datu precizitāte ir apstrīdēta un ka oficiāls lēmums vēl nav pieņemts. Šajā periodā datu pārzinis nedrīkst uzrādīt datus kā drošus vai galīgus, jo īpaši trešām personām.

Datu subjekta lūgums dzēst datus bieži vien ir pamatots uz apgalvojumu, ka datu apstrādei nav likumīga pamata. Šādi apgalvojumi bieži vien rodas tad, kad ir atsaukta piekrišana vai kad noteikti dati vairs nav vajadzīgi, lai izpildītu datu

184 ECT 2000. gada 4. maija spriedums lietā *Rotaru pret Rumāniju*, prasības pieteikums Nr. 28341/95.

185 ECT 2010. gada 27. aprīļa spriedums lietā *Ciubotaru pret Moldovu*, prasības pieteikums Nr. 27138/04, 51. un 59. punkts.

vākšanas nolūku. Pierādījuma slogs, ka datu apstrāde ir likumīga, gulsies uz datu pārzini, jo viņš atbild par apstrādes likumību. Atbilstoši atbildības principam pārzinim jāspēj jebkurā laikā pierādīt, ka viņa veiktajai datu apstrādei ir derīgs tiesisks pamats, pretējā gadījumā apstrāde ir jāaptur.

Ja datu apstrādi apstrīd, jo dati domājami ir nepareizi vai tiek nelikumīgi apstrādāti, datu subjekts saskaņā ar godprātīgas apstrādes principu var pieprasīt, lai apstrīdētos datus bloķē (proti, lai liedz pieeju tiem). Tas nozīmē, ka datus nedzēš, bet pārzinim jāatturas no to izmantošanas, kamēr tie ir bloķēti. Tas ir jo īpaši nepieciešami, ja turpmāka neprecīzu vai nelikumīgi glabātu datu izmantošana var nodarīt kaitējumu datu subjektam. Valsts tiesību aktos jāparedz sīkāki noteikumi par to, kad var rasties pienākums bloķēt datu izmantošanu un kā tas jāīsteno.

Datu subjektiem vēl ir tiesības saņemt no pārziņa paziņojumu trešām personām par jebkuru bloķēšanu, labošanu vai dzēšanu, ja tās ir saņēmušas datus pirms šīm apstrādes darbībām. Tā kā pārzinim jādokumentē datu atklāšana trešām personām, jābūt iespējamam identificēt datu saņēmējus un pieprasīt dzēst datus. Ja dati tomēr starplaikā ir publicēti internetā, piemēram, tad var būt neiespējami panākt datu dzēšanu visās instancēs, jo datu saņēmēji nav atrodami. Atbilstoši datu aizsardzības direktīvai, sazināšanās ar datu saņēmējiem datu labošanai, dzēšanai vai bloķēšanai ir obligāta, „ja vien tas neizrādās neiespējami vai nav saistīts ar nesamērīgām pūlēm".[186]

5.1.2. Iebilduma tiesības

Iebilduma tiesībās ietilpst tiesības iebilst pret automatizētiem individuāliem lēmumiem, iebilduma tiesības datu subjekta īpašās situācijas dēļ un tiesības iebilst pret datu turpmāku apstrādi tiešās tirgvedības nolūkos.

Tiesības iebilst pret automatizētiem individuāliem lēmumiem

Automatizēti lēmumi ir lēmumi, kas pieņemti, izmantojot tikai ar automatizētiem līdzekļiem apstrādātus personas datus. Ja šādiem lēmumiem visdrīzāk būs ievērojama ietekme uz attiecināmo personu dzīvi, piemēram, uz to kredītspēju, darba izpildi, uzvedību vai uzticamību, vajag īpašu aizsardzību, lai novērstu nepienācīgas sekas. Datu aizsardzības direktīvā ir paredzēts, ka automatizēti lēmumi nedrīkst

186 Datu aizsardzības direktīva, 12. panta c) punkta pēdējā teikuma otrā puse.

noteikt personām svarīgus jautājumus, un ir izvirzīta prasība, ka personām jābūt tiesībām uz automatizētu lēmumu pārskatīšanu.[187]

Piemērs: Svarīgs praktisks automatizētās lēmumu pieņemšanas piemērs ir kredītspējas novērtēšana. Lai ātri nolemtu par nākamā klienta kredītspēju, no klienta savāc noteiktus datus, piemēram, par profesionālo un ģimenes stāvokli, un apvieno ar datiem par subjektu, kas pieejami no citiem avotiem, piemēram, no kredītinformācijas sistēmām. Šos datus automātiski ievada novērtēšanas algoritmā, kas aprēķina kopējo vērtību, kura raksturo potenciālā klienta kredītspēju. Tādējādi uzņēmuma darbinieks var dažu sekunžu laikā nolemt, vai datu subjekts ir pieņemams kā klients vai nē.

Tomēr saskaņā ar direktīvu dalībvalstis paredz, ka uz personu var attiecināt automatizētu individuālu lēmumu, ja datu subjekta intereses netiek skartas, jo lēmums bija datu subjektam labvēlīgs, vai arī tās tiek garantētas ar citiem atbilstošiem līdzekļiem.[188] Tiesības iebilst pret automatizētiem lēmumiem ir raksturīgas arī **EP tiesību aktiem**, kā var redzēt Ieteikumā par profilēšanu.[189]

Iebilduma tiesības datu subjekta īpašās situācijas dēļ

Datu subjektiem nav vispārīgu tiesību iebilst pret savu datu apstrādi.[190] Datu aizsardzības direktīvas 14. panta a) punktā tomēr datu subjektam ir dotas pilnvaras uz viņa konkrēto situāciju attiecināmu nenoraidāmu likumīgu iemeslu dēļ iebilst pret datu apstrādi, kas attiecas uz viņu. Līdzīgas tiesības ir atzītas EP Ieteikumā par profilēšanu.[191] Šādu noteikumu mērķis ir datu subjekta datu apstrādē atrast pareizo līdzsvaru starp datu subjekta datu aizsardzības tiesībām un citu likumīgām tiesībām.

Piemērs: Banka septiņus gadus glabā datus par saviem klientiem, kuri laikā neatmaksā kredīta maksājumus. Klients, kura dati tiek glabāti datu bāzē, piesakās uz citu aizdevumu. Tiek apskatīta datu bāze, tiek sniegts finansiālā stāvokļa

187 Turpat, 15. panta 1. punkts.

188 Turpat, 15. panta 2. punkts.

189 Ieteikums par profilēšanu, 5. panta 5. punkts.

190 Sk. arī ECT 1997. gada 27. augusta spriedumu lietā *M.S. pret Zviedriju*, prasības pieteikums Nr. 20837/92, kur medicīniskie dati tika paziņoti bez piekrišanas vai iespējas iebilst; vai ECT 1987. gada 26. marta spriedumu lietā *Leander pret Zviedriju*, prasības pieteikums Nr. 9248/81; vai ECT 2011. gada 10. maija spriedumu lietā *Mosley pret Apvienoto Karalisti*, prasības pieteikums Nr. 48009/08.

191 Ieteikums par profilēšanu, 5. panta 3. punkts.

novērtējums, un klientam aizdevumu atsaka. Klients tomēr var iebilst pret to, ka viņa datus reģistrē datu bāzē, un lūgt dzēst savus datus, ja viņš vai viņa var pierādīt, ka nesamaksātais maksājums bija vienkārši kļūdas rezultāts, kas tika novērsts, tiklīdz klients par to uzzināja.

Sekmīga iebilduma sekas ir tādas, ka pārzinis vairs nedrīkst apstrādāt konkrētos datus. Tomēr apstrādes darbības, kas veiktas ar datu subjekta datiem pirms iebilduma, paliek likumīgas.

Tiesības iebilst pret datu turpmāku izmantošanu tiešās tirgvedības nolūkos

Datu aizsardzības direktīvas 14. panta b) punktā ir paredzētas konkrētas tiesības iebilst pret personas datu izmantošanu tiešas tirgvedības nolūkiem. Šādas tiesības ir noteiktas arī EP Ieteikumā par tiešo tirdzniecību [tirgvedību].[192] Šo iebilduma veidu ir paredzēts izvirzīt pirms datus padara pieejamus trešām personām tiešās tirgvedības nolūkā. Tāpēc ir jādod datu subjektam iespēja iebilst pirms datu nodošanas.

5.2. Neatkarīga uzraudzība

Galvenie punkti

- Lai nodrošinātu efektīvu datu aizsardzību, saskaņā ar valsts tiesību aktiem jāizveido neatkarīgas uzraudzības iestādes.
- Valsts uzraudzības iestādēm jārīkojas pilnīgi neatkarīgi, kas jāgarantē ar dibināšanas tiesību aktu un jāatspoguļo konkrētajā uzraudzības iestādes organizatoriskajā struktūrā.
- Uzraudzības iestādēm ir šādi īpaši uzdevumi, citu starpā:
  - pārraudzīt un veicināt datu aizsardzību valsts mērogā;
  - dot padomus datu subjektiem un pārziņiem, kā arī valdībai un plašai sabiedrībai;
  - uzklausīt sūdzības un palīdzēt datu subjektam, ja ir domājami datu aizsardzības tiesību aizskārumi;
  - uzraudzīt pārziņus un personas datu operatorus;

192 EP, Ministru komiteja (1985), Ieteikums Rec(85)20 dalībvalstīm par personas datu aizsardzību, ko izmanto tiešās tirdzniecības [tirgvedības] nolūkos, 1985, gada 25. oktobrī, 4. panta 1. punkts.

- iejaukties, ja nepieciešams,
  - izsakot piezīmes vai brīdinājumus, vai pat nosakot sodu pārziņiem un personas datu operatoriem,
  - izdodot rīkojumu labot, bloķēt vai dzēst datus,
  - nosakot apstrādes aizliegumu;
- celt prasības tiesā.

Datu aizsardzības direktīvā ir prasīta neatkarīga uzraudzība kā svarīgs mehānisms, lai nodrošinātu efektīvu datu aizsardzību. Direktīva ieviesa datu aizsardzības piespiedu izpildes instrumentu, kura agrāk nebija ne 108. konvencijā, ne ESAO Privātuma vadlīnijās.

Tā kā ir pierādījies, ka neatkarīga uzraudzība ir nepieciešama efektīvas datu aizsardzības attīstībai, jauns noteikums pārskatītajās ESAO Privātuma vadlīnijās, ko pieņēma 2013. gadā, aicina dalībvalstis „izveidot un uzturēt privātuma piespiedu izpildes iestādes ar pārvaldību, resursiem un tehnisko kompetenci, kas tām vajadzīgi pilnvaru efektīvai īstenošanai un objektīvai, neitrālai un konsekventai lēmumu pieņemšanai."[193]

Saskaņā ar EP tiesību aktiem, 108. konvencijas papildprotokolā uzraudzības iestāžu izveide ir paredzēta kā obligāts pasākums. Šā instrumenta 1. pantā ir iekļauts neatkarīgu uzraudzības iestāžu tiesiskais regulējums, kas Līgumslēdzējām Pusēm jāīsteno savos valsts tiesību aktos. Protokolā šādu iestāžu uzdevumu un pilnvaru aprakstam ir izmantoti līdzīgi formulējumi, kā izmantots datu aizsardzības direktīvā. Līdz ar to principā uzraudzības iestādēm gan saskaņā ar ES, gan EP tiesību aktiem ir jādarbojas vienādi.

Saskaņā ar ES tiesību aktiem uzraudzības iestāžu kompetences un organizatoriskā struktūra pirmoreiz tika izklāstītas datu aizsardzības direktīvas 28. panta 1. punktā. Regulā par aizsardzību attiecībā uz personas datu apstrādi ES iestādēs[194] ir noteikts, ka EDAU ir uzraudzības iestāde, kura uzrauga, kā datus apstrādā ES struktūras un

193 ESAO (2013), Pamatnostādnes, kas regulē privātās dzīves aizsardzību un personas datu pārrobežu plūsmas, 19. panta c) punkts.

194 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, 41.–48. pants.

iestādes. Izklāstot uzraudzības iestādes nozīmi un pienākumus, šī regula izmanto pieredzi, kas gūta kopš datu aizsardzības direktīvas izsludināšanas.

Datu aizsardzības iestāžu neatkarība ir garantēta LESD 16. panta 2. punktā un Hartas 8. panta 3. punktā. Šajā pēdējā noteikumā jo īpaši neatkarīgas iestādes veikta kontrole tiek aplūkota kā būtisks pamattiesību uz datu aizsardzību elements. Vēl datu aizsardzības direktīvā ir prasīts, lai dalībvalstis izveidotu direktīvas piemērošanas uzraudzības iestādes, kuras darbotos pilnīgi neatkarīgi.[195] Taču ne tikai tiesību aktā, uz kura pamata tiek izveidota uzraudzības iestāde, ir jābūt noteikumiem, kuri īpaši garantē neatkarību, – arī iestādes konkrētajai organizatoriskajai struktūrai ir jāpierāda neatkarība.

2010. gadā Tiesa pirmoreiz saskārās ar jautājumu par prasības par datu aizsardzības uzraudzības iestāžu neatkarību tvērumu.[196] Nākamais piemērs ilustrē tās domu gājienu.

Piemērs: Lietā *Komisija pret Vāciju*[197] Eiropas Komisija bija lūgusi Tiesu paziņot, ka Vācija ir kļūdaini transponējusi prasību par uzraudzības iestāžu, kas atbild par datu aizsardzības nodrošināšanu, „pilnīgu neatkarību" un tādējādi neizpildīja savu pienākumu saskaņā ar datu aizsardzības direktīvas 28. panta 1. punktu. Pēc Komisijas domām, problēma bija tā, ka Vācija dažādās federālajās zemēs (*Länder*) bija pakļāvusi valsts pārraudzībai kompetentās iestādes, kas uzrauga personu datu apstrādi privātajā sektorā.

Vērtējums par to, cik pamatota ir izskatāmā prasība, pēc Tiesas domām, bija atkarīgs no minētajā normā ietvertās prasības par neatkarību apjomu un attiecīgi – no šīs normas interpretācijas.

Tiesa uzsvēra, ka vārdi „pilnīgi neatkarīgi" direktīvas 28. panta 1. punktā ir jāinterpretē, pamatojoties uz minētās normas faktisko formulējumu un uz datu aizsardzības direktīvas mērķiem un sistēmu.[198] Tiesa uzsvēra, ka uzraudzības

195 Datu aizsardzības direktīva, 28. panta 1. punkta pēdējais teikums; 108. konvencija, papildprotokols, 1. panta 3. punkts.

196 Sk. *FRA* [2010. gadā pieņemto] dokumentu *Pamattiesības: izaicinājumi un sasniegumi 2010. gadā*, 2010. gada ziņojums, 59. lpp. *FRA* sīkāk risina šo jautājumu savā ziņojumā par *Datu aizsardzību Eiropas Savienībā: valsts datu aizsardzības iestāžu loma*, kas tika publicēts 2010. gada maijā.

197 Tiesas 2010. gada 9. marta spriedums lietā C-518/07 *Eiropas Komisija pret Vācijas Federatīvo Republiku*, 27. punkts.

198 Turpat, 17. un 29. punkts.

iestādes ir direktīvā nodrošināto ar personas datu apstrādi saistīto tiesību „garanti" un ka tāpēc to izveide dalībvalstīs „ir būtiska sastāvdaļa personu aizsardzībā attiecībā uz personas datu apstrādi".[199] Tiesa 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 valsts vai federālās zemes ietekmes, un nevis vienīgi no to uzraugāmo struktūru ietekmes".[200]

Tiesa arī konstatēja, ka „pilnīgas neatkarības" nozīme ir jāinterpretē, ņemot vērā EDAU neatkarību, kā tā definēta Regulā par aizsardzību attiecībā uz personas datu apstrādi ES iestādēs. Kā uzsvērusi Tiesa, minētās regulas 44. panta 2. punktā „ir izskaidrots šis neatkarības jēdziens, piebilstot, ka, veicot savus pienākumus, EDAU ne no viena nesaņem un negaida norādījumus". Tas izslēdz valsts pārraudzības iespēju pār neatkarīgu datu aizsardzības uzraudzības iestādi.[201]

Attiecīgi Tiesa uzskatīja, ka Vācijas datu aizsardzības iestādes federatīvās valsts mērogā, kas atbild par privātu struktūru veiktu personas datu apstrādes pārraudzību, nebija pietiekami neatkarīgas, jo bija pakļautas valsts pārraudzībai.

Piemērs: Lietā *Eiropas Komisija pret Austriju*[202] Tiesa uzsvēra līdzīgas problēmas saistībā ar dažu Austrijas Datu aizsardzības iestādes (Datu aizsardzības komisija, *DSK*) locekļu un personāla statusu. Tiesa šajā lietā secināja, ka Austrijas tiesību akti liedza Austrijas Datu aizsardzības iestādei īstenot savas funkcijas pilnīgi neatkarīgi datu aizsardzības direktīvas nozīmē. Austrijas DAĪ neatkarība nebija pietiekami nodrošināta, jo Federālā kanceleja nodrošina *DSK* savu darbaspēku, pārrauga *DSK*, un tai ir tiesības vienmēr būt informētai par tās darbu.

Piemērs: Lietā *Eiropas Komisija pret Ungāriju*, Tiesa norādīja, ka "prasība ... nodrošināt, lai katra uzraudzības iestāde tam uzticēto pienākumu izpildē darbotos pilnīgi neatkarīgi, nozīmē attiecīgajai dalībvalstij pienākumu ievērot šādas iestādes pilnvaru termiņa ilgumu līdz tās sākotnēji paredzētā pilnvaru termiņa beigām". Tiesa papildus konstatēja, ka priekšlaicīgi izbeidzot personas datu

199 Turpat, 23. punkts.

200 Turpat, 25. punkts.

201 Turpat, 27. punkts.

202 Tiesas 2012. gada 16. oktobra spriedums lietā C-614/10 *Eiropas Komisija pret Austrijas Republika*, 59. un 63. punkts.

> aizsardzības uzraudzības iestādes pilnvaru termiņu, Ungārija nav izpildījusi tai Direktīvas 95/46/EK uzliktos pienākumus ..."

Uzraudzības iestādēm saskaņā ar valsts tiesību aktiem ir, citu starpā, šādas pilnvaras un spējas:[203]

- dot pārziņiem un datu subjektiem padomus par visiem datu aizsardzības jautājumiem;
- izmeklēt apstrādes darbības un attiecīgi iejaukties;
- izteikt pārzinim piezīmes vai brīdinājumus;
- izdot rīkojumu par datu labošanu, bloķēšanu, dzēšanu vai iznīcināšanu;
- noteikt apstrādei pagaidu vai galīgu aizliegumu;
- celt prasības tiesā.

Lai spētu pildīt savas funkcijas, uzraudzības iestādei jābūt piekļuvei visiem personas datiem un informācijai, kas vajadzīga izmeklēšanai, kā arī piekļuvei visām telpām, kurās pārzinis tur būtisku informāciju.

Ir ievērojamas atšķirības starp valstu jurisdikcijām attiecībā uz uzraudzības iestādes konstatējumu procedūrām un juridisko iedarbību. Tās var būt diapazonā no ombuda veida ieteikumiem līdz tūlīt izpildāmiem lēmumiem. Tāpēc, analizējot kādā jurisdikcijā pieejamo tiesiskās aizsardzības līdzekļu efektivitāti, šajā saistībā ir jāspriež par tiesiskās aizsardzības instrumentiem.

203 Datu aizsardzības direktīva, 28. pants; vēl sk. Konvenciju Nr. 108, papildprotokola 1. pantu.

5.3. Tiesiskās aizsardzības līdzekļi un sankcijas

Galvenie punkti

- Atbilstoši 108. konvencijai, kā arī datu aizsardzības direktīvai valsts tiesību aktos ir jāizklāsta pienācīgi tiesiskās aizsardzības līdzekļi un sankcijas pret tiesību uz datu aizsardzību aizskārumu.
  - Tiesības uz efektīvu tiesiskās aizsardzības līdzekli saskaņā ar ES tiesību aktiem prasa, lai valsts tiesību aktos būtu noteikti tiesiskās aizsardzības līdzekļi pret datu aizsardzības tiesību aizskārumiem, neatkarīgi no iespējas vērsties uzraudzības iestādē.
  - Valsts tiesību aktos ir jāparedz sankcijas, kas būtu efektīvas, līdzvērtīgas, samērīgas un preventīvas.
- Pirms prasības celšanas tiesu instancēs vispirms ir jāvēršas pie pārziņa. Noteikt to, vai pirms prasības celšanas tiesā ir vai nav jāvēršas arī pie uzraudzības iestādes, tiek atstāts valsts tiesību aktu ziņā.
- Kā pēdējā instancē un noteiktos apstākļos datu subjekti var celt prasību par datu aizsardzības tiesību aktu pārkāpumiem Eiropas Cilvēktiesību tiesā.
- Vēl datu subjekti var vērsties Tiesā, bet tikai ļoti ierobežotā mērā.

Tiesības atbilstoši datu aizsardzības tiesību aktiem var īstenot tikai tā persona, kuras tiesības tiek skartas; tas būs kāds, kurš ir – vai vismaz apgalvo, ka ir – datu subjekts. Šādu personu tās tiesību īstenošanā var pārstāvēt personas, kuras atbilstoši valsts tiesību aktiem atbilst vajadzīgajām prasībām. Nepilngadīgos obligāti pārstāv viņu vecāki vai aizbildņi. Uzraudzības iestādēs personu var pārstāvēt arī asociācijas, kuru likumīgais mērķis ir veicināt datu aizsardzības tiesības.

5.3.1. Pieprasījumi pārzinim

3.2. iedaļā minētās tiesības vispirms ir jāīsteno attiecībā pret pārzini. Tieša vēršanās valsts uzraudzības iestādē vai tiesā nedos rezultātu, jo iestāde var tikai ieteikt vispirms vērsties pie pārziņa, un Tiesa atzīs prasību par nepieņemamu. Formālās prasības, kā iesniegt pārzinim juridiski derīgu pieprasījumu, jo īpaši tas, vai tam ir jābūt rakstiskam pieprasījumam vai nē, ir jāregulē valsts tiesību aktos.

Vienībai, pie kuras vērsās kā pie pārziņa, ir jāreaģē uz pieprasījumu, pat ja šī vienība nav pārzinis. Atbilde datu subjektam katrā ziņā ir jāsniedz valsts tiesību aktos noteiktajā termiņā, pat ja atbild tikai to, ka dati par pieprasījuma iesniedzēju netiek apstrādāti. Saskaņā ar datu aizsardzības direktīvas 12. panta a) punktu un 108. konvencijas 8. panta b) punktu pieprasījums ir jāapstrādā „bez pārmērīgas vilcināšanās". Tāpēc valsts tiesību aktos ir jāparedz atbildes sniegšanas periods, kas ir pietiekami īss, bet tomēr dod pārzinim iespēju pienācīgi apstrādāt pieprasījumu.

Pirms atbildēt uz pieprasījumu, vienībai, pie kuras ir vērsušies kā pie pārziņa, ir jānosaka pieprasījuma iesniedzēja identitāte, lai noteiktu, vai viņš vai viņa patiešām ir persona, par kuru uzdodas, un tādējādi novērstu smagu konfidencialitātes pārkāpumu. Ja valsts tiesību aktos nav īpaši regulētas prasības par identitātes noteikšanu, tas jānolemj pārzinim. Godprātīgas apstrādes princips tomēr prasa, lai pārziņi nenoteiktu pārmērīgi apgrūtinošus nosacījumus identifikācijas (un pieprasījuma autentiskuma, kā apspriests 2.1.1 iedaļā) atzīšanai.

Valsts tiesību aktos ir jāskata arī jautājums par to, vai pārziņi pirms atbildes sniegšanas uz pieprasījumiem var vai nevar pieprasīt pieprasījuma iesniedzējiem samaksu: direktīvas 12. panta a) punktā un 108. konvencijas 8. panta b) punktā ir paredzēts, ka atbilde uz piekļuves pieprasījumiem ir jāsniedz „bez pārmērīgas [...] izdevumiem". Daudzās Eiropas valstīs valsts tiesību akti paredz, ka uz pieprasījumiem atbilstoši datu aizsardzības tiesību aktiem ir jāatbild bez maksas, kamēr vien atbilde nerada pārmērīgas un neparastas pūles; savukārt pārziņus valsts tiesību akti parasti aizsargā pret tiesību saņemt atbildi uz pieprasījumiem ļaunprātīgu izmantošanu.

Ja persona, iestāde vai struktūra, pie kuras vēršas kā pie pārziņa, nenoliedz, ka ir pārzinis, tad šai vienībai valsts tiesību aktos paredzētajā termiņā ir:

- vai nu jāizpilda pieprasījums un jāpaziņo pieprasījuma iesniedzējai personai, kā tās pieprasījums tika izpildīts; vai

- jāinformē pieprasījuma iesniedzējs, kāpēc viņa vai viņas pieprasījums netiks izpildīts.

5.3.2. Uzraudzības iestādei iesniegtās prasības

Ja persona, kura ir iesniegusi piekļuves pieprasījumu vai izvirzījusi iebildumu pārzinim, nesaņem savlaicīgu un apmierinošu atbildi, šī persona var vērsties valsts datu aizsardzības uzraudzības iestādē ar palīdzības lūgumu. Procedūras laikā uzraudzības

iestādē ir jānoskaidro, vai personai, iestādei vai struktūrai, pie kuras vērsās pieprasījuma iesniedzējs, bija vai nebija pienākums atbildēt uz to, un vai atbilde bija vai nebija pareiza un pietiekama. Uzraudzības iestādei jāinformē attiecīgā persona par procedūras, kurā izskata sūdzību, iznākumu.[204] Valsts uzraudzības iestāžu procedūras rezultāta juridiskā ietekme ir atkarīga no valsts tiesību aktiem: vai iestādes lēmumus var juridiski izpildīt, proti, ka tos var piespiedu kārtā izpildīt oficiāla iestāde, vai varbūt ir nepieciešams iesniegt apelācijas sūdzību tiesā, ja pārzinis neievēro uzraudzības iestādes lēmumus (atzinumu, brīdinājumu utt.).

Ja ES iestādes vai struktūras domājami pārkāpj datu aizsardzības tiesības, kas garantētas LESD 16. pantā, datu subjekts var iesniegt sūdzību EDAU,[205] neatkarīgajai datu aizsardzības uzraudzības iestādei, saskaņā ar Regulu par aizsardzību attiecībā uz personas datu apstrādi ES iestādēs, kurā ir noteiktas EDAU saistības un pilnvaras. Ja EDAU nereaģē sešu mēnešu laikā, sūdzību uzskata par noraidītu.

Jābūt iespējai vērsties tiesās ar apelācijas sūdzībām pret valsts uzraudzības iestādes lēmumiem. Tas attiecas kā uz datu subjektu, tā uz pārziņiem, kuri ir bijuši lietas dalībnieki tiesvedībā uzraudzības iestādē.

Piemērs: Apvienotās Karalistes informācijas komisārs 2013. gada 24. jūlijā izdeva lēmumu, ar kuru prasīja Hertfordšīras policijai pārtraukt izmantot transportlīdzekļu numura zīmju izsekošanas sistēmu, ko viņš uzskatīja par nelikumīgu. Kameru ievāktie dati tika uzglabāti gan vietējās policijas spēku datu bāzēs, gan centralizētā datu bāzē. Numura zīmju fotogrāfijas tika uzglabātas divus gadus, un mašīnu fotogrāfijas – 90 dienas. Tika uzskatīts, ka tik plaša kameru un citu uzraudzības līdzekļu izmantošana nebija samērīga problēmai, ko tādējādi centās atrisināt.

5.3.3. Tiesā iesniegtas prasības

Atbilstoši datu aizsardzības direktīvai, ja persona, kas ir iesniegusi pārzinim lūgumu saskaņā ar datu aizsardzības tiesību aktiem, nav apmierināta ar pārziņa atbildi, šai personai ir jābūt tiesībām iesniegt prasību valsts tiesā.[206]

204 Datu aizsardzības direktīva, 28. panta 4. punkts.

205 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.

206 Datu aizsardzības direktīva, 22. pants.

Tas, vai pirms prasības celšanas tiesā ir vai nav obligāti vispirms vērsties pie uzraudzības iestādes, tiek atstāts valsts tiesību aktu regulējuma ziņā. Tomēr vairākumā gadījumu personām, kuras īsteno savas datu aizsardzības tiesības, būs izdevīgāk vispirms vērsties uzraudzības iestādē, jo procedūrām saistībā ar palīdzības lūgumiem ir jābūt nebirokrātiskām un bezmaksas. Arī uzraudzības iestādes lēmumā (atzinumā, brīdinājumā utt.) dokumentētā kompetence var palīdzēt datu subjektam aizstāvēt savas tiesības tiesu instancēs.

Saskaņā ar EP tiesību aktiem par datu aizsardzības tiesību pārkāpumiem, kas domājami izdarīti ECK Līgumslēdzējas Puses valsts līmenī un vienlaikus ir ECK 8. panta prasību pārkāpums, var papildus celt prasību Eiropas Cilvēktiesību tiesā pēc tam, kad ir izsmelti visi pieejamie valsts tiesiskās aizsardzības līdzekļi. Prasības celšanai ECT par ECK 8. panta prasību pārkāpumu ir jāatbilst arī citiem pieņemamības kritērijiem (ECK 34.–37. pants).[207]

Lai gan prasības ECT var celt tikai pret Līgumslēdzējām Pusēm, tās var netieši būt arī par privātu personu rīcību vai bezdarbību, tiktāl, ciktāl Līgumslēdzēja Puse nav izpildījusi savus pozitīvos pienākumus atbilstoši ECK un nav savas valsts tiesību aktos nodrošinājusi pietiekamu aizsardzību pret datu aizsardzības tiesību pārkāpumiem.

Piemērs: Lietā *K.U. pret Somiju*[208] prasītājs, nepilngadīga persona, apgalvoja, ka interneta iepazīšanās vietnē par viņu bija ielikta seksuālas dabas reklāma. Informāciju ielikušās personas identitāti interneta pakalpojumu sniedzējs neatklāja, ievērojot konfidencialitātes pienākumu saskaņā ar Somijas tiesību aktiem. Prasītājs apgalvoja, ka Somijas tiesību akti nesniedza pietiekamu aizsardzību pret tādām privātu personu darbībām, kuras ievietoja internetā inkriminējošus datus par prasītāju. ECT uzskatīja, ka valstīm ir ne tikai pienākums atturēties no patvaļīgas iejaukšanās personu privātajā dzīvē, bet tām var arī būt pozitīvi pienākumi, kas ietver „pasākumu pieņemšanu, kuru mērķis ir nodrošināt privātās dzīves neaizskaramību pat pašu personu savstarpējo attiecību jomā". Prasītāja gadījumā viņa praktiskai un efektīvai aizsardzībai bija vajadzīgs veikt iedarbīgus pasākumus, lai identificētu un apsūdzētu vainīgo. Tomēr valsts nebija piešķīrusi minēto aizsardzību, un Tiesa secināja, ka ir bijis ECK 8. panta prasību pārkāpums.

207 ECK, 34.–37. pants, pieejams: www.ECK.EP.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

208 ECT 2009. gada 2. marta spriedums lietā *K.U. pret Somiju*, prasības pieteikums Nr. 2872/02.

Piemērs: Lietā *Köpke pret Vāciju*[209] prasītāja bija turēta aizdomās par zādzību darbavietā un tāpēc pakļauta slepenai videonovērošanai. ECT secināja, ka nebija „nekā, kas liecinātu, ka valsts iestādes nebija nodrošinājušas atbilstošu līdzsvaru, savas rīcības brīvības robežās, starp prasītājas tiesībām uz viņas privātās dzīves neaizskaramību atbilstīgi 8. pantam un gan viņas darba devēja interesi aizsargāt savas īpašumtiesības, gan sabiedrības interesi, lai būtu pienācīga tieslietu pārvaldība". Tāpēc prasību atzina par nepieņemamu.

Ja ECT konstatē, ka kāda Valsts–Līgumslēdzēja Puse ir pārkāpusi kādas no ECK aizsargātajām tiesībām, Valstij–Līgumslēdzējai Pusei ir jāizpilda ECT spriedums. Izpildes pasākumiem ir visupirms jāpārtrauc pārkāpums un pēc iespējas jāmazina tā negatīvās sekas prasītājam. Spriedumu izpilde var arī prasīt vispārīgus pasākumus, lai novērstu Tiesas konstatētajiem līdzīgus pārkāpumus, – šie pasākumi var izpausties vai nu kā izmaiņas tiesību aktos, praksē vai citos pasākumos.

Ja ECT konstatē ECK pārkāpumu, ECK 41. pantā ir paredzēts, ka Tiesa cietušajai pusei [prasītājam] var piešķirt tikai taisnīgu kompensāciju, ko apmaksā Valsts–Līgumslēdzēja Puse.

Saskaņā ar ES tiesību aktiem[210] cietušie no tādu valsts datu aizsardzības tiesību aktu pārkāpumiem, ar kuriem īsteno ES datu aizsardzības tiesību aktus, dažkārt var celt prasību Tiesā. Ir divi iespējami scenāriji tam, kā datu subjekta apgalvojums par viņa vai viņas datu aizsardzības tiesību pārkāpumu var izraisīt tiesvedību Tiesā.

Pirmajā scenārijā datu subjektam jābūt tiešajam cietušajam no ES administratīvā vai reglamentējošā akta, kas pārkāpj personas tiesības uz datu aizsardzību. Atbilstoši LESD 263. panta ceturtajai daļai:

> *„jebkura fiziska vai juridiska persona [...] var celt prasību par tiesību aktu, kas adresēts šai personai, vai kas viņu skar tieši un individuāli, un par reglamentējošu aktu, kas viņu skar tieši, bet nav saistīts ar īstenošanas pasākumiem."*

Tādējādi cietušie no nelikumīgas savu datu apstrādes, ko veikusi kāda ES struktūra, var tieši vērsties Vispārējā tiesā, kas ir Tiesas iestāde ar kompetenci pieņemt

209 ECT 2010. gada 5. oktobra spriedums lietā *Köpke pret Vāciju* (dec.), prasības pieteikums Nr. 420/07.

210 ES (2007), Lisabonas Līgums, ar ko groza Līgumu par Eiropas Savienību un Līgumu par Eiropas Kopienas izveidi, parakstīts Lisaboā 2007. gada 13. decembrī, OV 2007 C 306. Sk. arī Līguma par Eiropas Savienību, OV 2012 C 326 un LESD, OV 2012 C 326, konsolidētās versijas.

spriedumus Regulas par aizsardzību attiecībā uz personas datu apstrādi ES iestādēs jautājumos. Iespēja tieši vērsties Tiesā pastāv arī tad, ja personas juridisko stāvokli tieši ietekmē kāds ES tiesību noteikums.

Otrais scenārijs skar Tiesas kompetenci sniegt prejudiciālus nolēmumus atbilstoši LESD 267. pantam.

Datu subjekti var lūgt savas valsts tiesai, lai tā lūdz Tiesai paskaidrojumus par ES Līgumu interpretāciju un par ES iestāžu, struktūru, biroju vai aģentūru tiesību aktu interpretāciju un spēkā esamību. Šādus paskaidrojumus dēvē par prejudiciāliem nolēmumiem. Tas nav tiešs prasītāja tiesiskās aizsardzības līdzeklis, bet dod iespēju valstu tiesām nodrošināt, ka tās piemēro ES tiesību aktu pareizo interpretāciju.

Ja kāds no lietas dalībniekiem valsts tiesā prasa uzdot Tiesai prejudiciālu jautājumu, pienākums izpildīt šo prasību ir tikai valstu pēdējās instances tiesām, pret kuru spriedumiem nav tiesiskās aizsardzības līdzekļu.

Piemērs: Lietā *Kärntner Landesregierung un citi*[211] Austrijas Konstitucionālā tiesa uzdeva Tiesai jautājumus par Direktīvas 2006/24/EK (*Datu saglabāšanas direktīvas*) 3.–9. panta spēkā esamību, ņemot vērā Hartas 7., 9. un 11. pantu, un par to, vai zināmi Austrijas federatīvā likuma par telekomunikācijām, ar ko transponēja datu saglabāšanas direktīvu, bija vai nebija nesaderīgi ar datu aizsardzības direktīvas un Regulas par aizsardzību attiecībā uz personas datu apstrādi ES iestādēs aspektiem.

Seitlinger k–gs, viens no prasītājiem tiesvedībā Konstitucionālajā tiesā, apgalvoja, ka viņš izmanto telefonu, internetu un e-pastu gan darba nolūkiem, gan privātajā dzīvē. Līdz ar to informācija, ko viņš nosūta un saņem, tiek raidīta cauri publiskajiem telekomunikāciju tīkliem. Saskaņā ar Austrijas 2003. gada Telekomunikāciju likumu *Seitlinger* k–ga telekomunikāciju pakalpojumu sniedzējam ir izvirzīta juridiska prasība vākt un glabāt datus par to, kā viņš izmanto tīklu. *Seitlinger* k–gs saprata, ka šāda viņa personas datu vākšana un glabāšana nekādā veidā nebija nepieciešama informācijas nogādāšanas tīklā no punkta A līdz punktam B tehniskajiem nolūkiem. Šo datu vākšana un glabāšana absolūti nebija vajadzīga arī rēķinu izrakstīšanas nolūkiem. *Seitlinger* k–gs katrā ziņā nebija piekritis šādai savu personas datu izmantošanai. Vienīgais

211 Tiesas 2014. gada 8. aprīļa spriedums apvienotajās lietās C-293/12 un C-594/12 *Digital Rights Ireland pret Seitling un citiem*.

iemesls visu šo papildu datu vākšanai un glabāšanai bija Austrijas 2003. gada Telekomunikāciju likums.

Tāpēc *Seitlinger* k–gs cēla prasību Austrijas Konstitucionālajā tiesā, kurā apgalvoja, ka viņa telekomunikāciju pakalpojumu sniedzējam tiesību aktos noteiktie pienākumi pārkāpa viņa pamattiesības saskaņā ar ES Hartas 8. pantu.

Tiesa pieņem spriedumu tikai par tai iesniegtā lūguma sniegt prejudiciālu nolēmumu elementiem. Par sprieduma pieņemšanu pamata lietā paliek atbildīga valsts tiesa.

Principā Tiesai ir jāatbild uz tai uzdotajiem jautājumiem. Tā nevar atteikt sniegt prejudicālu nolēmumu uz tā pamata, ka šī atbilde nebūtu ne būtiska, ne savlaicīga attiecībā uz pamata lietu. Tā tomēr var noraidīt jautājumu, ja tas neietilpst tās kompetenču jomā.

Visbeidzot, ja ES iestāde vai struktūra personas datu apstrādes gaitā domājami pārkāpj LESD 16. pantā garantētās tiesības uz datu aizsardzību, datu subjekts var celt prasību Vispārējā tiesā (Regulas par aizsardzību attiecībā uz personas datu apstrādi ES iestādēs 32. panta 1. un 4. punkts). Tas pats attiecas uz EDAU lēmumiem par tādiem pārkāpumiem (Regulas par aizsardzību attiecībā uz personas datu apstrādi ES iestādēs 32. panta 3. punkts).

Kamēr Tiesas Vispārējā tiesa ir kompetenta pieņemt spriedumus Regulas par aizsardzību attiecībā uz personas datu apstrādi ES iestādēs jautājumos, ja tomēr tiesiskās aizsardzības līdzekli meklē kāda persona, kas ir ES iestāžu vai struktūru personāla loceklis, šai personai jāvēršas ES Civildienesta tiesā.

Piemērs: Lieta *Eiropas Komisija pret The Bavarian Lager Co. Ltd*[212] atspoguļo tiesiskās aizsardzības līdzekļus, kas ir pieejami pret ES iestāžu un struktūru darbībām vai lēmumiem saistībā ar datu aizsardzību.

Bavarian Lager prasīja Eiropas Komisijai piekļuvi pilnam sanāksmes, kas notika Komisijā un domājami attiecās uz uzņēmumam būtiskiem juridiskiem jautājumiem, protokolam. Komisija bija noraidījusi uzņēmējsabiedrības piekļuves

212 Tiesas 2010. gada 29. jūnija spriedums lietā C-28/08 P *Eiropas Komisija pret The Bavarian Lager Co. Ltd.*

pieprasījumu, pamatojoties uz svarīgākām datu aizsardzības interesēm.[213] Bavarian Lager, piemērojot Regulas par aizsardzību attiecībā uz personas datu apstrādi ES iestādēs 32. pantu, par šo lēmumu bija iesniegusi prasību Tiesā, precīzāk, Pirmās instances tiesā (Vispārējās tiesas priekštece). Savā lēmumā lietā T194/04 *Bavarian Lager pret Komisiju* Pirmās instances tiesa atcēla Komisijas lēmumu noraidīt piekļuves pieprasījumu. Eiropas Komisija iesniedza Tiesā apelācijas sūdzību par šo lēmumu. Tiesa (Lielajā palātā) pieņēma spriedumu, atceļot Pirmās instances tiesas spriedumu, un apstiprināja Eiropas Komisijas noraidījumu piekļuves pieprasījumam.

5.3.4. Sankcijas

Saskaņā ar EP tiesību aktiem 108. konvencijas 10. pantā ir paredzēts, ka katrai Pusei jānosaka piemērotas sankcijas un tiesiskās aizsardzības līdzekļi pret to valsts tiesību aktu noteikumu pārkāpumiem, kuri īsteno 108. konvencijā izklāstītos datu aizsardzības pamatprincipus.[214] Saskaņā ar ES tiesību aktiem, datu aizsardzības direktīvas 24. pantā ir noteikts, ka dalībvalstis „paredz atbilstošus pasākumus, lai nodrošinātu šīs direktīvas noteikumu ieviešanu pilnībā, un īpaši nosaka sankcijas, kas jāuzliek gadījumā, ja tiek pārkāpti [..] pieņemtie noteikumi [..]".

Abi instrumenti piešķir dalībvalstīm plašu rīcības brīvību piemērotu sankciju un tiesiskās aizsardzības līdzekļu izvēlē. Juridiskais instruments arī nedod īpašas vadlīnijas par piemērotu sankciju raksturu vai veidu, kā arī nesniedz sankciju piemērus.

Tomēr:

> *„lai gan ES dalībvalstīm ir rīcības brīvība, nosakot piemērotākos pasākumus to tiesību garantēšanai, ko personas gūst no ES tiesību aktiem saskaņā ar LES 4. panta 3. punktā noteikto lojālas sadarbības principu, ir jāievēro prasību minimums attiecībā uz efektivitāti, līdzvērtību, samērīgumu un preventīvo raksturu."*[215]

213 Šā argumenta analīzei skat.: EDAU (2011), *Publiska piekļuve dokumentiem, kuros ir personas dati pēc sprieduma pieņemšanas lietā Bavarian Lager*, Briselē, EDAU, pieejams šādā tīmekļa vietnē: www.secure.EDAU.europa.eu/EDAUWEB/webdav/site/mySite/shared/Documents/EDAU/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

214 ECT 2008. gada 17. jūlija spriedums lietā *I. pret Somiju*, prasības pieteikums Nr. 20511/03; ECT 2008. gada 2. decembra spriedums lietā *K.U. pret Somiju*, prasības pieteikums Nr. 2872/02.

215 *FRA* (2012), *Eiropas Savienības Pamattiesību aģentūras atzinums par ierosināto datu aizsardzības reformu paketi*, 2/2012, Vīne, 2012. gada 1. oktobrī, 27. lpp.

Tiesa ir atkārtoti apgalvojusi, ka valsts tiesību aktos nevar pilnīgi brīvi noteikt sankcijas.

> Piemērs: Lietā *Von Colson* un *Kamann pret Land Nordrhein-Westfalen*[216] Tiesa norādīja, ka visām dalībvalstīm, kurām direktīva ir adresēta, ir pienākums veikt savās valsts tiesību sistēmās visus pasākumus, lai nodrošinātu tās pilnu efektivitāti, saskaņā ar izvirzīto mērķi. Tiesa uzskatīja, ka, lai gan ir dalībvalstu ziņā izvēlēties veidus un līdzekļus, ar kuriem nodrošināt direktīvas īstenošanu, šī brīvība neskar tām noteikto pienākumu. It īpaši, efektīviem tiesiskās aizsardzības līdzekļiem ir jādod personai iespēja izvirzīt un piespiedu kārtā izmantot konkrētās tiesības pilnā apjomā pēc būtības. Lai sasniegtu tādu patiesu un efektīvu aizsardzību, tiesiskās aizsardzības līdzekļiem ir jārada pamats piemērot soda un/vai kompensācijas procedūras, kas paredz sankcijas ar preventīvu ietekmi.

Attiecībā uz sankcijām pret ES tiesību pārkāpumiem, ko izdara ES iestādes vai struktūras, īpašs Regulas par aizsardzību attiecībā uz personas datu apstrādi ES iestādēs noteikums paredz sankcijas tikai disciplinārsoda veidā. Atbilstoši regulas 49. pantam „[j]a Eiropas Kopienu ierēdnis vai cits darbinieks tīšām vai nolaidības dēļ neievēro šajā regulā paredzētos pienākumus, viņš [vai viņa] ir disciplināri atbildīgs[-a] [...]".

216 Tiesas 1984. gada 10. aprīļa spriedums lietā C-14/83 *Sabine von Kolson and Elisabeth Kamann pret Land Nordrhein-Westfalen*.

6

Pārrobežu datu plūsmas

ES	Aplūkotie jautājumi	EP
Pārrobežu datu plūsmas		
Datu aizsardzības direktīva, 25. panta 1. punkts Tiesas 2003. gada 6. novembra spriedums lietā C-101/01 *Bodil Lindqvist*	**Definīcija**	108. konvencija, papildprotokols, 2. panta 1. punkts
Brīva datu plūsma		
Datu aizsardzības direktīva, 1. panta 2. punkts	**ES dalībvalstu starpā**	
	108. konvencijas Līgumslēdzēju Pušu starpā	108. konvencija, 12. panta 2. punkts
Datu aizsardzības direktīva, 25. pants	**Uz trešām valstīm ar pienācīgu datu aizsardzības līmeni**	108. konvencija, papildprotokols, 2. panta 1. punkts
Datu aizsardzības direktīva, 26. panta 1. punkts	**Uz trešām valstīm īpašos gadījumos**	108. konvencija, papildprotokols, 2. panta 2. punkta a) apakšpunkts
Ierobežota datu plūsma uz trešām valstīm		
Datu aizsardzības direktīva, 26. panta 2. punkts Datu aizsardzības direktīva, 26. panta 4. punkts	**Līguma punkti**	108. konvencija, papildprotokols, 2. panta 2. punkta b) apakšpunkts Vadlīnijas līguma punktu sagatavošanai
Datu aizsardzības direktīva, 26. panta 2. punkts	**Saistošie korporatīvie noteikumi**	
Piemēri: ES–ASV PDR-Nolīgums ES–ASV SWIFT-Nolīgums	**Īpaši starptautiskie nolīgumi**	

Datu aizsardzības direktīva paredz ne tikai brīvu datu plūsmu starp dalībvalstīm, bet arī satur noteikumus par prasībām personas datu nodošanai trešām valstīm ārpus ES. EP arī atzina to, cik svarīgi ir īstenot normas attiecībā uz pārrobežu datu plūsmām uz trešām valstīm, un 2001. gadā pieņēma 108. konvencijas papildprotokolu. Šis protokols pārņēma galvenos regulējošos aspektus par pārrobežu datu plūsmām no Konvencijas Līgumslēdzējām Pusēm un ES dalībvalstīm.

6.1. Pārrobežu datu plūsmu raksturs

Galvenie punkti

- Pārrobežu datu plūsma ir personas datu nodošana saņēmējam, kurš vai kas ir pakļauts ārvalstu jurisdikcijai.

108. konvencijas papildprotokola 2. panta 1. punktā pārrobežu datu plūsma ir aprakstīta kā personas datu nodošana saņēmējam, kurš vai kas ir pakļauts ārvalstu jurisdikcijai. Datu aizsardzības direktīvas 25. panta 1. punktā tiek regulēta „personas datu, kuri atrodas apstrādē vai ir paredzēti apstrādei pēc pārsūtīšanas [nodošanas]", pārsūtīšana [nodošana] trešai valstij. Tāda datu nodošana ir atļauta tikai atbilstoši normām, kas noteiktas 108. konvencijas papildprotokola 2. pantā, un – ES dalībvalstīm – vēl arī datu aizsardzības direktīvas 25. un 26. pantā.

Piemērs: Lietā *Bodil Lindqvist*[217] Tiesa uzskatīja, ka „darbība, kuras ietvaros interneta mājas lapā 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 3. panta 1. punkta izpratnē".

Tad Tiesa norādīja, ka direktīvā ir arī paredzēti speciāli noteikumi, kuru mērķis ir nodrošināt dalībvalstu kontroli par personas datu pārsūtīšanu [nodošanu] trešaj]ām valstīm.

Tomēr, ņemot vērā, pirmkārt, interneta attīstības pakāpi izstrādes laikā un, otrkārt, to, ka tajā nav kritēriju par interneta lietošanas piemērošanu, „nevar

217 Tiesas 2003. gada 6. novembra spriedums lietā C-101/01 *Bodil Lindqvist*, 27., 68. un 69. punkts.

prezumēt, ka Kopienu likumdevējam būtu nolūks nākotnē jēdzienā „[datu] pārsūtīšana uz trešām valstīm" iekļaut datu ievietošanu interneta mājas lapā, [..], pat ja tādējādi šie dati ir padarīti pieejami trešo valstu personām, kuru rīcībā ir tehniskie līdzekļi, lai tiem piekļūtu".

Pretējā gadījumā, ja direktīva „tiktu interpretēta tādā nozīmē, ka katru reizi, kad personas dati tiek ievietoti interneta mājas lapā, notiek „datu pārsūtīšana uz treš[aj]ām valstīm", šai pārsūtīšanai noteikti būtu jābūt pārsūtīšanai uz visām treš[aj]ām valstīm, kurās pastāv nepieciešamie tehniskie līdzekļi, lai piekļūtu internetam. Tādējādi [direktīvā] paredzētā īpašā sistēma attiecībā uz darbībām internetā noteikti kļūtu par vispārpiemērojamu sistēmu. Tiklīdz kā Komisija [..] konstatētu, ka viena vienīga trešā valsts nenodrošina pienācīgu aizsardzības līmeni, dalībvalstīm būtu pienākums aizkavēt jebkādu personas datu ievietošanu internetā."

Princips, ka vienkārša (personas) datu publicēšana nav uzskatāma par pārrobežu datu plūsmu, attiecas arī uz publiskiem reģistriem tiešsaistē vai plašsaziņas līdzekļiem, piemēram, (elektroniskiem) laikrakstiem un televīziju. Tikai tā komunikācija, kas ir adresēta konkrētiem saņēmējiem, var atbilst „pārrobežu datu plūsmas" jēdzienam.

6.2. Brīvas datu plūsmas dalībvalstu vai Līgumslēdzēju Pušu starpā

Galvenie punkti

- Uz personas datu nodošanu citai Eiropas Ekonomikas zonas dalībvalstij vai citai 108. konvencijas Līgumslēdzējai Pusei ierobežojumi nedrīkst attiekties.

Atbilstoši 108. konvencijas 12. panta 2. punktam, **saskaņā ar EP tiesību aktiem** starp konvencijas līgumslēdzējām pusēm jābūt brīvai personas datu plūsmai. Valsts tiesību aktos nedrīkst ierobežot personas datu eksportu uz kādu līgumslēdzēju pusi, izņemot šādus gadījumus:

- to prasa datu īpašais raksturs;[218] vai

218 108. konvencija, 12. panta 3. punkta a) apakšpunkts.

- ierobežojums ir nepieciešams, lai novērstu, ka tiek apieti valsts juridiskie noteikumi par pārrobežu datu plūsmu pie trešām personām.[219]

Saskaņā ar ES tiesību aktiem ierobežot vai aizliegt brīvu datu plūsmu starp dalībvalstīm ir aizliegts ar datu aizsardzības direktīvas 1. panta 2. punktu. Ar Līgumu par Eiropas Ekonomikas zonu (EEZ)[220] brīvas datu plūsmas teritoriālais tvērums ir paplašināts, lai ietvertu iekšējā tirgū arī Islandi [Īslandi], Lihtenšteinu un Norvēģiju.

Piemērs: Ja kādas starptautiskas, vairākās ES dalībvalstīs – tostarp Slovēnijā un Francijā – reģistrētas uzņēmumu grupas filiāle nodod personas datus no Slovēnijas uz Franciju, Slovēnijas valsts tiesību akti nedrīkst ierobežot vai aizliegt šādu datu plūsmu.

Ja tomēr tā pati Slovēnijas filiāle vēlas nodot tos pašus personas datus mātes uzņēmumam Amerikas Savienotajās Valstīs, Slovēnijas datu eksportētājam ir jāizpilda procedūras, kas paredzētas Slovēnijas tiesību aktos attiecībā uz pārrobežu datu plūsmu uz trešām valstīm bez adekvātas datu aizsardzības, izņemot gadījumus, kad mātes uzņēmums ir pievienojies Droša patvēruma principiem – brīvprātīgam rīcības kodeksam par adekvāta datu aizsardzības līmeņa nodrošināšanu (sk. 6.3.1 iedaļu).

Pārrobežu datu plūsmas EEZ dalībvalstīm nolūkiem, kas neietilpst iekšējā tirgus jomā, piemēram, noziegumu izmeklēšanai, tomēr nav pakļautas datu aizsardzības direktīvas noteikumiem, un tāpēc uz tām neattiecas brīvas datu plūsmas princips. Kas attiecas uz EP tiesību aktiem, visas jomas ir ietvertas 108. konvencijas un 108. konvencijas papildprotokola darbības jomā, lai gan Līgumslēdzējas Puses var izdarīt izņēmumus. Visas EEZ dalībvalstis ir arī 108. konvencijas slēdzējas.

219 Turpat, 12. panta 3. punkta b) apakšpunkts.

220 Padomes un Komisijas 1993. gada 13. decembra Lēmums par Eiropas Ekonomiskās zonas līguma noslēgšanu starp Eiropas Kopienu, tās dalībvalstīm un Austrijas Republiku, Somijas Republiku, Islandes Republiku, Lihtenšteinas Grāfisti [Firstisti], Norvēģijas Karalisti, Zviedrijas Karalisti un Šveices Konfederāciju, OV 1994 L 1.

6.3. Brīvas datu plūsmas uz trešām valstīm

Galvenie punkti

- Uz personas datu nodošanu trešām valstīm neattiecas valsts datu aizsardzības tiesību aktos noteiktie ierobežojumi, ja:
  - ir noskaidrots, ka datu aizsardzība pie saņēmēja ir adekvāta; vai
  - tas ir nepieciešams īpašās datu subjekta interesēs vai citu prevalējošās likumīgās interesēs – jo īpaši svarīgās sabiedrības interesēs.
- Datu aizsardzības adekvātums trešā valstī nozīmē, ka šīs valsts tiesību aktos ir efektīvi īstenoti galvenie datu aizsardzības principi.
- Saskaņā ar ES tiesību aktiem datu aizsardzības adekvātumu trešā valstī novērtē Eiropas Komisija. Saskaņā ar EP tiesību aktiem adekvātuma novērtēšanas regulējums ir jānosaka valsts tiesību aktos.

6.3.1. Brīva datu plūsma adekvātas aizsardzības dēļ

Saskaņā ar **EP tiesību aktiem** valsts tiesību aktos drīkst paredzēt brīvu datu plūsmu uz valstīm, kas nav līgumslēdzējas, ja saņēmēja valsts vai organizācija nodrošina adekvātu aizsardzības līmeni plānotajai datu nodošanai.[221] Valsts tiesību aktos paredz, kā novērtēt datu aizsardzības līmeni kādā [konkrētā] ārvalstī un kam tas jādara.

Saskaņā ar ES tiesību aktiem brīva datu plūsma uz trešām valstīm ar adekvātu datu aizsardzības līmeni ir paredzēta datu aizsardzības direktīvas 25. panta 1. punktā. Drīzāk tieši adekvātuma prasība, nevis līdzvērtības prasība padara iespējamu ievērot dažādos datu aizsardzības īstenošanas veidus. Atbilstoši direktīvas 25. panta 6. punktam Eiropas Komisijas kompetencē ir novērtēt datu aizsardzības līmeni ārvalstīs, konstatējot adekvātumu un konsultējoties par novērtēšanu ar 29. panta darba grupu, kura ir devusi būtisku ieguldījumu 25. un 26. panta interpretācijā.[222]

221 108. konvencija, papildprotokols, 2. panta 1. punkts

222 Sk., piemēram, 29. panta darba grupa (2003), *Darba dokuments par personas datu pārsūtīšanu uz trešām valstīm: ES Datu aizsardzības direktīvas 26. panta 2. punkta piemērošana saistošiem uzņēmuma noteikumiem [saistošajiem korporatīvajiem noteikumiem] par starptautisku datu pārsūtīšanu [nodošanu]*, WP 74, Briselē, 2003. gada 3. jūnijs; un 29. panta darba grupa (2005), *Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta vienotu interpretāciju,* WP 114, Briselē, 2005. gada 25. novembrī.

Eiropas Komisijas veiktam adekvātuma konstatējumam ir saistoša iedarbība. Ja Eiropas Komisija publicē adekvātuma konstatējumu par noteiktu valsti Eiropas Savienības *Oficiālajā Vēstnesī*, visām EEZ dalībvalstīm un to struktūrām ir jāievēro šis lēmums, kas nozīmē, ka datu plūsma uz šo valsti var notikt, neveicot pārbaudes vai licencēšanas procedūras valsts iestādēs.[223]

Eiropas Komisija spēj arī novērtēt valsts tiesību sistēmas daļas vai aprobežoties ar atsevišķiem tematiem. Komisija izdarīja adekvātuma konstatējumu, piemēram, tikai attiecībā uz Kanādas privātās tirdzniecības tiesību aktiem.[224] Ir arī vairāki adekvātuma konstatējumi nodošanai, ko veic uz ES un ārvalstu nolīgumu pamata. Šie lēmumi attiecas tikai uz atsevišķu datu nodošanas veidu, piemēram, Pasažieru datu reģistru nodošanu, ko veic aviokompānijas, ārvalstu robežkontroles iestādēm, kad aviokompānija lido no ES uz noteiktiem aizokeāna galamērķiem (sk. 6.4.3 iedaļu). Nesenākā datu nodošanas praksē, pamatojoties uz īpašiem ES un trešo valstu nolīgumiem, parasti atsakās no vajadzības pēc adekvātuma konstatējumiem, pieņemot, ka nolīgums pats par sevi piedāvā adekvātu datu aizsardzības līmeni.[225]

Viens no svarīgākajiem adekvātuma lēmumiem faktiski neattiecas uz juridisko noteikumu kopumu.[226] Drīzāk tas attiecas uz normām, kā Rīcības kodekss, kas pazīstamas kā Droša patvēruma [privātuma] principi. Šos principus izstrādāja ES un Amerikas Savienoto Valstu starpā ASV uzņēmumiem. Dalību Drošā patvērumā panāk, deklarējot ASV Tirdzniecības departamentam brīvprātīgas saistības, ko dokumentē minētā departamenta publicētā sarakstā. Viens no svarīgiem adekvātuma elementiem ir datu aizsardzības īstenošanas efektivitāte. Droša patvēruma pasākumā ir paredzēts arī zināms apjoms valsts uzraudzības: Drošam patvērumam drīkst

223 Pastāvīgi atjauninātu valstu sarakstu, kas ir saņēmušas adekvātuma atzinumu, sk. Eiropas Komisijas Tieslietu Ģenerāldirektorāta mājaslapā, pieejams šādā tīmekļa vietnē: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

224 Eiropas Komisija (2002), [Komisijas] 2001. gada 20. decembra Lēmums 2002/2/EK par personas datu pienācīgu aizsardzību, kas noteikta Kanādas likumā par personas datu un elektronisko dokumentu aizsardzību, atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK, OV 2002 L 2.

225 Piemēram, Nolīgums starp Amerikas Savienotajām Valstīm un Eiropas Savienību par pasažieru datu reģistru lietošanu un pārsūtīšanu ASV Valsts drošības departamentam (OV 2012 L 215, 5.–14. lpp.) vai 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 8, 11.–16. lpp.

226 Eiropas Komisija (2000), Komisijas 2000. gada 26. jūlija Lēmums 2000/520/EK atbilstīgi 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, OV 2000 L 215.

pievienoties tikai tie uzņēmumi, kuri pakļaujas ASV Federālās tirdzniecības komisijas uzraudzībai.

6.3.2. Brīva datu plūsma īpašos gadījumos

Saskaņā ar EP tiesību aktiem 108. konvencijas papildprotokola 2. panta 2. punkts atļauj nodot personas datus trešām valstīm, ja nav adekvātas datu aizsardzības, kamēr vien nodošana ir paredzēta valsts tiesību aktos un ir nepieciešama:

- īpašām datu subjekta interesēm; vai
- likumīgi prevalējošām citu interesēm, jo īpaši svarīgām sabiedriskām interesēm.

Saskaņā ar ES tiesību aktiem datu aizsardzības direktīvas 26. panta 1. punktā ir ietverti noteikumi, kas ir līdzīgi 108. konvencijas papildprotokola noteikumiem.

Atbilstīgi direktīvai datu subjekta intereses var attaisnot brīvu datu plūsmu uz trešo valsti, ja:

- ir dota datu subjekta nepārprotama piekrišana datu eksportam; vai
- datu subjekts iestājas – vai grasās iestāties – līgumiskās attiecībās, kas skaidri prasa datu nodošanu saņēmējam ārzemēs; vai
- datu subjekta interesēs ir slēgts līgums starp datu pārzini un trešo personu; vai
- nodošana ir vajadzīga, lai aizsargātu būtiskas datu subjekta intereses;
- no publiskiem reģistriem izgūtu datu nodošanai; šis ir piemērs, kad sabiedrības vispārējās prevalējošās interesēs ir piekļūt publiskos reģistros uzglabātai informācijai.

Citu likumīgas intereses var attaisnot brīvu datu pārrobežu plūsmu:[227]

- svarīgu publisku interešu vārdā, kas nav valsts vai sabiedriskās drošības jautājumi, jo uz tiem neattiecas datu aizsardzības direktīva; vai

227 Datu aizsardzības direktīva, 26. panta 1. punkta d) apakšpunkts.

- , lai celtu, īstenotu vai aizstāvētu tiesībpamatotus prasījumus.

Iepriekš minētie gadījumi ir jāsaprot kā izņēmumi no normas, ka, lai netraucēti nodotu datus citām valstīm, ir vajadzīgs adekvāts datu aizsardzības līmenis saņēmējā valstī. Izņēmumi vienmēr ir jāinterpretē ierobežojoši. To ir atkārtoti uzsvērusi 29. panta darba grupa saistībā ar datu aizsardzības direktīvas 26. panta 1. punktu, jo īpaši, ja piekrišana ir domātais pamats datu nodošanai.[228] 29. panta darba grupa secināja, ka vispārīgās normas par piekrišanas juridisko nozīmi arī attiecas uz direktīvas 26. panta 1. punktu. Ja, piemēram, darba attiecību kontekstā nav skaidrs, vai darba ņēmēju dotā piekrišana ir patiešām brīva piekrišana, tad datu nodošanu nevar pamatot ar direktīvas 26. panta 1. punkta a) apakšpunktu. Tādos gadījumos piemēros 26. panta 2. punktu, kas prasa, lai valsts datu aizsardzības iestādes izdotu licenci datu nodošanai.

6.4. Ierobežotas datu plūsmas uz trešām valstīm

Galvenie punkti

- Pirms datu eksportēšanas uz trešām valstīm, kurās nenodrošina adekvātu datu aizsardzības līmeni, pārzinim varbūt būs jāļauj uzraudzības iestādei pārbaudīt plānoto datu plūsmu.
- Pārzinim, kurš vēlas eksportēt datus, šīs pārbaudes laikā ir jāpierāda divas lietas:
  - ka pastāv tiesisks pamats datu nodošanai saņēmējam; un
  - ka ir ieviesti pasākumi, lai nodrošinātu adekvātu datu aizsardzību pie saņēmēja.
- Pasākumi, lai izveidotu adekvātu datu aizsardzību pie saņēmēja, var ietvert šādus:
  - līgumu parakstīšana datu eksportēšanas pārziņa un ārvalstu datu saņēmēja starpā; vai
  - saistošie korporatīvie noteikumi, parasti piemērojami datu nodošanai daudznacionālā uzņēmumu grupā.
- Datu nodošanu ārvalstu iestādēm var regulēt arī ar īpašu starptautisku nolīgumu.

228 Sk. jo īpaši 29. panta darba grupas (2005) *Darba dokumentu par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta vienotu interpretāciju*, WP 114, Briselē, 2005. gada 25. novembrī.

Datu aizsardzības direktīva un 108. konvencijas papildprotokols ļauj valsts tiesību aktiem izveidot režīmus pārrobežu datu plūsmām uz trešām valstīm, nenodrošinot adekvātu datu aizsardzības līmeni, kamēr vien pārzinis ir veicis īpašus pasākumus, lai nodrošinātu adekvātas datu aizsardzības garantijas pie saņēmēja un kamēr vien pārzinis var to pierādīt kompetentajai iestādei. Šī prasība ir skaidri pieminēta tikai 108. konvencijas papildprotokolā; tomēr to uzskata par standarta procedūru arī atbilstoši datu aizsardzības direktīvai.

6.4.1. Līguma punkti

Gan **EP tiesību aktos,** gan **ES tiesību aktos** ir pieminēti līguma punkti, par ko vienojas datu eksportēšanas pārzinis un saņēmējs trešā valstī, kā iespējams līdzeklis pietiekamā līmenī aizsargāt datu aizsardzību pie saņēmēja.

ES mērogā Eiropas Komisija ar 29. panta darba grupas palīdzību izstrādāja standarta līguma punktus [līguma standartklauzulas], ko ar Komisijas lēmumu oficiāli sertificēja kā adekvātas datu aizsardzības pierādījumu.[229] Tā kā Komisijas lēmumi uzliek dalībvalstīm saistības kopumā, valsts iestādēm, kuras atbild par pārrobežu datu plūsmu uzraudzību, savās procedūrās ir jāatzīst minētie standarta līguma punkti.[230] Tādējādi, ja datu eksportēšanas pārzinis un trešās valsts saņēmējs piekrīt un paraksta šos punktus, tam būtu jānoder uzraudzības iestādei kā pietiekamam pierādījumam, ka ir ieviestas pienācīgas garantijas.

Standarta līguma punktu esība ES tiesiskajā regulējumā neliedz pārziņiem formulēt citus *ad hoc* līguma punktus. Tomēr tiem jārada tāds pats aizsardzības līmenis, kāds paredzēts standarta līguma punktos. Svarīgākās standarta līguma punktu iezīmes ir šādas:

- ieinteresētās trešās personas [saņēmēja] punkts, kas dod datu subjektiem tiesības īstenot līgumtiesības, pat ja tie nav līguma slēdzējpuse;

- datu saņēmējs vai importētājs piekrīt pakļauties datu eksportēšanas pārziņa valsts uzraudzības iestādes procedūrai un/vai tiesām domstarpību gadījumā;

229 Datu aizsardzības direktīva, 26. panta 4. punkts.

230 LESD, 288. pants.

Tagad nodošanai „pārzinis pārzinim" ir pieejami divi standarta punktu komplekti, no kuriem datu eksportēšanas pārzinis var izvēlēties.[231] Nodošanai „pārzinis personas datu operatoram" ir tikai viens standarta līguma punktu komplekts.[232]

EP tiesību aktu kontekstā 108. konvencijas Konsultatīvā komiteja izstrādāja vadlīnijas par līguma punktu sagatavošanu.[233]

6.4.2. Saistošie korporatīvie noteikumi

Daudzpusējie saistošie korporatīvie noteikumi (*BCR*) ļoti bieži iesaista vienlaikus vairākas Eiropas datu aizsardzības iestādes.[234] Lai apstiprinātu *BCR*, *BCR* projekts kopā ar standartizētām pieteikuma veidlapām jānosūta vadošajai iestādei.[235] Vadošo iestādi var identificēt no standartizētās pieteikuma veidlapas. Šī iestāde tad informē visas uzraudzības iestādes EEZ dalībvalstīs, kur ir izveidotas grupas filiāles, lai gan to dalība *BCR* novērtēšanas procesā ir brīvprātīga. Lai gan tas nav saistoši, visām datu aizsardzības iestādēm būtu jāiekļauj novērtēšanas rezultāts savās formālajās licencēšanas procedūrās.

6.4.3. Īpaši starptautiskie nolīgumi

ES ir noslēgusi īpašus nolīgumus par datu nodošanas veidiem:

231 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.

232 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.

233 EP (108. konvencijas Konsultatīvā komiteja, 2002), *Vadlīnijas līguma punktu sagatavošanai, kas regulē datu aizsardzību, nododot personas datus trešām personām, kas nenodrošina adekvātu datu [aizsardzības] līmeni.*

234 Pienācīgu saistošo korporatīvo noteikumu saturs un struktūra ir paskaidroti 29. panta darba grupas (2008) *Darba dokumentā, ar ko izveido saistošo uzņēmuma [korporatīvo] noteikumu struktūras shēmu,* WP 154, Briselē, 2008. gada 24. jūnijā; un 29. panta darba grupas (2008) *Darba dokumentā, ar ko izveido tabulu ar noteikumiem un principiem, kas jāietver saistošajos uzņēmuma [korporatīvajos] noteikumos,* WP 153, Briselē, 2008. gada 24. jūnijā.

235 29. panta darba grupa (2007), *Ieteikums Nr. 1/2007 par standarta pieteikumu, lai saņemtu apstiprinājumu saistošajiem korporatīvajiem noteikumiem personas datu nodošanai*, WP 133, Briselē, 2007. gada 10. janvārī.

Pasažieru datu reģistri

Pasažieru datu reģistru (PDR) datus savāc gaisa pārvadātāji rezervācijas procesā, un šie dati ietver aviopasažieru vārdus/uzvārdus, adreses, kredītkaršu informāciju un sēdvietas numuru. Saskaņā ar ASV tiesību aktiem aviopārvadātajiem pirms pasažieru izlidošanas ir jādara šie dati pieejami [ASV] Tēvzemes drošības departamentam. Tas attiecas uz lidojumiem uz vai no Amerikas Savienotajām Valstīm.

Lai nodrošinātu pasažieru datu reģistra (PDR) datu aizsardzības līmeni atbilstošu Direktīvas 95/46/EK nosacījumiem, 2004. gadā tika pieņemta "PDR tiesību aktu pakete"[236], kurā ietilpa ASV Tēvzemes drošības departamenta datu apstrādes atbilstība datu aizsardzības līmenim.

Pēc tam, ka Tiesa PDR paketi bija anulējusi[237], ES un Savienotās Valstis parakstīja divus atsevišķus nolīgumus ar divkāršu nolūku: pirmkārt, sniegt tiesisku pamatu PDR datu atklāšanai ASV iestādēm, un otrkārt, izveidot adekvātu datu aizsardzību saņēmējā valstī.

Pirmajam nolīgumam par datu koplietošanu un pārvaldību ES valstu un ASV starpā, parakstītam 2012. gadā, bija vairāki trūkumi, un tas tika aizstāts tajā pašā gadā ar jaunu nolīgumu, lai labāk nodrošinātu juridisko noteiktību.[238] Jaunais nolīgums piedāvā nozīmīgus uzlabojumus. Tas ierobežo un izskaidro nolūkus, kuriem informāciju drīkst izmantot, piemēram, pārrobežu noziegumi un terorisms, un tas nosaka laikposmu **kādā** datus drīkst uzglabāt: pēc sešiem mēnešiem, datus nepieciešams depersonalizēt un aizsegt. Savu datu ļaunprātīgas izmantošanas gadījumā katram ir tiesības prasīt administratīvo un tiesisko palīdzību saskaņā ar ASV tiesību aktiem. Viņiem ir arī tiesības uz piekļuvi saviem PDR datiem un tiesības prasīt ASV Tēvzemes

236 2004. gada 17. maija Padomes Lēmums par nolīguma noslēgšanu starp Eiropas Kopienu un Amerikas Savienotajām Valstīm attiecībā uz personas datu apstrādi un pārsūtīšanu, ko aviopārvadātāji veic ASV Nacionālās drošības ministrijas Muitas un robežsardzes departamentam, OV 2004 L 183, 83 lpp., un 2004. gada 14. maija Komisijas Lēmums par pietiekamu aizsardzību *Pasažieru Datu Reģistrā* iekļautajiem lidmašīnu pasažieru personas datiem, kas nosūtīti Amerikas Savienoto Valstu Muitas un robežapsardzes birojam, OV 2004 L 235, 11-22 lpp.

237 Tiesas 2006. gada 30. maija spriedums apvienotajās lietās C-317/04 un C-318/04, *Eiropas Parlaments pret Eiropas Savienības Padomi*, 57, 58 un 59 punkti, kurā tiesa lēma, ka ne viens ne otrs no lēmumiem par atbilstošu datu aizsardzības līmeni, ne nolīgums par datu apstrādi, neietilpa Direktīvas jomā.

238 Padomes 2012. gada 26. aprīļa Lēmums 2012/472/ES par to, lai noslēgtu Nolīgumu starp Amerikas Savienotajām Valstīm un Eiropas Savienību par pasažieru datu reģistra datu izmantošanu un pārsūtīšanu Amerikas Savienoto Valstu Iekšzemes drošības departamentam, OV 2012 L 215/4. Nolīguma teksts ir pievienots šim lēmumam, OV 2012 L 215, 5.–14. lpp.

drošības departamentam izdarīt labojumus, tostarp dzēst datus, ja informācija ir neprecīza.

Nolīgums, kas stājās spēkā 2012. gada 1. jūlijā, būs spēkā septiņus gadus – līdz 2019. gadam.

2011. gada decembrī Eiropas Savienības Padome apstiprināja atjaunināt ES un Austrālijas Nolīgumu par PDR datu apstrādi un pārsūtīšanu.[239] ES un Austrālijas nolīgums par PDR datiem ir vēl viens solis ES darba programmā, kur ietilpst globālas PDR vadlīnijas,[240] tiek izveidota ES-PDR shēma[241] un tiek apspriesti nolīgumi ar trešām valstīm.[242]

Finanšu ziņojumapmaiņas dati

Beļģijā bāzētā Vispasaules Starpbanku finanšu telekomunikāciju sabiedrība (SWIFT), kas ir personas datu operators lielākajai daļai globālo naudas pārskaitījumu no Eiropas bankām, izmantoja "spoguļserveri" kādā no saviem datošanas centriem Amerikas Savienotajās Valstīs un saņēma pieprasījumu atklāt datus ASV Valsts kases departamentam terorisma izmeklēšanas nolūkiem.[243]

239 Padomes 2011. gada 13. decembra Lēmums 2012/381/ES par to, lai noslēgtu Nolīgumu starp Eiropas Savienību un Austrāliju par gaisa pārvadātāju veikto pasažieru datu reģistra (PDR) datu apstrādi un pārsūtīšanu Austrālijas Muitas un robežapsardzes dienestam, OV 2012 L 186/3. Šis Nolīgums, aizstāja agrāku 2008 gada Nolīgumu. Tā teksts ir pievienots šim lēmumam, OV 2012 L 186, 4.–16. lpp.

240 Sk. jo īpaši Komisijas 2010. gada 21. septembra Paziņojumu par vispārējo pieeju pasažieru datu reģistra (PDR) datu nosūtīšanai [nodošanai] trešām valstīm, COM(2010) 492 final, Briselē, 2010. gada 21. septembrī. Sk. arī 29. panta darba grupas (2010) *Atzinumu 7/2010 par Eiropas Komisijas Paziņojumu par vispārējo pieeju pasažieru datu reģistra (PDR) datu nosūtīšanai trešām valstīm,* WP 178, Briselē, 2010 gada 12. novembrī.

241 Priekšlikums Eiropas Parlamenta un Padomes Direktīvai par PDR datu izmantošanu, lai novērstu, atklātu, izmeklētu teroristu nodarījumus un smagus noziegumus un sauktu pie atbildības par tiem, COM(2011) 32 final, Briselē, 2011. gada 2. februārī. 2011. gada aprīlī Eiropas Parlaments lūdza *FRA* sniegt atzinumu par šo priekšlikumu un tā atbilstību Eiropas Savienības Pamattiesību hartai. Sk.: FRA (2011), *Atzinums 1/2011 – Pasažieru datu reģistrs*, Vīne, 2011. gada 14. jūnijā.

242 ES pašlaik apspriež jaunu PDR nolīgumu ar Kanādu, kas aizstās 2006. gada pašreiz spēkā esošo.

243 Sk. šajā sakarā 29. panta darba grupas (2011) *Atzinumu 14/2011 par datu aizsardzības jautājumiem, kas attiecas uz nelikumīgi iegūtu* līdzekļu *legalizācijas un teroristu finansēšanas novēršanu*, WP 186, Briselē, 2011. gada 13. jūnijā, 29. panta darba grupas (2006) *Atzinumu 10/2006 par personas datu apstrādi, ko veic Society for Worldwide Interbank Financial Telecommunications (SWIFT)*, WP 128, Briselē, 2006. gada 22. novembrī; 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"*.

No ES viedokļa, nebija pietiekama tiesiska pamata atklāt šos būtībā Eiropas datus, kuriem varēja piekļūt Amerikas Savienotajās Valstīs tikai tāpēc, ka viens no SWIFT datu pakalpojumu apstrādes centriem atradās Amerikas Savienotajās Valstīs. Tā kā ASV Valsts kases departamenta piekļuve veidoja datu nodošanu atbilstīgi datu aizsardzības direktīvas 26. pantam, ir jāievēro šā noteikuma prasības.

2010. gadā ES un ASV starpā tika noslēgts speciāls nolīgums, zināms kā SWIFT nolīgums, lai sniegtu vajadzīgo tiesisko pamatu un nodrošinātu adekvātu datu aizsardzību.[244]

Atbilstīgi šim nolīgumam SWIFT bāzē uzglabātos finanšu datus dara pieejamus ASV Valsts kases departamentam, lai novērstu, izmeklētu, atklātu terorismu vai terorisma finansēšanu un sauktu pie atbildības par to. ASV Valsts kases departaments var pieprasīt finanšu datus no SWIFT, ar nosacījumu, ka šis pieprasījums:

- pēc iespējas skaidri identificē finanšu datus,
- skaidri pamato datu vajadzību,
- ir izstrādāts pēc iespējas šauri, lai maksimāli mazinātu pieprasīto datu apjomu,
- neprasa datus, kas saistīti ar Vienoto euro maksājumu telpu (SEPA).

Eiropolam jāsaņem katra ASV Valsts kases departamenta pieprasījuma kopija un jāpārbauda, vai ir vai nav ievēroti SWIFT nolīguma principi.[245] Ja apstiprinās, ka tie ir ievēroti, tad SWIFT jāsniedz finanšu dati tieši ASV Valsts kases departamentam. Departamentam jāuzglabā finanšu dati drošā fiziskā vidē, kur tiem var piekļūt tikai analītiķi, kuri izmeklē terorismu vai tā finansēšanu, un finanšu dati nedrīkst būt savstarpēji saistīti ar jebkuru citu datu bāzi. Parasti no SWIFT saņemtos finanšu datus dzēš ne vēlāk kā piecus gadus pēc saņemšanas. Finanšu datus, kas ir būtiski specifiskām izmeklēšanām vai apsūdzībām, var saglabāt tik ilgi, cik nepieciešams šīm izmeklēšanām vai apsūdzībām.

244 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.

245 Europol Apvienotā uzraudzības iestāde ir veikusi Europol darbības auditus šajā jomā, kuru rezultāti pieejami: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

ASV Valsts kases departaments var nodot no SWIFT saņemtajiem datiem gūto informāciju īpašām likuma uzraudzības, sabiedriskās drošības vai terorisma apkarošanas iestādēm ASV vai ārpus to robežām tikai tādēļ, lai izmeklētu, atklātu, novērstu terorismu un tā finansēšanu vai sauktu pie atbildības par to. Ja finanšu datu tālāknodošana skar kādu ES dalībvalsts pilsoni vai pastāvīgo iedzīvotāju, koplietot datus trešās valsts iestādēm var tikai tad, ja iepriekš ir saņemta attiecīgās dalībvalsts kompetento iestāžu atļauja. Izņēmumi ir pieļaujami tikai tad, ja datu koplietošana ir būtiska, lai novērstu tūlītēju un nopietnu sabiedriskās drošības apdraudējumu.

Neatkarīgi uzraudzītāji, tostarp Eiropas Komisijas norīkota persona, uzrauga atbilstību SWIFT nolīguma principiem.

Datu subjektiem ir tiesības saņemt apstiprinājumu no kompetentās ES datu aizsardzības iestādes, ka ir ievērotas to personas datu aizsardzības tiesības. Datu subjektiem arī ir tiesības labot, dzēst vai bloķēt savus datus, ko savācis un uzglabā ASV Valsts kases departaments atbilstoši SWIFT nolīgumam. Tomēr uz datu subjektu piekļuves tiesībām var attiekties zināmi juridiski ierobežojumi. Ja piekļuve tiek atteikta, tad datu subjekts rakstiski jāinformē par atteikumu un par viņa tiesībām prasīt Amerikas Savienotajās Valstīs administratīvu un tiesisku palīdzību.

SWIFT nolīgums ir spēkā piecus gadus – līdz 2015. gada augustam. Tā derīguma termiņš automātiski pagarinās par turpmākiem viena gada periodiem, ja vien kāda no pusēm sešus mēnešus iepriekš nepaziņo otrai savu nodomu vairs nepagarināt nolīgumu.

7

Datu aizsardzība policijas un krimināltiesību kontekstā

ES	Aplūkotie jautājumi	EP
	Vispārīgi	108. konvencija
	Policija	Policijas ieteikums
		ECT 2009. gada 17. decembra spriedums lietā *B.B. pret Franciju*, prasības pieteikums Nr. 5335/06
		ECT 2008. gada 4. decembra spriedums lietā *S. un Marper pret Apvienoto Karalisti*, prasības pieteikums Nr. 30562/04 un Nr. 30566/04
		ECT 2005. gada 31. maija spriedums lietā *Vetter pret Franciju*, prasības pieteikums Nr. 59842/00
	Kibernoziedzība	Kibernoziedzības Konvencija
Datu aizsardzība saistībā ar policijas un tiesu iestāžu pārrobežu sadarbību		
Datu aizsardzības pamatlēmums	Vispārīgi	108. konvencija Policijas ieteikums
Prīmes lēmums	Par īpašajiem datiem: pirkstu nospiedumi, DNS, huligānisms utt.	108. konvencija Policijas ieteikums
Europol lēmums Eurojust lēmums Frontex regula	Ko veic īpašas aģentūras	108. konvencija Policijas datu ieteikums
Šengenas II lēmums VIS regula Eurodac regula CIS lēmums	Ko veic īpašas kopīgās informācijas sistēmas	108. konvencija Policijas ieteikums
		ECT 2010. gada 2. februāra spriedums lietā *Dalea pret Franciju*, prasības pieteikums Nr. 964/07

Lai līdzsvarotu personas intereses par savu datu aizsardzību un sabiedrības intereses par datu vākšanu noziedzības apkarošanas un valsts un sabiedriskās drošības nodrošināšanas nolūkā, EP un ES ir ieviesušas īpašus juridiskos instrumentus.

7.1. EP tiesību akti par datu aizsardzību policijas un krimināltiesību jautājumos

Galvenie punkti

- 108. konvencija un EP Ieteikums par policiju attiecas uz datu aizsardzību visās policijas darba jomās.
- Konvencija par kibernoziedzību (*Budapeštas Konvencija*) ir saistošs starptautisks juridisks instruments, kas nodarbojas ar noziegumiem, kas veikti pret elektroniskiem tīkliem un ar to starpniecību.

Eiropas mērogā 108. konvencija attiecas uz visām personas datu apstrādes jomām, un ar tās noteikumiem ir plānots regulēt vispār personas datu apstrādi. Līdz ar to 108. konvencija attiecas uz datu aizsardzību policijas un krimināltiesību jomā, lai gan Līgumslēdzējas puses var ierobežot tās piemērošanu.

Policijas un krimināltiesību iestāžu juridisko uzdevumu veikšanai bieži vien ir jāapstrādā personas dati, kas var radīt nopietnas sekas iesaistītajām personām. EP 1987. gadā pieņemtais Policijas datu ieteikums dod pamatnostādnes līgumslēdzējām pusēm par to, kā piešķirt ietekmi 108. konvencijas principiem saistībā ar personas datu apstrādi, ko veic policijas iestādes.[246]

7.1.1. Policijas ieteikums

ECT ir pastāvīgi apgalvojusi, ka tas, ka policija vai valsts drošības iestādes krāj un saglabā personas datus, ir ECK 8. panta 1. punktā garantēto tiesību aizskārums. Daudzi ECT spriedumi ir par šādu aizskārumu attaisnošanu.[247]

246 EP, Ministru komiteja (1987), 1987. gada 17. septembra Ieteikums Nr. Rec(87)15 dalībvalstīm, kas regulē personas datu izmantošanu policijas sektorā.

247 Sk., piemēram, ECT 1987. gada 26. marta spriedumu lietā *Leander pret Zviedriju*, prasības pieteikums Nr. 9248/81; ECT 2012. gada 13. novembra spriedums lietā *M.M. pret Apvienoto Karalisti*, prasības pieteikums Nr. 24029/07; ECT 2013. gada 18. aprīļa spriedums lietā *M.K. pret Franciju*, prasības pieteikums Nr. 19522/09.

Piemērs: Lietā *B.B. pret Franciju*[248] ECT nolēma, ka uz notiesāta dzimumnoziedznieka iekļaušanu valsts tiesu datu bāzē attiecās ECK 8. pants. Tomēr, ņemot vērā, ka bija īstenotas pietiekamas datu aizsardzības garantijas, piemēram, datu subjekta tiesības pieprasīt dzēst datus, ierobežots datu uzglabāšanas ilgums un ierobežota piekļuve tādiem datiem, bija nodrošināts atbilstošs līdzsvars starp konkurējošām iesaistītajām privātajām un publiskajām interesēm. Tiesa secināja, ka nav bijis ECK 8. panta prasību pārkāpuma.

Piemērs: Lietā *S.* un *Marper pret Apvienoto Karalisti*[249] abi prasītāji bija apsūdzēti, bet ne notiesāti, par noziedzīgiem nodarījumiem. Tomēr viņu pirkstu nospiedumi, DNS profili un šūnu paraugi tika turēti un uzglabāti policijā. Neierobežota biometrisko datu saglabāšana bija atļauta ar nolikumu, ja personu turēja aizdomās par noziedzīgu nodarījumu, pat ja vēlāk aizdomās turēto attaisnoja vai atbrīvoja. ECT uzskatīja, ka visaptveroša un nediskriminējoša personas datu saglabāšana, kas nebija ierobežota laikā, un kur attaisnotām personām bija tikai ierobežota iespēja prasīt dzēst datus, bija nesamērīgs prasītāju tiesību uz privātās dzīves neaizskaramību aizskārums. Tiesa secināja, ka ir bijis ECK 8. panta pārkāpums.

Daudzi turpmāki ECT spriedumi ir par uzraudzības iestāžu veikta tiesību uz datu aizsardzību aizskāruma attaisnošanu.

Piemērs: Lietā *Allan pret Apvienoto Karalisti*[250] iestādes bija slepeni ierakstījušas kāda cietumnieka privātas sarunas ar draugu cietuma apmeklējumu telpā un ar vienu līdzapsūdzētu biedru cietuma kamerā. ECT uzskatīja, ka audio- un videoieraksta ierīču izmantošana prasītāja kamerā, cietuma apmeklējumu telpā un pie ieslodzīta cietuma biedra bija prasītāja tiesību uz privāto dzīvi aizskārums. Tā kā attiecīgajā laikā nebija statutāras sistēmas, lai regulētu to, kā policija izmanto slepenas ierakstu ierīces, minētais aizskārums nenotika saskaņā ar tiesību aktiem. Tiesa secināja, ka ir bijis ECK 8. panta tiesību pārkāpums.

248 ECT 2009. gada 17. decembra spriedums lietā *B.B. pret Franciju*, prasības pieteikums Nr. 5335/06.

249 ECT 2008. gada 4. decembra spriedums lietā *S. un Marper pret Apvienoto Karalisti*, prasības pieteikums Nr. 30562/04 un Nr. 30566/04, 119. un 125. punkts.

250 ECT 2002. gada 5. novembra spriedums lietā *Allan pret Apvienoto Karalisti*, prasības pieteikums Nr. 48539/99.

Piemērs: Lietā *Klass un citi pret Vāciju*[251] prasītāji apgalvoja, ka vairāki Vācijas leģislatīvie akti, kas atļāva slepeni uzraudzīt parasto pastu, e-pastu un telekomunikācijas, pārkāpa ECK 8. panta prasības, konkrēti tāpēc, ka attiecīgā persona nebija informēta par uzraudzības pasākumiem un nevarēja vērsties tiesās pēc minēto pasākumu beigām. ECT uzskatīja, ka uzraudzības drauds katrā ziņā aizskāra komunikācijas brīvību e-pasta un telekomunikāciju pakalpojumu lietotāju starpā. Tomēr tā konstatēja, ka ir tikušas ieviestas pietiekamas garantijas pret ļaunprātīgu izmantošanu. Vācijas leģislatūra bija attaisnota, uzskatot minētos pasākumus par nepieciešamiem demokrātiskā sabiedrībā valsts drošības interesēs un lai novērstu nekārtības vai noziedzību. Tiesa secināja, ka nav bijis ECK 8. panta prasību pārkāpuma.

Tā kā datu apstrādei, ko veic policijas iestādes, var būt ievērojama ietekme uz attiecīgajām personām, sīki izstrādātas datu aizsardzības normas datu bāzu uzturēšanai šajā jomā ir īpaši vajadzīgas. EP Ieteikums par policiju cenšas risināt šo jautājumu, sniedzot vadlīnijas par to, kā jāvāc dati policijas darbam, kā jāuztur datu datnes šajā jomā, kam jābūt atļaujai piekļūt šīm datnēm, tostarp nosacījumi par datu nodošanu ārvalstu policijas iestādēm, kā datu subjektiem jāspēj īstenot savas datu aizsardzības tiesības, un kā jāīsteno neatkarīgu iestāžu veikta kontrole. Tiek aplūkots arī pienākums nodrošināt adekvātu datu drošību.

Ieteikumā nav paredzēts, ka policijas iestādes var nediskriminēti un neierobežoti laikā vākt datus. Tas ierobežo personas datu vākšanu, ko veic policijas iestādes, līdz tam, kas ir stingri nepieciešams, lai novērstu reālu apdraudējumu vai apkarotu specifiskus noziedzīgus nodarījumus. Jebkura papildu datu vākšana jāpamato uz īpašiem valsts tiesību aktiem. Sensitīvu datu apstrāde jāierobežo līdz tam, kas ir absolūti nepieciešams saistībā ar konkrētu izmeklēšanu.

Ja personas datus vāc, datu subjektam to nezinot, datu subjekts jāinformē par datu vākšanu tiklīdz tāda atklāšana vairs netraucē izmeklēšanai. Datu vākšanai, ko veic ar tehniskas uzraudzības vai citiem automatizētiem līdzekļiem, jāpamato uz īpašiem juridiskiem noteikumiem.

Piemērs: Lietā *Vetter pret Franciju*[252] anonīmi liecinieki bija apsūdzējuši prasītāju par slepkavību. Tā kā prasītājs regulāri gāja uz kāda drauga mājām, policija tur ar izmeklēšanas tiesneša atļauju uzstādīja noklausīšanās ierīces. Pamatojo-

251 ECT 1978. gada 6. septembra spriedums lietā *Klass un citi pret Vāciju*, prasības pieteikums Nr. 5029/71.

252 ECT 2005. gada 31. maija spriedums lietā *Vetter pret Franciju*, prasības pieteikums Nr. 59842/00.

ties uz ierakstītajām sarunām prasītāju apcietināja un sauca pie atbildības par slepkavību. Viņš prasīja, lai ierakstu paziņotu par nepieņemamu un neiekļautu kā pierādījumu, jo īpaši apgalvojot, ka tas nebija paredzēts tiesību aktos. Eiropas Cilvēktiesību tiesai svarīgākais bija jautājums par to, vai noklausīšanās ierīču izmantošana bija vai nebija „saskaņā ar tiesību aktiem". Privātu telpu slepena noklausīšanās acīmredzami nav Kriminālprocesa kodeksa 100. un nākamo pantu darbības jomā, jo minētie noteikumi attiecas uz telefona līniju pārtveršanu. Kodeksa 81. pantā nebija saprātīgi skaidri norādīts iestāžu rīcības brīvības tvērums vai īstenošanas veids, atļaujot uzraudzīt privātas sarunas. Attiecīgi prasītājam nebija nodrošināts aizsardzības līmeņa minimums, uz kuru pilsoņiem ir tiesības atbilstīgi likuma varai demokrātiskā sabiedrībā. Tiesa secināja, ka ir bijis ECK 8. panta prasību pārkāpums.

Ieteikumā ir secināts, ka, uzglabājot personas datus, ir skaidri jānošķir starp: administratīvajiem datiem un policijas datiem, dažāda veida datu subjektiem, kā aizdomās turamie, notiesātās personas, upuri un liecinieki; un dati, ko uzskata par stingriem faktiem, jānošķir no datiem, kuru pamatā ir aizdomas vai spekulācija.

Policijas datiem ir jābūt stingri ierobežotiem pēc nolūka. Tas ietekmē to, kā policijas datus paziņo trešām personām: tādu datu nodošana vai paziņošana policijas jomā ir jāregulē, vadoties no tā, vai pastāv likumīgas intereses informācijas koplietošanai vai nepastāv. Tādu datu nodošana vai paziņošana ārpus policijas jomas ir jāatļauj tikai tad, ja ir skaidrs juridisks pienākums vai atļauja. Starptautiska nodošana vai paziņošana ir jāierobežo līdz ārvalstu policijas iestādēm un jāpamato uz speciāliem tiesiskiem noteikumiem, pēc iespējas starptautiskiem nolīgumiem, izņemot gadījumus, kad tas ir nepieciešams nopietna un tūlītēja apdraudējuma novēršanai.

Datu apstrāde, ko veic policija, jāpakļauj neatkarīgai uzraudzībai, lai nodrošinātu atbilstību valsts datu aizsardzības tiesību aktiem. Datu subjektiem jābūt visām 108. konvencijā ietvertajām piekļuves tiesībām. Ja datu subjekta piekļuves tiesības ir ierobežotas saskaņā ar 108. konvencijas 9. pantu efektīvas policijas izmeklēšanas interesēs, datu subjektam ir jābūt tiesībām atbilstoši valsts tiesību aktiem iesniegt sūdzību valsts datu aizsardzības uzraudzības iestādē vai citā neatkarīgā struktūrā.

7.1.2. Budapeštas Konvencija par kibernoziedzību

Tā kā kriminālās darbības arvien vairāk izmanto un ietekmē elektroniskās datu apstrādes sistēmas, šīs problēmas risināšanai vajag jaunus juridiskos noteikumus krimināljomā. Tāpēc EP pieņēma starptautisku juridisku instrumentu, Konvenciju par

kibernoziedzību – kas zināma arī kā Budapeštas konvencija – lai risinātu jautājumu par noziegumiem, kas pastrādāti pret elektroniskajiem tīkliem un ar to starpniecību.[253] Šī konvencija ir atvērta, lai tai pievienotos arī valstis, kas nav EP biedri, un līdz 2013. gada vidum Konvencijas līgumslēdzējas puses bija četras valstis ārpus EP – Amerikas Savienotās Valstis, Austrālija, Dominikānas Republika un Japāna, un vēl 12 valstis, kas neietilpst EP, bija to parakstījušas vai bija uzaicinātas pievienoties.

Konvencija par kibernoziedzību paliek visietekmīgākais starptautiskais līgums, kas risina tiesību aktu prasību pārkāpumus interneta vai citos informācijas tīklos. Tā prasa saviem dalībniekiem atjaunināt un saskaņot tiesību aktus krimināljomā pret hakeru darbību un citiem drošības pārkāpumiem, tostarp pārkāpumiem saistībā ar autortiesībām, datorveicinātu krāpšanu, bērnu pornogrāfiju un citām nelikumīgām kiberdarbībām. Konvencijā ir arī paredzētas procesuālas pilnvaras, kas attiecas uz datortīklu pārmeklēšanu un komunikāciju pārtveršanu saistībā ar kibernoziedzības apkarošanu. Visbeidzot, tā dod iespēju efektīvi sadarboties starptautiskā mērogā. Konvencijas papildprotokols nosaka krimināatbildību par rasisma un ksenofobijas propagandu datoru tīklos.

Lai gan konvencija faktiski nav datu aizsardzības veicināšanas instruments, tā nosaka krimināatbildību par darbībām, kuras var aizskart datu subjekta tiesības uz savu datu aizsardzību. Konvencija arī nosaka Līgumslēdzējām Pusēm par pienākumu, īstenojot konvenciju, paredzēt, lai adekvāti tiktu aizsargātas cilvēktiesības un brīvības, tostarp saskaņā ar ECK garantētās tiesības, kā tiesības uz datu aizsardzību.[254]

7.2. ES tiesību akti par datu aizsardzību policijas un krimināllietu jomā

Galvenie punkti

- ES mērogā datu aizsardzību policijas un krimināltiesību jomā regulē tikai saistībā ar policijas un tiesu iestāžu pārrobežu sadarbību.

253 Eiropas Padome, Ministru komiteja (2001), Konvencija par kibernoziedzību, CETS Nr. 185, Budapešta, 2001. gada 23. novembrī, stājās spēkā 2004. gada 1. jūlijā.

254 Turpat, 15. panta 1. punkts.

- Īpaši datu aizsardzība režīmi pastāv Eiropas Policijas birojam (*Europol*) un ES Tiesu iestāžu sadarbības struktūrvienībai (*Eurojust*) – ES iestādēm, kuras palīdz un veicina pārrobežu tiesībaizsardzību.
- Īpaši datu aizsardzības režīmi pastāv arī kopīgajām informācijas sistēmām, kas izveidotas ES mērogā pārrobežu informācijas apmaiņai starp kompetentajām policijas un tiesu iestādēm. Svarīgi piemēri ir Šengena II, Vīzu informācijas sistēma (*VIS*) un *Eurodac* – centralizēta sistēma, kas satur datus par to trešo valstu pilsoņu pirkstu nospiedumiem, kuri iesniedz patvēruma pieteikumu kādā no ES dalībvalstīm.

Datu aizsardzības direktīva neattiecas uz policijas un krimināltiesību jomu. 7.2.1 iedaļā ir aprakstīti svarīgākie juridiskie instrumenti šajā jomā.

7.2.1. Datu aizsardzības pamatlēmums

Padomes Pamatlēmuma 2008/977/TI par tādu personas datu aizsardzību, ko apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās (*Datu aizsardzības pamatlēmums*)[255] mērķis ir nodrošināt fiziskām personām personas datu aizsardzību, kad to personas datus apstrādā, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības vai piespriestu krimināLsodu par tiem. Dalībvalstu vai ES vārdā rīkojas kompetentās iestādes, kuras darbojas policijas un krimināltiesību jomā. Šīs iestādes ir ES aģentūras vai struktūras, kā arī dalībvalstu iestādes.[256] Pamatlēmuma piemērojamība ir ierobežota līdz datu aizsardzības nodrošināšanai šo iestāžu pārrobežu sadarbībā un neattiecas uz valsts drošību.

Datu aizsardzības pamatlēmums lielā mērā pamatojas uz principiem un definīcijām, kas ietverti 108. konvencijā un datu aizsardzības direktīvā.

Datus drīkst izmantot tikai kompetentā iestāde un tikai tam nolūkam, kuram datus nodeva vai darīja pieejamus. Saņēmējai dalībvalstij jāievēro visi nododošās dalībvalsts tiesību aktos paredzētie ierobežojumi attiecībā uz datu apmaiņu. Datu izmantošana saņēmējā valstī citam nolūkam tomēr ir atļauta ar zināmiem nosacījumiem. Sūtījumu ielādēšana un nosūtīšana ir specifisks kompetento iestāžu uzdevums, lai palīdzētu noskaidrot pienākumus, kuri izriet no sūdzībām. Lai pārrobežu sadarbības gaitā saņemtos datu tālāk nodotu trešām personām, ir vajadzīga datu izcelsmes dalībvalsts piekrišana, lai gan steidzamos gadījumos ir paredzēti izņēmumi.

255 Eiropas Savienības Padome (2008), Padomes 2008. gada 27. novembra Pamatlēmums 2008/977/TI par tādu personas datu aizsardzību, ko apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās (Datu aizsardzības pamatlēmums), OV 2008 L 350.

256 Turpat, 2. panta h) punkts.

Kompetentajām iestādēm ir jāveic vajadzīgie drošības pasākumi, lai aizsargātu personas datus pret jebkādu nelikumīgu apstrādes formu.

Katrai dalībvalstij jānodrošina, ka viena vai vairākas neatkarīgas valsts uzraudzības iestādes atbild par saskaņā ar Datu aizsardzības pamatlēmumu pieņemto noteikumu piemērošanas pārraudzību un padomu došanu saistībā ar tiem. Tās arī izskata jebkuras personas iesniegtu pieprasījumu par viņa vai viņas tiesību un brīvību aizsardzību saistībā ar personas datu apstrādi, ko veic kompetentās iestādes.

Datu subjektam ir tiesības saņemt informāciju par viņa vai viņas personas datu apstrādi un tiesības uz piekļuvi datiem, kā arī uz to labošanu, dzēšanu vai bloķēšanu. Ja šo tiesību īstenošanu atsaka uz pārliecinoša pamata, datu subjektam ir jābūt tiesībām vērsties ar sūdzību kompetentajā valsts uzraudzības iestādē un/vai tiesā. Ja personai tiek nodarīts kaitējums sakarā ar valsts tiesību aktu, ar kuriem īsteno Datu aizsardzības pamatlēmumu, prasību pārkāpumu, šai personai ir tiesības saņemt atlīdzību no pārziņa.[257] Parasti datu subjektiem ir jābūt piekļuvei tiesiskās aizsardzības līdzeklim pret jebkuru viņu tiesību, ko garantē valsts tiesību akti, ar kuriem īsteno Datu aizsardzības pamatlēmumu, aizskārumu.[258]

Eiropas Komisija ierosināja reformu, kura ietver Vispārīgo datu aizsardzības regulu[259] un Vispārīgo datu aizsardzības direktīvu.[260] Šī jaunā direktīva aizstās pašreizējo Datu aizsardzības pamatlēmumu un piemēros vispārīgus principus un normas policijas un tiesu iestāžu sadarbībai krimināllietās.

257 Turpat, 19. pants.

258 Turpat, 20. pants.

259 Eiropas Komisija (2012), *Priekšlikums Eiropas Parlamenta un Padomes Regulai par personu aizsardzību attiecībā uz personas datu apstrādi un par šādu datu brīvu apriti (Vispārīgā datu aizsardzības regula)*, COM(2012) 11 final, Briselē, 2012. gada 25. janvārī.

260 Eiropas Komisija (2012), *Priekšlikums Eiropas Parlamenta un Padomes direktīvai 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 (Vispārīgā datu aizsardzības direktīva)*, COM(2012) 10 final, Briselē, 2012. gada 25. janvārī.

7.2.2. Specifiskāki juridiskie instrumenti par datu aizsardzību policijas un tiesībaizsardzības iestāžu pārrobežu sadarbībā

Papildus Datu aizsardzības pamatlēmumam dalībvalstu rīcībā noteiktās jomās esošo datu apmaiņu regulē vairāki juridiskie instrumenti, piemēram, Padomes Pamatlēmums 2009/315/TI par organizatoriskiem pasākumiem un saturu no sodāmības reģistra iegūtas informācijas apmaiņai starp dalībvalstīm un Padomes lēmums par sadarbības pasākumiem starp dalībvalstu finanšu ziņu vākšanas vienībām attiecībā uz informācijas apmaiņu.[261]

Ļoti svarīgi ir tas, ka kompetento iestāžu pārrobežu sadarbība[262] arvien vairāk ietver imigrācijas datu apmaiņu. Šī tiesību joma neietilpst policijas un krimināltiesību lietās, bet daudzos aspektos ir būtiska policijas un tiesu iestāžu darbam. Tas pats attiecas uz datiem par precēm, ko ieved vai izved no ES. Iekšējo ES robežkontroļu atcelšana ir palielinājusi krāpšanas risku, liekot dalībvalstīm intensificēt sadarbību, jo īpaši pastiprinot pārrobežu informācijas apmaiņu, lai efektīvāk atklātu valstu un ES muitas tiesību pārkāpumus un sauktu pie atbildības par tiem.

Prīmes lēmums

Svarīgs institucionalizētas pārrobežu sadarbības, ko īsteno, veicot valstu rīcībā esošu datu apmaiņu, piemērs ir Padomes Lēmums 2008/615/TI par pārrobežu sadarbības pastiprināšanu, jo īpaši apkarojot terorismu un pārrobežu noziedzību (Prīmes lēmums), kas ietvēra Prīmes lēmumu ES tiesībās 2008. gadā.[263] Prīmes lēmums bija

261 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.

262 Eiropas Komisija (2012), Komisijas Paziņojums Eiropas Parlamentam un Padomei – Tiesībaizsardzības iestāžu sadarbības stiprināšana ES: Eiropas Informācijas apmaiņas modelis (*EIXM*), COM(2012) 735 final, Briselē, 2012. gada 7. decembrī

263 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.

starptautisks policijas sadarbības līgums, ko 2005. gadā parakstīja Austrija, Beļģija, Francija, Luksemburga, Nīderlande, Spānija un Vācija.[264]

Prīmes lēmuma mērķis ir palīdzēt dalībvalstīm uzlabot informācijas koplietošanu nolūkā novērst un apkarot noziedzību trīs jomās: terorismu, pārrobežu noziedzību un nelegālo migrāciju. Šajā nolūkā lēmumā ir paredzēti noteikumi attiecībā uz:

- automatizētu piekļuvi DNS profiliem, pirkstu nospiedumu datiem un noteiktiem valstu transportlīdzekļu reģistrācijas datiem;
- datu piegādi saistībā ar lieliem notikumiem, kuriem ir pārrobežu apmērs;
- informācijas piegādi, lai novērstu teroristu nodarījumus;
- citiem pasākumiem, lai pastiprinātu pārrobežu policijas sadarbību.

Datu bāzes, kuras tiek darītas pieejamas saskaņā ar Prīmes lēmumu, pilnībā pārvalda valsts tiesību akti, bet datu apmaiņu papildus regulē lēmums un vēlāk pieņemtais Datu aizsardzības pamatlēmums. Par šādu datu plūsmu uzraudzību kompetentās iestādes ir valstu datu aizsardzības uzraudzības iestādes.

7.2.3. Datu aizsardzība *Europol* [Eiropolā] un *Eurojust* [Eirojustā]

Europol

Europol, ES tiesībaizsardzības aģentūras galvenais birojs atrodas Hāgā, bet *Europol* valstu vienības (*ENU*) – katrā dalībvalstī. *Europol* tika izveidots 1998. gadā; tā pašreizējais juridiskais ES iestādes statuss pamatojas uz Padomes lēmumu, ar ko izveido Eiropas Policijas biroju (*Europol lēmums*).[265] *Europol* darbības mērķis ir palī-

264 Līgums, 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; pieejams tīmekļa vietnē: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

265 Eiropas Savienības Padome (2009), Padomes 2009. gada 6. aprīļa Lēmums, ar ko izveido Eiropas Policijas biroju (*Europol*), OV 2009 L 121. Sk. arī Komisijas priekšlikumu regulai, kas tādējādi paredz jauna *Europol* tiesisko regulējumu, kas seko un aizstāj *Europol*, kas izveidots ar Padomes 2009. gada 6. aprīļa Lēmumu, ar ko izveido Eiropas Policijas biroju (*Europol*), un *CEPOL*, kas izveidota ar Padomes Lēmumu 2005/681/TI, ar ko izveido Eiropas Policijas akadēmiju (*CEPOL*), COM(2013) 173 final.

dzēt novērst un izmeklēt organizēto noziedzību, terorismu un citus smagu noziegumu veidus, kā uzskaitīts *Europol* lēmuma pielikumā, kas skar divas vai vairāk dalībvalstis.

Lai sasniegtu savus mērķus, *Europol* ir izveidojis *Europol* Informācijas sistēmu, kas nodrošina dalībvalstīm datu bāzi kriminālās izlūkinformācijas un informācijas caur savām *ENU* apmaiņai. *Europol* Informācijas sistēmu var izmantot, lai darītu pieejamus datus par personām, kuras tur aizdomās vai kuras ir notiesātas par *Europol* kompetencē esošiem noziedzīgiem nodarījumiem; vai personām, par kurām ir faktiskas norādes, ka tās izdarīs šādus nodarījumus. *Europol* un *ENU* var ievadīt datus tieši *Europol* Informācijas sistēmā un izgūt datus no tās. Tikai tā persona, kas ievadīja datus sistēmā, var tos grozīt, labot vai dzēst.

Kad nepieciešams *Europol* uzdevumu izpildei, tas var uzglabāt, grozīt un izmantot datus par noziedzīgiem nodarījumiem analīzes darba datnēs. Analīzes darba datnes ir atvērtas nolūkā apkopot, apstrādāt vai izmantot datus, lai palīdzētu konkrētām krimināLizmeklēšanām, ko veic *Europol* kopā ar ES dalībvalstīm.

Reaģējot uz jaunākajiem notikumiem, 2013. gada 1. janvārī tika izveidots Eiropas Kibernoziedzības centrs.[266] Šis centrs darbojas kā ES informācijas par kibernoziedzību centrmezgls, veicinot ātrāku reakciju uz tiešsaistes noziegumu gadījumā, izstrādājot un izvietojot digitālos tiesu ekspertīzes līdzekļus un nodrošinot labāko praksi kibernoziedzības izmeklēšanai. Centrs koncentrējas uz kibernoziedzību:

- kuru veic organizētas grupas, lai radītu lielus noziedzīgus ieņēmumus, kā krāpšana tiešsaistē;
- kura rada nopietnu kaitējumu upurim, kā bērnu seksuāla izmantošana tiešsaistē;
- kura skar kritisko infrastruktūru un informācijas sistēmas Savienībā.

Tiek pastiprināts datu aizsardzības režīms, kas regulē *Europol* darbības. *Europol* lēmuma 27. pantā ir noteikts, ka jāpiemēro 108. konvencijā un Ieteikumā par policijas datiem noteiktie principi attiecībā uz automatizētu un neautomatizētu datu apstrādi. Datu nodošanai starp *Europol* un dalībvalstīm arī ir jāatbilst normām, kas ietvertas Datu aizsardzības pamatlēmumā.

266 Sk. arī EDAU (2012), *Datu aizsardzības uzraudzītāja atzinums par Eiropas Komisijas Paziņojumu Padomei un Eiropas Parlamentam par Eiropas Kibernoziedzības centra izveidi*, Briselē, 2012. gada 29. jūnijā.

Lai nodrošinātu atbilstību piemērojamajiem datu aizsardzības tiesību aktiem un, jo īpaši, to, ka personas datu apstrāde neaizskar personas tiesības, neatkarīgā Europol Apvienotā uzraudzības iestāde (AUI) pārskata un uzrauga *Europol* darbības.[267] Katrai personai ir tiesības piekļūt jebkuriem personas datiem, kas par attiecīgo personu var būt *Europol* rīcībā, kā arī ir tiesības lūgt, lai šos datus pārbauda, labo vai dzēš. Ja persona nav apmierināta ar *Europol* lēmumu attiecībā uz šo tiesību īstenošanu, viņš vai viņa var iesniegt apelācijas sūdzību AUI Apelāciju komitejā.

Ja kaitējums tiek nodarīts tā rezultātā, ka *Europol* uzglabātajos vai apstrādātajos datos ir juridiskas vai faktiskas kļūdas, cietusī persona var lūgt kaitējuma atlīdzināšanu tikai tās dalībvalsts kompetentajā tiesā, kurā iestājās notikums, kurš radīja kaitējumu.[268] *Europol* atlīdzinās zaudējumus dalībvalstij, ja kaitējums radies tāpēc, ka *Europol* nav izpildījis savus juridiskos pienākumus.

Eurojust

2002. gadā izveidotais *Eurojust* ir ES struktūra, ar galveno biroju Hāgā, kas veicina tiesu iestāžu sadarbību izmeklēšanās un apsūdzību izvirzīšanā par smagiem noziegumiem, kuri skar vismaz divas dalībvalstis.[269] *Eurojust* kompetencē ir:

- stimulēt un uzlabot izmeklēšanu un apsūdzības izvirzīšanu saskaņošanu starp dažādu dalībvalstu kompetentajām iestādēm;

- atvieglot pieprasījumu un lēmumu izpildi saistībā ar tiesu iestāžu sadarbību.

Eurojust funkcijas pilda valstu dalībnieki. Katra dalībvalsts deleģē uz *Eurojust* vienu tiesnesi vai prokuroru, kura statusu regulē valsts tiesību akti un kuram ir nodotas vajadzīgās pilnvaras, lai viņš/viņa varētu veikt uzdevumus, kas vajadzīgi tiesu iestāžu sadarbības stimulēšanai un uzlabošanai. Papildus, valstu dalībnieki rīkojas kopīgi kā kolēģija, lai pildītu īpašus *Eurojust* uzdevumus.

267 *Europol* lēmums, 34. pants.

268 Turpat, 52. pants.

269 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 lēmumi*).

Eurojust var apstrādāt personas datus tiktāl, ciktāl tas nepieciešams tā mērķu sasniegšanai. Tas tomēr ir ierobežots līdz specifiskai informācijai par personām, kuras tiek turētas aizdomās par dalību *Eurojust* kompetencē esošā noziedzīgā nodarījumā, vai par tiesājamību par tādu nodarījumu. *Eurojust* var arī apstrādāt noteiktu informāciju attiecībā uz *Eurojust* kompetencē esošu noziedzīgu nodarījumu liecinieki vai upuriem.[270] Ārkārtas apstākļos *Eurojust* ierobežotu laika posmu var apstrādāt plašākus personas datus saistībā ar kāda pārkāpuma apstākļiem, ja tādi dati ir tūlīt būtiski notiekošai izmeklēšanai. Savas kompetences ietvaros *Eurojust* var sadarboties ar citām ES iestādēm, struktūrām un aģentūrām, un veikt ar tām datu apmaiņu. *Eurojust* var arī sadarboties un veikt personas datu apmaiņu ar trešām valstīm un organizācijām.

Saistībā ar datu aizsardzību *Eurojust* jāgarantē tāds aizsardzības līmenis, kas ir vismaz līdzvērtīgs Eiropas Padomes 108. konvencijā un tās turpmākajos grozījumos noteiktajiem principiem. Datu apmaiņas gadījumā jāievēro īpašas normas un ierobežojumi, ko īsteno vai nu ar sadarbības nolīgumu vai darba vienošanos saskaņā ar *Eurojust* Padomes lēmumiem un *Eurojust* Datu aizsardzības normām.[271]

Eurojust iestādē ir izveidota neatkarīga AUI, kuras uzdevums ir pārraudzīt *Eurojust* veikto personas datu apstrādi. Personas var iesniegt sūdzību AUI, ja tās neapmierina *Eurojust* atbilde uz lūgumu par piekļuvi personas datiem, par to labošanu, bloķēšanu vai dzēšanu. Ja *Eurojust* nelikumīgi apstrādā personas datus, *Eurojust* par jebkuru datu subjektam nodarīto kaitējumu būs atbildīga saskaņā ar tās dalībvalsts tiesību aktiem, kurā atrodas tās galvenais birojs, proti, Nīderlandes [tiesību aktiem].

7.2.4. Datu aizsardzība kopīgajās informācijas sistēmās ES mērogā

Papildus datu apmaiņai dalībvalstu starpā un speciālu ES iestāžu izveidei, lai apkarotu pārrobežu noziedzību, ES mērogā ir izveidotas vairākas kopīgas informācijas sistēmas, lai tās kalpotu kā platformas datu apmaiņai kompetento valstu un ES iestāžu starpā konkrētiem tiesībaizsardzības – tostarp imigrācijas tiesību aktu un muitas tiesību aktu aizsardzības – nolūkiem. Dažas no minētajām sistēmām tika izstrādātas uz daudzpusēju nolīgumu pamata, ko vēlāk papildināja ES juridiskie instrumenti

270 Padomes Lēmuma 2002/187/TI, kas grozīts ar Padomes Lēmumu 2003/659/TI un ar Padomes Lēmumu 2009/426/TI, konsolidētā versija, 15. panta 2. punkts.

271 *Eurojust* 2005. gada 19. marta personas datu apstrādes un aizsardzības reglaments, OV 2005 C 68/01, 1. lpp.

un sistēmas, kā Šengenas informācijas sistēma, Vīzu informācijas sistēma, *Eurodac*, *Eurosur* vai Muitas informācijas sistēma.

2012. gadā izveidotā Eiropas Aģentūra lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*)[272] atbild par otrās paaudzes Šengenas informācijas sistēmas (*SIS II*), Vīzu informācijas sistēmas (*VIS*) un *Eurodac* ilgtermiņa operatīvo pārvaldību. *eu-LISA* pamatuzdevums ir nodrošināt informācijas tehnoloģiju sistēmu efektīvu, drošu un ilgstošu darbību. Tā arī atbild par vajadzīgo pasākumu veikšanu, lai nodrošinātu sistēmu un datu drošību.

Šengenas informācijas sistēma

1985. gadā vairākas agrāko Eiropas Kopienu dalībvalstis noslēdza Nolīgumu starp Beniluksa Ekonomikas savienības valstīm, Vācijas Federatīvo Republiku un Francijas Republiku par pakāpenisku kontroles atcelšanu pie kopīgām robežām (*Šengenas Nolīgums*), cenšoties izveidot personu brīvas pārvietošanās teritoriju, ko nekavētu robežkontroles Šengenas teritorijā.[273] Lai radītu pretsparu sabiedriskās drošības apdraudējumam, kas varēja rasties no atvērtām robežām, tika izveidotas pastiprinātas kontroles pie Šengenas ārējām robežām, kā arī tika izveidota cieša sadarbība starp valstu policijas un tiesu iestādēm.

Kā sekas tam, ka Šengenas Nolīgumam pievienojās papildu valstis, Šengenas sistēma ar Amsterdamas Līgumu beidzot tika integrēta ES tiesiskajā regulējumā.[274] Šis lēmums tika īstenots 1999. gadā. Jaunākā Šengenas informācijas sistēmas versija, tā dēvētā *SIS II*, sāka darboties 2013. gada 9. aprīlī. Tagad tā apkalpo visas ES dalībvalstis, kā arī Islandi [Īslandi], Lihtenšteinu, Norvēģiju un Šveici.[275] *Europol* un *Eurojust* arī ir pieeja *SIS II*.

272 Eiropas Parlamenta un Padomes 2011. gada 25. oktobra Regula (ES) Nr. 1077/2011, ar ko izveido Eiropas Aģentūru lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā, OV 2011 L 286.

273 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.

274 Eiropas Kopienas (1997), Amsterdamas Līgums, ar ko groza Līgumu par Eiropas Savienību, Eiropas Kopienu dibināšanas līgumi un daži saistītie akti, OV 1997 C 340.

275 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, 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, OV 2007 L 205.

SIS II sastāvā ietilpst centrālā sistēma (*C-SIS*), valsts sistēma (*N-SIS*) katrā dalībvalstī un komunikācijas infrastruktūra starp centrālo sistēmu un valstu sistēmām. *C-SIS* satur noteiktus datus, ko dalībvalstis ievadījušas par personām un priekšmetiem. *C-SIS* sistēmu izmanto valstu robežkontroles, policijas, muitas, vīzu un tiesu iestādes visā Šengenas zonā. Katra dalībvalsts darbina *C-SIS* nacionālo kopiju, zināmu kā Valstu Šengenas informācijas sistēmas (*N-SIS*), ko pastāvīgi atjaunina, tādējādi atjauninot arī *C-SIS*. *N-SIS* sistēmu skatās un trauksmi izsludina gadījumos, kad:

- personai nav tiesību ieceļot vai uzturēties Šengenas teritorijā; vai
- personu vai priekšmetu meklē tiesu vai tiesībaizsardzības iestādes; vai
- persona ir izsludināta par pazudušu; vai
- preces – piemēram, banknotes, mašīnas, furgoni, šaujamieroči un identitātes dokumenti – ir izsludinātas par pazudušu vai nozagtu īpašumu.

Brīdinājuma gadījumā ar Valstu Šengenas informācijas sistēmu starpniecību sāk kontroles procedūras.

SIS II ir jaunas funkcionālās iespējas, piemēram, iespēja ievadīt: biometriskos datus, piemēram, pirkstu nospiedumus un fotogrāfijas; vai jaunas brīdinājumu kategorijas, piemēram, nozagtas laivas, gaisa kuģus, konteinerus vai maksāšanas līdzekļus; un pastiprināti brīdinājumi par personām un priekšmetiem; Eiropas apcietināšanas orderu (*EAW*) par personām, kuras meklē, lai apcietinātu, nodotu vai izdotu, kopijas.

Padomes Lēmums 2007/533/TI par otrās paaudzes Šengenas Informācijas sistēmas (*SIS II*) izveidi, darbību un izmantošanu (Šengenas II lēmums) ietver 108. konvenciju: „Personas datus, kas apstrādāti, piemērojot šo lēmumu, aizsargā saskaņā ar Eiropas Padomes 108. konvenciju".[276] Ja valsts policijas iestādes izmanto personas datus, piemērojot Šengenas II lēmumu, valsts tiesību aktos ir jāīsteno 108. konvencijas noteikumi, kā arī Ieteikums par policijas datiem.

Kompetentā valsts uzraudzības iestāde katrā dalībvalstī uzrauga savas valsts *N-SIS*. Jo īpaši, tai jāpārbauda to datu kvalitāte, ko dalībvalsts ievada *C-SIS* sistēmā ar *N-SIS* sistēmu starpniecību. Valsts uzraudzības iestādei jānodrošina, ka vismaz reizi četros

276 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, OV 2007 L 205, 57. pants.

gados notiek datu apstrādes darbību valsts *N-SIS* sistēmā revīzija. Valsts uzraudzības iestādes un EDAU sadarbojas un nodrošina saskaņotu *SIS* uzraudzību, kamēr EDAU atbild par *C-SIS* sistēmas uzraudzību. Caurskatāmības labad reizi divos gados Eiropas Parlamentam, Padomei un *eu-LISA* nosūta kopīgu pārskatu par veiktajām darbībām.

Personu piekļuves tiesības saistībā ar *SIS II* var īstenot ikvienā dalībvalstī, jo katra *N-SIS* ir precīza *C-SIS* kopija.

Piemērs: Lietā *Dalea pret Franciju*[277] prasītājam bija atteikta vīza Francijas apmeklējumam, jo Francijas iestādes bija ziņojušas Šengenas informācijas sistēmai, ka viņam ieceļošana jāatsaka. Prasītājs neveiksmīgi lūdza piekļuvi datiem un to labošanu vai dzēšanu vispirms Francijas Datu aizsardzības komisijā un pēc tam Valsts Padomē. ECT uzskatīja, ka datu par prasītāju paziņošana Šengenas informācijas sistēmai ir bijusi saskaņā ar tiesību aktiem un ir centusies panākt likumīgo valsts drošības aizsardzības mērķi. Tā kā prasītājs nepierādīja, kā tieši atteikuma ieceļot Šengenas zonā dēļ viņam ir nodarīts kaitējums, un tā kā bija veikti pietiekami pasākumi, lai pasargātu viņu no patvaļīgiem lēmumiem, viņa tiesību uz privāto dzīvi aizskārums bija bijis samērīgs. Tāpēc prasītāja sūdzību saskaņā ar 8. pantu atzina par nepieņemamu.

Vīzu informācijas sistēma

Vīzu informācijas sistēma (*VIS*), ko darbina arī *eu-LISA*, tika izstrādāta, lai atbalstītu kopīgas ES vīzu politikas īstenošanu.[278] *VIS* atļauj dalībvalstīm veikt vīzu datu apmaiņu caur sistēmu, kas savieno Šengenas valstu konsulātus, kuri atrodas ārpus ES, ar visu Šengenas valstu ārējās robežas šķērsošanas punktiem. *VIS* apstrādā datus par īstermiņa vīzu pieteikumiem, kas iesniegti, lai apciemotu vai tranzītā šķērsotu Šengenas teritoriju. *VIS* dod iespēju robežas iestādēm ar biometrisko datu palīdzību pārbaudīt, vai persona, kura uzrāda vīzu, ir likumīga vīzas turētāja vai nē, un lai identificētu personas bez dokumentiem vai ar viltotiem dokumentiem.

277 ECT 2010. gada 2. februāra spriedums lietā *Dalea pret Franciju*, (dec.) prasības pieteikums Nr. 964/07.

278 Eiropas Savienības Padome (2004), Padomes 2004. gada 8. jūnija Lēmums, ar kuru 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 (*VIS* regula), OV 2008 L 218; 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.

Atbilstoši Eiropas Parlamenta un Padomes Regulai (EK) Nr. 767/2008 par Vīzu informācijas sistēmu (*VIS*) un datu apmaiņu starp dalībvalstīm saistībā ar īstermiņa vīzām (*VIS regula*) *VIS* drīkst reģistrēt tikai datus par pieteikuma iesniedzēju, viņa vai viņas vīzām, fotogrāfijas, pirkstu nospiedumus, saites ar agrākajiem pieteikumiem, kā arī pieteikuma iesniedzēju pavadošo personu pieteikuma datnes.[279] Piekļuve *VIS*, lai ievadītu, grozītu vai dzēstu datus, ir ierobežota un ir atļauta tikai dalībvalstu vīzu iestādēm, savukārt piekļuve datiem konsultācijas nolūkos ir atļauta vīzu iestādēm un iestādēm, kuru kompetencē ir pārbaudes ārējās robežas šķērsošanas punktos, imigrācijas pārbaudes un patvērums. Ar zināmiem nosacījumiem valstu kompetentās policijas iestādes un *Europol* var lūgt piekļuvi *VIS* ievadītajiem datiem, lai novērstu, atklātu un izmeklētu teroristu nodarījumus un noziedzīgus nodarījumus.[280]

Eurodac

Eurodac nosaukums attiecas uz daktilogrammām jeb pirkstu nospiedumiem. Tā ir centralizēta sistēma, kurā ietilpst dati par trešo valstu pilsoņu, kuri iesniedz patvēruma pieteikumu kādā no ES dalībvalstīm, pirkstu nospiedumiem.[281] Sistēma darbojas kopš 2003. gada janvāra, un tās mērķis ir palīdzēt noteikt dalībvalsti, kura ir atbildīga par īpašu patvēruma pieteikumu atbilstoši Padomes Regulai (EK) Nr. 343/2003, ar ko paredz kritērijus un mehānismus, lai noteiktu dalībvalsti, kura ir atbildīga par trešās valsts pilsoņa patvēruma pieteikuma izskatīšanu, kas iesniegts kādā no dalībvalstīm (*Dublinas II regula*).[282] *Eurodac* esošos personas datus var izmantot tikai tādiem nolūkiem, kas atvieglo Dublinas II regulas piemērošanu; par jebkuru citu izmantošanu tiks uzlikts sods.

Eurodac sastāv no centrālās vienības, ko darbina *eu-LISA*, pirkstu nospiedumu uzglabāšanai un salīdzināšanai, un no sistēmas elektroniskai datu nodošanai starp dalībvalstīm un centrālo datu bāzi. Dalībvalstis paņem un nodod katra vismaz 14 gadus

279 5. pants Eiropas Parlamenta un Padomes Regulā (EK) Nr. 767/2008 par Vīzu informācijas sistēmu (*VIS*) un datu apmaiņu starp dalībvalstīm saistībā ar īstermiņa vīzām (*VIS regula*), OV 2008 L 218.

280 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.

281 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*).

282 Padomes 2003. gada 18. februāra Regula (EK) Nr. 343/2003, ar ko paredz kritērijus un mehānismus, lai noteiktu dalībvalsti, kura ir atbildīga par trešās valsts pilsoņa patvēruma pieteikuma izskatīšanu, kas iesniegts kādā no dalībvalstīm, OV 2003 L 50 (*Dublinas II regula*).

veca trešās valsts pilsoņa vai bezvalstnieka, kurš lūdz patvērumu šo valstu teritorijā vai kurš ir aizturēts par nelikumīgu šo valstu ārējās robežas šķērsošanu, pirkstu nospiedumus. Dalībvalstis var arī paņemt un nodot trešo valstu pilsoņu vai bezvalstnieku, kuri atklāti uzturamies šo valstu teritorijā bez atļaujas, pirkstu nospiedumus.

Datus par pirkstu nospiedumiem *Eurodac* datu bāzē uzglabā tikai pseidonimizētā formā. Saskaņas gadījumā pseidonīmu kopā ar pirmās dalībvalsts, kura nodeva datus par pirkstu nospiedumiem, nosaukumu atklāj otrai dalībvalstij. Šī otrā dalībvalsts tad vēršas pie pirmās dalībvalsts, jo saskaņā ar Dublinas II regulu pirmā dalībvalsts ir atbildīga par patvēruma pieteikuma apstrādi.

Eurodac uzglabātie personas dati, kas attiecas uz patvēruma pieteikumu iesniedzējiem, tiek turēti 10 gadus pēc pirkstu nospiedumu paņemšanas dienas, izņemot gadījumus, kad datu subjekts iegūst kādas ES dalībvalsts pilsonību. Šādā gadījumā dati ir tūlīt jādzēš. Datus par ārvalstu pilsoņiem, kuri aizturēti par neatļautu ārējās robežas šķērsošanu, saglabā divus gadus. Šie dati ir jādzēš tūlīt, ja datu subjekts saņem uzturēšanās atļauju, pamet ES teritoriju vai iegūst kādas dalībvalsts pilsonību.

Papildus visām ES dalībvalstīm *Eurodac* uz starptautisku nolīgumu pamata piemēro arī Islande [Īslande], Norvēģija, Lihtenšteina un Šveice.

Eurosur

Eiropas Robežu uzraudzības sistēma (*Eurosur*)[283] ir izstrādāta tā, lai pastiprinātu Šengenas ārējo robežu kontroli, atklājot, novēršot un apkarojot nelegālo imigrāciju un pārrobežu noziedzību. Tā noder, lai pastiprinātu informācijas apmaiņu un operatīvo sadarbību starp valstu koordinācijas centriem un *Frontex* – ES aģentūru, kas atbild par jaunas integrētās robežu pārvaldības koncepcijas izstrādi un piemērošanu.[284] Tās galvenie mērķi ir šādi:

- samazināt nelegālo migrantu skaitu, kuri neatklāti iekļūst Savienībā;
- samazināt nelegālo migrantu nāves gadījumu skaitu, glābjot vairāk dzīvību jūrā;

283 Eiropas Parlamenta un Padomes Regula (ES) Nr. 1052/2013, ar ko izveido Eiropas Robežu uzraudzības sistēmu (*Eurosur*), OV 2013 L 295.

284 Eiropas Parlamenta un Padomes 2011. gada 25. oktobra Regula (ES) Nr. 1168/2011, ar kuru groza Padomes Regulu (EK) Nr. 2007/2004, ar ko izveido Eiropas Aģentūru operatīvās sadarbības vadībai pie Eiropas Savienības dalībvalstu ārējām robežām, OV 2011 L 394 (*Frontex regula*).

- palielināt ES iekšējo drošību kopumā, veicinot pārrobežu noziedzības novēršanu.[285]

Tā sāka darboties 2013. gada 2. decembrī visās dalībvalstīs ar ārējām robežām, un no 2014. gada 1. decembra sāks darboties pārējās. Šo regulu piemēros dalībvalstu sauszemes, ārējo jūras robežu un gaisa robežu uzraudzībai.

Muitas informācijas sistēma

Vēl viena svarīga kopīga informācijas sistēma, kas izveidota ES mērogā, ir Muitas informācijas sistēma (*CIS*).[286] Iekšējā tirgus izveides gaitā tika atceltas visas pārbaudes un formalitātes attiecībā uz precēm, ko pārvadā ES teritorijā, un tas noveda pie paaugstināta krāpšanas riska. Šo risku līdzsvaroja intensificēta sadarbība starp dalībvalstu muitas pārvaldēm. *CIS* nolūks ir palīdzēt dalībvalstīm novērst un izmeklēt smagus valstu un ES muitas un lauksaimniecības tiesību aktu pārkāpumus, kā arī saukt pie atbildības par tiem.

CIS iekļautā informācija ietver personas datus par aizturētām, arestētām vai konfiscētām izejvielām, transporta līdzekļiem, darījumiem, personām, precēm un skaidru naudu. Šo informāciju drīkst izmantot tikai, lai veiktu apskates, sniegtu ziņojumus vai veiktu īpašas inspekcijas, vai stratēģiskajai vai operatīvajai analīzei attiecībā uz personām, kuras tur aizdomās par muitas noteikumu pārkāpšanu.

Piekļuve *CIS* tiek piešķirta valstu muitas, nodokļu, lauksaimniecības, sabiedrības veselības un policijas iestādēm, kā arī *Europol* un *Eurojust*.

Personas datu apstrādei jāatbilst īpašajām normām, kas noteiktas *CIS* Konvencijā,[287] kā arī noteikumiem, kas paredzēti Datu aizsardzības direktīvā, Regulā par aizsardzību

285 Sk. arī: Eiropas Komisija (2008), Komisijas Paziņojumu Eiropas Parlamentam un Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai – Eiropas Robežu uzraudzības sistēmas (*Eurosur*) izveidošanas izpēte, COM(2008) 68 final, Briselē, 2008. gada 13. februārī; Eiropas Komisija (2011), Ietekmes novērtējums, kas pievienots priekšlikumam Eiropas Parlamenta un Padomes regulai, ar ko izveido Eiropas Robežu uzraudzības sistēmu (*Eurosur*), personāla darba dokuments, SEC(2011) 1536 final, Briselē, 2011. gada 12. decembrī, 18. lpp.

286 Eiropas Savienības Padome (1995), Padomes 1995. gada 26. jūlija akts, ar ko sagatavo Konvenciju par informācijas tehnoloģiju izmantošanu muitas vajadzībām, OV 1995 C 316, grozīts ar Eiropas Savienības Padome (2009), 1997. gada 13. marta Regula Nr. 515/97 par dalībvalstu pārvaldes iestāžu savstarpēju palīdzību un šo iestāžu un Komisijas sadarbība, lai nodrošinātu muitas un lauksaimniecibas tiesību aktu pareizu piemērošanu; Padomes 2009. gada 30. novembra Lēmumu 2009/917/TI par informācijas tehnoloģiju izmantošanu muitas vajadzībām, OV 2009 L 323 (*CIS lēmums*).

287 Turpat.

attiecībā uz personas datu apstrādi ES iestādēs, 108. konvencijā un Ieteikumā par policijas datiem. EDAS ir atbildīga uzraudzīt CIS atbilstību Regulai (EK) Nr. 45/2001, un vismaz reizi gadā sasauc uz sanāksmi valstu datu aizsardzības uzraudzības iestādes kuras ir kompetentas ar CIS saistītajos uzraudzības jautājumos.

8

Citi specifiski Eiropas tiesību akti datu aizsardzības jomās

ES	Aplūkotie jautājumi	EP
Datu aizsardzības direktīva E-privātuma direktīva	**Elektroniskā komunikācija**	108. konvencija Ieteikums par telekomunikāciju pakalpojumiem
Datu aizsardzības direktīva, 8. panta 2. punkta b) apakšpunkts	**Nodarbināšanas attiecības**	108. konvencija Ieteikums par nodarbināšanu
		ECT 2007. gada 3. aprīļa spriedums lietā *Copland pret Apvienoto Karalisti*, prasības pieteikums Nr. 62617/00
Datu aizsardzības direktīva, 8. panta 3. punkts	**Medicīniskie dati**	108. konvencija Ieteikums par medicīniskajiem datiem
		ECT 1997. gada 25. februāra spriedums lietā *Z. pret Somiju, prasības pieteikums* Nr. 22009/93
Klīnisko izmēģinājumu direktīva	**Klīniskie izmēģinājumi**	
Datu aizsardzības direktīva, 6. panta 1. punkta b) un e) apakšpunkts, 13. panta 2. punkts	**Statistika**	108. konvencija Ieteikums par statistikas datiem

ES	Aplūkotie jautājumi	EP
Regula (EK) Nr. 223/2009 par Eiropas statistiku Tiesas 2008. gada 16. decembra spriedums lietā C-524/06 *Huber pret Vāciju*	**Oficiālā statistika**	108. konvencija Ieteikums par statistikas datiem
Direktīva 2004/39/EK, kas attiecas uz finanšu instrumentu tirgiem Regula (ES) Nr. 648/2012 par ārpusbiržas atvasinātajiem instrumentiem, centrālajiem darījumu partneriem un darījumu reģistriem Regula (ES) Nr. 1060/2009 par kredītreitingu aģentūrām Direktīva 2007/64/EK par maksājumu pakalpojumiem iekšējā tirgū	**Finanšu dati**	108. konvencija Ieteikums 90(19), ko izmanto maksājumiem un citām saistītām darbībām ECT 2012. gada 6. decembra spriedums lietā *Michaud pret Franciju*, prasības pieteikums Nr. 12323/11

Vairākos gadījumos Eiropas līmenī ir pieņemti īpaši juridiskie instrumenti, kas detalizētāk piemēro 108. konvencijas vai datu aizsardzības direktīvas vispārīgās normas specifiskām situācijām.

8.1. Elektroniskā komunikācija

Galvenie punkti

- Specifiskas datu aizsardzības normas telekomunikāciju jomā, ar īpašu atsauci uz telefona pakalpojumiem, ir ietvertas EP 1995. gada ieteikumā.
- Personas datu apstrāde saistībā ar komunikāciju pakalpojumu sniegšanu ES mērogā regulē e-privātuma direktīva.
- Elektronisko komunikāciju konfidencialitāte attiecas ne tikai uz komunikācijas saturu, bet arī uz noslodzes datiem, kā informācija par to, kurš ar kuru, kad un cik ilgi ir komunicējis, un atrašanās vietas dati, kā informācija par to, no kurienes dati tika paziņoti.

Komunikāciju tīkliem ir pastiprināts potenciāls neattaisnoti iejaukties lietotāju personīgajā sfērā, jo šādi tīkli dod papildu tehniskas iespējas noklausīties un izpētīt tajos veiktu komunikāciju. Līdz ar to uzskatīja par nepieciešamiem īpašus datu aizsardzības regulējumus, lai mazinātu īpašus riskus komunikāciju pakalpojumu lietotājiem.

1995. gadā EP izdeva Ieteikumu par datu aizsardzību telekomunikāciju jomā, ar īpašu atsauci uz telefona pakalpojumiem.[288] Atbilstoši šim ieteikumam personas datu vākšanas un apstrādes nolūks telekomunikāciju kontekstā ir jāierobežo līdz šādiem: savienot lietotāju ar tīklu, darīt pieejamu kādu konkrētu telekomunikāciju pakalpojumu, izrakstīt rēķinu, veikt pārbaudes, nodrošināt optimālu tehnisko darbību un attīstīt tīklu un pakalpojumu.

Īpaša uzmanība tika pievērsta arī tam, kā telekomunikāciju tīklus izmanto tiešās tirgvedības sūtījumu nosūtīšanai. Parasti tiešās tirgvedības sūtījumus nedrīkst sūtīt abonentam, kurš ir konkrēti atteicies no iespējas saņemt reklāmas sūtījumus. Automatizētas zvanīšanas ierīces iepriekš ierakstītu reklāmas sūtījumu nodošanai drīkst izmantot tikai tad, ja abonents ir devis konkrētu piekrišana. Valsts tiesību aktos šajā jomā ir jāparedz sīki izstrādātas normas.

Kas attiecas uz **ES tiesisko regulējumu,** pēc pirmā mēģinājuma 1997. gadā 2002. gadā tika pieņemta un 2009. gadā – grozīta Direktīva par privāto dzīvi un elektronisko komunikāciju (*e-privātuma direktīva*), lai papildinātu un konkretizētu datu aizsardzības direktīvas noteikumus telekomunikāciju nozarē.[289] E-privātuma direktīvas piemērošana ir ierobežota un attiecas tikai uz komunikāciju pakalpojumiem publiskajos elektroniskajos tīklos.

E-privātuma direktīva nošķir trīs galvenās datu kategorijas, kas rodas komunikācijas gaitā:

- dati, kuri veido komunikācijas laikā nosūtīto sūtījumu saturu; šie dati ir stingri konfidenciāli;

- dati, kas nepieciešami komunikācijas izveidei un uzturēšanai, tā sauktie noslodzes dati, piemēram, informācija par komunikācijas partneriem, komunikācijas laiku un ilgumu;

288 EP, Ministru komiteja (1995), Ieteikums Rec(95)4 dalībvalstīm par personas datu aizsardzību telekomunikāciju jomā, ar īpašu atsauci uz telefona pakalpojumiem, 1995. gada 7. februārī.

289 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*), kas grozīta ar Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīvu 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.

- noslodzes datos ir dati, kuri konkrēti attiecas uz komunikācijas ierīces atrašanās vietu, tā sauktie atrašanās vietas dati; šie dati vienlaikus ir dati par komunikācijas ierīču *lietotāju* atrašanās vietu, un ir īpaši svarīgi saistībā ar mobilo komunikācijas ierīču lietotājiem.

Pakalpojuma sniedzējs noslodzes datus var izmantot tikai, lai izrakstītu rēķinus un sniegtu pakalpojuma tehnisko nodrošinājumu. Tomēr ar datu subjekta piekrišanu šos datus var atklāt citiem pārziņiem, kuri piedāvā pievienotās vērtības pakalpojumus, piemēram, sniedz informāciju saistībā ar lietotāja atrašanās vietu, par tuvāko metro staciju vai aptieku vai laika prognozi šai atrašanās vietai.

Citai piekļuvei datiem par komunikāciju elektroniskajos tīklos, kā piekļuvei noziegumu izmeklēšanas nolūkos, atbilstoši e-privātuma direktīvas 15. pantam ir jāatbilst prasībām par tiesību uz datu aizsardzību, kuras noteiktas ECK 8. panta 2. punktā un apstiprinātas Hartas 8. un 52. pantā, pamatotu aizskārumu.

2009. gada grozījumi e-privātuma direktīvā[290] ievieš šādus:

- Ierobežojumi e-pastu nosūtīšanai tiešās tirgvedības nolūkos tika attiecināti arī uz īsziņu nosūtīšanas pakalpojumiem (SMS), multivides ziņojumu pakalpojumiem (MMS) un citiem tamlīdzīgu lietojumu veidiem; tirgvedības e-pasti ir aizliegti, ja nav saņemta iepriekšēja piekrišana. Bez šādas piekrišanas ar tirgvedības e-pastiem var vērsties tikai pie agrākajiem klientiem, ja viņi ir darījuši pieejamu savu e-pasta adresi un neiebilst.

- Dalībvalstīm tika noteikts pienākums nodrošināt tiesiskās aizsardzības līdzekļus pret nevēlamu komunikāciju aizlieguma pārkāpumiem.[291]

- Iestatīt sīkdatnes – programmatūru, kas pārrauga un reģistrē datora lietotāja darbības, vairs nav atļauts bez datora lietotāja piekrišanas. Valsts tiesību aktos ir sīkāk jāregulē tas, kā izteikt un saņemt piekrišanu, lai piedāvātu pietiekamu aizsardzību.[292]

290 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.

291 Sk. grozīto direktīvu, 13. pants.

292 Sk. turpat, 5. pants; sk. arī 29. panta darba grupa (2012), *Atzinums 04/2012 par atbrīvojumu piekrišanai par sīkdatnēm*, WP 194, Briselē, 2012. gada 7. jūnijs.

Ja datu aizsardzības pārkāpums notiek nesankcionētas piekļuves datiem, datu pazaudēšanas vai iznīcināšanas dēļ, ir tūlīt jāinformē kompetentā uzraudzības iestāde. Abonentiem jābūt informētiem gadījumos, kad iespējamais kaitējums tiem nodarīts datu aizsardzības pārkāpumu dēļ.[293]

Datu saglabāšanas direktīvā[294] (2014. gada 8. aprīlī konstatēta par spēkā neesošu) bija noteikts pienākums komunikāciju pakalpojumu sniedzējiem turēt pieejamus noslodzes datus, jo īpaši smagu noziegumu apkarošanai, vismaz sešus mēnešus, bet ne ilgāk kā 24 mēnešus, neatkarīgi no tā, vai pakalpojuma sniedzējam šie dati joprojām bija vai vairs nebija vajadzīgi, lai izrakstītu rēķinus vai tehniski nodrošinātu pakalpojumu.

ES dalībvalstis ieceļ neatkarīgas valsts iestādes, kuras atbild par saglabāto datu drošības uzraudzīšanu.

Telekomunikāciju datu saglabāšana acīmredzami aizskar tiesības uz datu aizsardzību.[295] Par to, vai šāds aizskārums ir vai nav pamatots, šobrīd notiek vairākas tiesvedības ES dalībvalstīs[296].

Piemērs: Lietā *Digital Rights Ireland un Seitlinger in citi*, Tiesa konstatēja datu saglabāšanas direktīvu par spēkā neesošu. Tiesa atzina, ka "*direktīvas plaša apjoma un īpaši būtiska iejaukšanās šajās pamattiesībās...nav precīzi reglamentēta ar tiesību normām, kas ļautu nodrošināt, lai tā patiešām būtu ierobežota ar absolūti nepieciešamo.*"

Būtisks jautājums elektronisko komunikāciju jomā ir valsts iestāžu iejaukšanās. Komunikācijas uzraudzības vai pārtveršanas līdzekļi, kā noklausīšanās vai

293 Sk. arī 29. panta darba grupa (2011), *Darba dokuments 01/2011 par pašreizējo ES personas datu pārkāpumu regulējumu un ieteikumiem par nākotnes politikas attīstību*, WP 184, Briselē, 2011. gada 5. aprīlī.

294 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.

295 EDAU (2011), *2011. gada 31. maija Atzinums par Komisijas Novērtējuma ziņojumu Eiropas Parlamentam un Padomei par datu saglabāšanas direktīvu (Direktīva 2006/24/EK)*, 2011. gada 31. maijā.

296 Vācija, Federatīvā Konstitucionālā tiesa (*Bundesverfassungsgericht*), 1 BvR 256/08, 2010. gada 2. martā; Rumānija, Federālā Konstitucionālā tiesa (*Curtea Constituțională a României*), *Nr. 1258*, 2009. gada 8. oktobrī; Čehijas Republika, Konstitucionālā tiesa (*Ústavní soud České republiky*), *94/2011 Coll.*, 2011. gada 22. martā.

pārtveršanas ierīces, ir pieļaujami tikai tad, ja tas ir paredzēts tiesību aktos un ir nepieciešams pasākums demokrātiskā sabiedrībā, lai aizsargātu valsts drošību, sabiedrības drošību, valsts monetārās intereses vai apkarotu noziedzīgus nodarījumus; vai, lai aizsargātu datu subjektu vai citu personu tiesības un brīvības.

Piemērs: Lietā *Malone pret Apvienoto Karalisti*[297] prasītājam bija izvirzīta apsūdzība par vairākiem nodarījumiem saistībā ar negodīgu rīcību ar zagtām precēm. Viņa prāvas laikā atklājās, ka prasītāja telefona saruna bija pārtverta, pamatojoties uz orderi, ko bija izdevis Iekšlietu ministrijas valsts sekretārs. Lai gan veids, kādā prasītāja komunikācija bija pārtverta, bija likumīgs saskaņā ar valsts tiesību aktiem, ECT konstatēja, ka nav bijis juridisku normu par valsts iestādēm šajā jomā piešķirtās rīcības brīvības īstenošanas tvērumu un veidu, un ka iejaukšanās, kas izriet no konkrētās prakses pastāvēšanas, tātad nav bijusi „saskaņā ar tiesību aktiem". Tiesa uzskatīja, ka ir bijis ECK 8. panta prasību pārkāpums.

8.2. Dati, kas saistīti ar nodarbinātību

Galvenie punkti

- Īpašas datu aizsardzības normas nodarbināšanas attiecībās ir ietvertas EP Ieteikumā par nodarbināšanas datiem.
- Datu aizsardzības direktīvā uz nodarbināšanas attiecībām ir konkrēta atsauce tikai saistībā ar sensitīvu datu apstrādi.
- Piekrišanas, kam jābūt brīvi dotai, spēkā esamība kā tiesisks pamats darbinieku datu apstrādei var būt apšaubāma, ņemot vērā ekonomiskā līdzsvara trūkumu starp darba devēju un darbiniekiem. Piekrišanas došanas apstākļi ir rūpīgi jāizvērtē.

Savienībā nav konkrēta tiesiskā regulējuma, kas regulētu datu apstrādi saistībā ar nodarbināšanu. Datu aizsardzības direktīvā nodarbināšanas attiecības konkrēti ir minētas tikai direktīvas 8. panta 2. punktā, kas attiecas uz sensitīvu datu apstrādi.

297 ECT 1984. gada 2. augusta spriedums lietā *Malone pret Apvienoto Karalisti*, prasības pieteikums Nr. 8691/79.

Kas attiecas uz EP, Ieteikums par nodarbināšanas datiem tika izdots 1989. gadā un pašlaik tiek atjaunināts.[298]

Pētījums par biežāk sastopamajām datu aizsardzības problēmām, kas raksturīgas nodarbināšanas jomai, ir atrodams 29. panta darba grupas darba dokumentā.[299] Darba grupa analizēja, kāda nozīme ir piekrišanai kā tiesiskam pamatam ar nodarbināšanu saistītu datu apstrādei.[300] Darba grupa konstatēja, ka ekonomiskā līdzsvara trūkums starp darba devēju, kas prasa piekrišanu, un darbinieku, kas dod piekrišanu, bieži vien raisīs šaubas par to, vai piekrišana tika brīvi dota vai nē. Tāpēc, novērtējot piekrišanas spēkā esamību saistībā ar nodarbināšanu, ir rūpīgi jāizsver apstākļi, kādos piekrišana tika prasīta.

Bieži sastopama datu aizsardzības problēma tipiskā mūsdienu darba vidē ir jautājums par to, cik likumīgi ir uzraudzīt darbinieku elektronisko komunikāciju darbavietā. Bieži tiek apgalvots, ka šo problēmu var viegli atrisināt, aizliedzot darbā privātiem mērķiem izmantot komunikāciju ierīces. Šāds vispārīgs aizliegums tomēr var būt nesamērīgs un nereāls. Nākamais ECT spriedums ir īpaši interesants šajā saistībā:

> Piemērs: Lietā *Copland pret Apvienoto Karalisti*[301] slepeni tika uzraudzīts, kā kāda koledžas darbiniece izmantoja telefonu, e-pastu un internetu, lai noskaidrotu, vai viņa pārmērīgi izmantoja koledžas ierīces personīgām vajadzībām. ECT uzskatīja, ka uz telefona zvaniem no darba vietas attiecās privātās dzīves un korespondences jēdziens. Tāpēc tādus zvanus un e-pastus, kas nosūtīti no darba, kā arī informāciju, kas izriet no personīgā interneta lietošanas uzraudzīšanas, sargāja ECK 8. pants. Prasītājas gadījumā nebija noteikumu, kas regulētu apstākļus, kādos darba devēji var uzraudzīt to, kā darbinieki izmanto telefonu, e-pastu un internetu. Tāpēc iejaukšanās nebija saskaņā ar tiesību aktiem. Tiesa secināja, ka ir bijis ECK 8. panta prasību pārkāpums.

298 Eiropas Padome, Ministru komiteja (1989), Ieteikums Rec(89)2 dalībvalstīm par tādu personas datu aizsardzību, ko izmanto nodarbināšanas nolūkiem, 1989. gada 18. janvārī. Sk. turpmāk 108. konvencijas Konsultatīvo komiteju, Pētījumu par Ieteikumu Nr. R (89) 2 par tādu personas datu aizsardzību, ko izmanto nodarbināšanas nolūkiem, un lai ierosinātu priekšlikumus iepriekš minētā ieteikuma pārskatīšanai, 2011. gada 9. septembrī.

299 29. panta darba grupa (2001), *Atzinums 8/2001 par personas datu apstrādi nodarbinātības [nodarbināšanas] jomā*, WP 48, Briselē, 2001. gada 13. septembrī.

300 29. panta darba grupa (2005), Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta vienotu interpretāciju,WP 114, Briselē, 2005. gada 25. novembrī.

301 ECT 2007. gada 3. aprīļa spriedums lietā *Copland pret Apvienoto Karalisti*, prasības pieteikums Nr. 62617/00.

Atbilstoši EP Ieteikumam par nodarbināšanu personas datus, ko ievāc nodarbināšanas nolūkiem, var iegūt no individuālā darbinieka tieši.

Personas dati, ko ievāc pieņemšanai darbā, ir jāierobežo līdz informācijai, kas nepieciešama, lai novērtētu kandidātu piemērotību un viņu karjeras potenciālu.

Ieteikumā ir konkrēti pieminēti arī subjektīvie vērtējuma dati, kas attiecas uz individuālu darbinieku sniegumu vai potenciālu. Šādi dati ir jāpamato uz godprātīgiem un godīgiem novērtējumiem, un to formulējums nedrīkst būt aizvainojošs. To prasa godprātīgas datu apstrādes un datu precizitātes principi.

Īpašs datu aizsardzības tiesību aktu aspekts darba devēja–darbinieka attiecībās ir darbinieku pārstāvju loma. Šādi pārstāvji drīkst saņemt darbinieku personas datus tikai tiktāl, ciktāl tas ir nepieciešams, lai dotu viņiem iespēju pārstāvēt darbinieku intereses.

Sensitīvus personas datus, kas ievākti nodarbināšanas nolūkos, drīkst apstrādāt tikai īpašos gadījumos un atbilstoši valsts tiesību aktos paredzētajām garantijām. Darba devēji drīkst jautāt darbiniekiem vai darba kandidātiem par viņu veselības stāvokli vai pārbaudīt viņu veselības stāvokli tikai tādēļ, lai: noteiktu viņu piemērotību nodarbināšanai, izpildītu profilaktiskās medicīnas prasības vai atļautu piešķirt sociālos pabalstus. Veselības datus nedrīkst ievākt no citiem avotiem, kā vien no attiecīgā darbinieka, izņemot gadījumus, kad ir saņemta skaidri pausta un informēta piekrišana vai ja tas ir noteikts valsts tiesību aktos.

Saskaņā ar Ieteikumu par nodarbināšanu darbiniekiem ir jābūt informētiem par savu personas datu apstrādes nolūku, par uzglabāto datu veidu, par vienībām, kurām datus regulāri paziņo, un par šādu paziņojumu tiesisko pamatu. Vēl darba devējiem iepriekš jāinformē savi darbinieki par darbinieku personas datu apstrādes vai darbinieku pārvietošanās un ražīguma uzraudzības automatizēto sistēmu ieviešanu vai pielāgošanu.

Darbiniekiem ir jābūt piekļuves tiesībām saviem datiem, kas saistīti ar nodarbināšanu, kā arī datu labošanas vai dzēšanas tiesībām. Ja tiek apstrādāti subjektīvie vērtējuma dati, darbiniekiem vēl ir jābūt tiesībām apstrīdēt šo subjektīvo spriedumu. Šādas tiesības tomēr var uz laiku tikt ierobežotas, iekšējas izmeklēšanas nolūkā. Ja kādam darbiniekam liedz piekļuvi ar nodarbināšanu saistītiem personas datiem, liedz iespēju tos labot vai dzēst, valsts tiesību aktos ir jāparedz atbilstošas garantijas šāda lieguma apstrīdēšanai.

8.3. Medicīniskie dati

Galvenais punkts

- Medicīniskie dati ir sensitīvi dati un tāpēc tie bauda īpašu aizsardzību.

Personas datus par datu subjekta veselības stāvokli klasificē kā sensitīvus datus atbilstoši datu aizsardzības direktīvas 8. panta 1. punktam un 108. konvencijas 6. pantam. Savukārt uz medicīniskajiem datiem attiecas stingrāks datu apstrādes režīms nekā uz nesensitīviem datiem.

Piemērs: Lietā *Z. pret Somiju*[302] prasītājas bijušais vīrs, kurš bija HIV inficēts, bija pastrādājis vairākus dzimumnoziegumus. Vēlāk viņu notiesāja par slepkavību, pamatojoties uz to, ka viņš apzināti bija pakļāvis upurus HIV infekcijas riskam. Valsts tiesa izdeva rīkojumu, ka pilnam spriedumam un lietas dokumentiem jāpaliek slepeniem 10 gadus, lai gan prasītāja lūdza ilgāku slepenības periodu. Apelācijas tiesa minētās prasības noraidīja, un tās spriedumā bija pilnībā norādīts gan prasītājas, gan viņas bijušā vīra vārds/uzvārds. ECT uzskatīja, ka šāda iejaukšanās nav uzskatāma par nepieciešamu demokrātiskā sabiedrībā, jo medicīnisko datu aizsardzība bija būtiska, lai varētu izmantot tiesības uz privātās un ģimenes dzīves neaizskaramību, jo īpaši, ja runa ir par HIV infekcijām, ņemot vērā, ka šis stāvoklis daudzās sabiedrībās tiek uztverts kā apkaunojošs. Tāpēc Tiesa secināja, ka, piešķirot piekļuvi prasītāja identitātei un datiem par viņa veselības stāvokli, kā aprakstīts apelācijas tiesas spriedumā, vien 10 gadus pēc sprieduma stāšanās spēkā, tiktu pārkāptas ECK 8. panta prasības.

Datu aizsardzības direktīvas 8. panta 3. punktā ir atļauts apstrādāt medicīniskos datus, ja datu apstrādi pieprasa profilaktiskās medicīnas, medicīniskas diagnozes, aprūpes vai ārstēšanas vai veselības aprūpes pakalpojumu pārvaldības nodrošināšanas nolūkiem. Tomēr apstrāde ir pieļaujama tikai tad, ja šos datus apstrādā

302 ECT 1997. gada 25. februāra spriedums lietā *Z. pret Somiju, prasības pieteikums* Nr. 22009/93, 94. un 112. punkts; sk. arī ECT 1997. gada 27. augusta spriedumu lietā *M.S. pret Zviedriju*, prasības pieteikums Nr. 20837/92; ECT 2006. gada 10. oktobra spriedumu lietā *L.L. pret Franciju*, prasības pieteikums Nr. 7508/02; ECT 2008. gada 17. jūlija spriedumu lietā *I. pret Somiju*, prasības pieteikums Nr. 20511/03; ECT 2009. gada 28. aprīļa spriedumu lietā *K.H. un citi pret Slovākiju*, prasības pieteikums Nr. 32881/04; ECT 2009. gada 2. jūnija spriedumsu lietā *Szuluk pret Apvienoto Karalisti*, prasības pieteikums Nr. 36936/05.

veselības aizsardzības darba profesionālis, uz kuru attiecas dienesta noslēpuma pienākums, vai cita persona, uz kuru arī attiecas līdzvērtīgs pienākums.[303]

EP 1997. gada Ieteikumā par medicīniskiem datiem 108. konvencijas principus sīkāk piemēro datu apstrādei medicīnas jomā.[304] Ierosinātās normas ir saskaņā ar datu aizsardzības direktīvas normām, kuras attiecas uz medicīnisko datu apstrādes likumīgiem nolūkiem, nepieciešamos pienākumus ievērot dienesta noslēpumu personām, kuras izmanto veselības datus, un datu subjektu tiesībām uz caurskatāmību un piekļuvi, labošanu un dzēšanu. Turklāt medicīniskos datus, kurus likumīgi apstrādā veselības aprūpes darba profesionāļi, nedrīkst nodot tiesībaizsardzības iestādēm, ja vien nav sniegtas „pietiekamas garantijas, lai novērstu atklāšanu, kas nav savienojama ar ECK 8. pantā garantēto [..] privātās dzīves neaizskaramību".[305]

Vēl Medicīnisko datu ieteikumā ir īpaši noteikumi par nedzimušu bērnu un rīcībnespējīgu personu medicīniskajiem datiem un par ģenētisko datu apstrādi. Zinātniskā pētniecība ir konkrēti atzīta par iemeslu, kad datus var saglabāt ilgāk nekā tie vajadzīgi, lai gan tos parasti vajadzēs anonimizēt. Medicīnisko datu ieteikuma 12. pantā ir ierosināts sīks regulējums situācijām, kurās pētniekiem vajag personas datus, un ar anonimizētiem datiem nepietiek.

Pseidonimizācija var būt atbilstošs līdzeklis, lai apmierinātu zinātniskās vajadzības un vienlaikus aizsargātu attiecīgo pacientu intereses. Pseidonimizācijas jēdziens saistībā ar datu aizsardzību ir sīkāk paskaidrots 2.1.3 iedaļā.

Valstu un Eiropas mērogā notiek intensīvas diskusijas par ierosmēm uzglabāt elektroniskā veselības datu datnē informāciju par pacienta ārstēšanu.[306] Īpašs aspekts elektronisko veselības datņu ieviešanai valsts mēroga sistēmās ir to pārrobežu pieejamība: tas ir īpaši svarīgs temats Savienībā saistībā ar pārrobežu veselības aprūpi.[307]

303 Sk. arī ECT 2008. gada 25. novembra spriedumu lietā *Biriuk pret Lietuvu*, prasības pieteikums Nr. 23373/03.

304 EP, Ministriju komiteja (1997), Ieteikums Rec(97)5 dalībvalstīm par medicīnisko datu aizsardzību, 1997. gada 13. februārī.

305 ECT 2013. gada 6. jūnija spriedums lietā *Avilkina un citi pret Krieviju*, prasības pieteikums Nr. 1585/09, 53. punkts (spriedums vēl nav galīgs).

306 29. panta darba grupa (2007), *Darba dokuments par personas ar veselību saistīto datu apstrādi elektroniskajās pacienta veselības kartēs,* WP 131, Briselē, 2007. gada 15. februārī.

307 Eiropas Parlamenta un Padomes 2011. gada 9. marta Direktīva 2011/24/ES par pacientu tiesību piemērošanu pārrobežu veselības aprūpē, OV 2011 L 88.

Cita apspriesta joma saistībā ar jaunajiem noteikumiem ir klīniskie izmēģinājumi, citiem vārdiem, jaunu zāļu izmēģināšana uz pacientiem dokumentētā izpētes vidē; arī šim tematam ir ievērojamas sekas uz datu aizsardzību. Klīniskos izmēģinājumus ar cilvēkiem paredzētām zālēm regulē Eiropas Parlamenta un Padomes 2001. gada 4. aprīļa Direktīva 2001/20/EK par dalībvalstu normatīvo un administratīvo aktu tuvināšanu attiecībā uz labas klīniskās prakses ieviešanu klīniskās izpētes veikšanā ar cilvēkiem paredzētām zālēm (*Klīnisko izmēģinājumu direktīva*).[308] 2012. gada decembrī Eiropas Komisija iesniedza priekšlikumu regulai, ar ko aizstāt Klīnisko izmēģinājumu direktīvu, lai padarītu izmēģinājumu procedūras viendabīgākas un efektīvākas.[309]

Saistībā ar personas datiem veselības nozarē ir vēl daudz citu leģislatīvu un citu ierosmju, kas tiek skatītas ES mērogā.[310]

8.4. Datu apstrāde statistikas nolūkiem

Galvenie punkti

- Datus, kas ievākti statistikas nolūkiem, nedrīkst izmantot nevienam citam nolūkam.
- Datus, kas likumīgi ievākti jebkuram nolūkam, var tālāk izmantot statistikas nolūkiem, ja vien valsts tiesību aktos ir paredzētas pienācīgas garantijas, ko lietotāji ievēro. Šajā nolūkā ir jo īpaši jāparedz anonimizēšana vai pseidonimizācija pirms datu nodošanas trešām personām.

Datu aizsardzības direktīvā datu apstrāde statistikas nolūkiem ir minēta saistībā ar iespējamām atkāpēm no datu aizsardzības principiem. Direktīvas 6. panta 1. punkta b) apakšpunktā ir noteikts, ka no nolūka ierobežošanas principa var atkāpties saskaņā ar valsts tiesību aktiem, lai turpmāk datus izmantotu statistikas nolūkiem, lai gan valsts tiesību aktos ir jānosaka arī visas vajadzīgās garantijas. Direktīvas

308 Eiropas Parlamenta un Padomes 2001. gada 4. aprīļa Direktīva 2001/20/EK par dalībvalstu normatīvo un administratīvo aktu tuvināšanu attiecībā uz labas klīniskās prakses ieviešanu klīniskās izpētes veikšanā ar cilvēkiem paredzētām zālēm, OV 2001 L 121.

309 Eiropas Komisija (2012), *Priekšlikums Eiropas Parlamenta un Padomes Regulai par cilvēkiem paredzētu zāļu klīniskajiem izmēģinājumiem un par Direktīvas 2001/20/EK atcelšanu*, COM(2012) 369 final, Briselē, 2012. gada 17. jūlijā.

310 EDAU (2013), *Eiropas Datu aizsardzības uzraudzītāja Atzinums par Komisijas paziņojumu „E-veselības rīcības plāns 2012.–2020. gadam – inovatīva veselības aprūpe 21. gadsimtam”*, Briselē, 2013. gada 27. martā.

13. panta 2. punktā ir atļauts ar valsts tiesību aktiem ierobežot piekļuves tiesības, ja datus apstrādā tikai un vienīgi statistikas nolūkiem; arī šajā gadījumā valsts tiesību aktos ir jābūt noteiktām atbilstošām garantijām. Šajā saistībā datu aizsardzības direktīva nosaka īpašu prasību, ka datus, kas iegūti vai radīti statistiskās izpētes gaitā, nedrīkst izmantot konkrētu lēmumu pieņemšanai attiecībā uz datu subjektiem.

Lai gan datus, ko pārzinis likumīgi ievācis jebkuram nolūkam, šis pārzinis var atkārtoti izmantot saviem statistikas nolūkiem – tā sauktajai sekundārajai statistikai –, datiem jābūt anonimizētiem vai pseidonimizētiem, atkarībā no konteksta, pirms to nodošanas trešām personām statistikas nolūkos, izņemot gadījumus, kad datu subjekts ir tam piekritis vai tas ir konkrēti paredzēts valsts tiesību aktos. Tas izriet no prasības par atbilstošām garantijām saskaņā ar datu aizsardzības direktīvas 6. panta 1. punkta b) apakšpunktu.

Svarīgākie gadījumi, kad datus izmanto statistikas nolūkiem, ir oficiālā statistika, ko veic valstu un ES statistikas biroji, pamatojoties uz valstu un ES tiesību aktiem par oficiālo statistiku. Atbilstoši šiem tiesību aktiem pilsoņiem un uzņēmumiem parasti ir pienākums atklāt datus statistikas iestādēm. Uz amatpersonām, kuras strādā statistikas birojos, parasti attiecas īpaši dienesta noslēpuma pienākumi, kas tiek rūpīgi ievēroti, jo tie ir būtiski svarīgi augstam pilsoņu uzticēšanās līmenim, kas ir nepieciešams, ja dati ir jādara pieejami statistikas iestādēm.

Regulā (EK) Nr. 223/2009 par Eiropas statistiku (*Eiropas Statistikas regula*) ir ietvertas būtiskas normas par datu aizsardzību oficiālajā statistikā, un tāpēc tās arī var uzskatīt par attiecināmām uz oficiālo statistiku valsts mērogā.[311] Regulā ir saglabāts princips, ka oficiālās statistikas darbībām ir vajadzīgs pietiekami precīzs tiesiskais pamats.[312]

311 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.

312 Šis princips tiks sīkāk aplūkots *Eurostat* Prakses kodeksā, kas saskaņā ar Eiropas Statistikas regulas 11. pantu dod ētikas vadlīnijas par oficiālās statistikas veikšanu, tostarp personas datu izsvērtu izmantošanu; pieejams tīmekļa vietnē: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

Piemērs: Lietā *Huber pret Vāciju*[313] Tiesa konstatēja, ka iestādes veikta personas datu vākšana un uzglabāšana statistiskiem mērķiem pati par sevi nebija pietiekams iemesls, lai apstrāde būtu likumīga. Tiesību aktam, kas paredz personas datu apstrādi, arī bija jāatbilst vajadzības prasībai, kas konkrētajā gadījumā tā nebija.

Saistībā ar EP, 1997. gadā tika izdots Ieteikums par statistikas datiem, kas attiecas uz statistikas sniegumu publiskajā un privātajā sektorā.[314] Šis ieteikums ieviesa principus, kuri sakrīt ar iepriekš aprakstītajām galvenajām datu aizsardzības direktīvas normām. Sīkāk izstrādātas normas ir dotas par šādiem jautājumiem:

Tā kā datus, ko pārzinis ievācis statistikas nolūkiem, nedrīkst izmantot nevienam citam nolūkam, dati, kuri ievākti nestatistiskam nolūkam, ir pieejami turpmākai statistiskai izmantošanai. Ieteikums par statistikas datiem pat atļauj paziņot datus trešām personām, ja tas ir tikai statistikas nolūkiem. Šādos gadījumos pusēm jāvienojas un jāuzraksta turpmākas likumīgas izmantošanas statistikai apjoms. Tā kā tas nevar aizstāt datu subjekta piekrišanu, ir jāpieņem, ka valsts tiesību aktos ir jābūt noteiktām atbilstošām papildu garantijām, lai pēc iespējas mazinātu personas datu ļaunprātīgas izmantošanas risku –, piemēram, pienākumam pirms nodošanas anonimizēt vai pseidonimizēt datus.

Uz cilvēkiem, kuri profesionāli nodarbojas ar statistisko izpēti, ir jāattiecas īpašiem dienesta noslēpuma pienākumiem – kas ir raksturīgi oficiālajai statistikai – saskaņā ar valsts tiesību aktiem. Tas jāattiecina arī uz intervētājiem, ja viņi tiek nodarbināti datu ievākšanā no datu subjektiem vai citām personām.

Ja statistikas pētījums, kas izmanto personas datus, nav paredzēts tiesību aktos, datu subjektiem ir jāpiekrīt savu datu izmantošanai, lai tā būtu likumīga, vai arī viņiem ir jābūt vismaz iespējai iebilst. Ja personas datus ievāc statistikas nolūkiem, intervējot personas, tad šīs personas ir skaidri jāinformē par to, vai datu atklāšana ir obligāta saskaņā ar valsts tiesību aktiem vai nē. Sensitīvus datus nedrīkst ievākt tā, ka personu var identificēt, izņemot gadījumus, kad tas ir konkrēti atļauts valsts tiesību aktos.

313 Tiesas 2008. gada 16. decembra spriedums lietā C-524/06 *Huber/Vācija*, jo īpaši. skat. 68. punktu.

314 Eiropas Padome, Ministru komiteja (1997), Ieteikums Rec(97)18 dalībvalstīm par personas datu, kas ievākti un apstrādāti statistikas nolūkiem, aizsardzību, 1997. gada 30. septembrī.

Ja statistikas pētījumu nevar veikt bez anonimiem datiem, un personas dati ir patiešām vajadzīgi, šim nolūkam ievāktie dati ir jāanonimizē, tiklīdz tas ir izdarāms. Statistikas pētījuma rezultāti mazākais nedrīkst dot iespēju identificēt jebkuru datu subjektu, izņemot gadījumus, kad tas acīmredzami nerada nekādu risku.

Pēc statistikas analīzes pabeigšanas izmantotie personas dati ir jādzēš vai jāpadara anonīmi. Šajā gadījumā Ieteikums par statistikas datiem ierosina identifikācijas datus uzglabāt atsevišķi no citiem personas datiem. Tas nozīmē, piemēram, ka dati ir jāpseidonimizē, un atsevišķi no pseidonimizētajiem datiem ir jāuzglabā vai nu atšifrēšanas atslēga vai saraksts ar identificējošiem sinonīmiem.

8.5. Finanšu dati

Galvenie punkti

- Lai gan finanšu dati nav sensitīvi dati 108. konvencijas vai datu aizsardzības direktīvas nozīmē, to apstrādei vajag īpašas garantijas, lai nodrošinātu precizitāti un datu drošību.
- Elektroniskajām maksājumu sistēmām ir vajadzīga iebūvēta datu aizsardzība, tā dēvētā integrētā privātuma aizsardzība.
- Īpašas datu aizsardzības problēmas šajā jomā rodas no vajadzības, lai būtu ieviesti piemēroti autentifikācijas mehānismi.

Piemērs: Lietā *Michaud pret Franciju*[315] prasītājs, kāds Francijas jurists, apstrīdēja savu pienākumu saskaņā ar Francijas tiesību aktiem ziņot par aizdomām saistībā ar iespējamām savu klientu nelikumīgi iegūtu līdzekļu legalizēšanas darbībām. ECT norādīja, ka prasība juristiem ziņot administratīvajām iestādēm informāciju par citu personu, kas juristam tapusi zināma [informācijas] apmaiņas ceļā ar minēto personu, bija ECK 8. pantā noteikto jurista tiesību uz savas korespondences un privātās dzīves neaizskaramību aizskārums, jo minētais jēdziens attiecās uz profesionālām vai uzņēmējdarbībām. Tomēr iejaukšanās bija saskaņā ar tiesību aktiem un centās sasniegt izvirzītu mērķi, proti, nekārtību un noziedzības novēršanu. Tā kā uz juristiem attiecās pienākums ziņot par aiz-

315 ECT 2012. gada 6. decembra spriedums lietā *Michaud pret Franciju*, prasības pieteikums Nr. 12323/11; sk. arī 1992. gada 16. decembra spriedumu lietā *Niemietz pret Vāciju*, prasības pieteikums Nr. 13710/88, 29. punkts, un ECT 1997. gada 25. jūnija spriedumu lietā *Halford pret Apvienoto Karalisti*, prasības pieteikums Nr. 20605/92, 42. punkts.

domām tikai ļoti šauros apstākļos, ECT uzskatīja, ka šis pienākums ir samērīgs, secinot, ka nav bijis 8. panta prasību pārkāpuma.

108. konvencijā paredzētā datu aizsardzības vispārīgā tiesiskā regulējuma piemērošana maksājumiem tika izstrādāta EP 1990. gada Ieteikumā Rec(90)19.[316] Šajā ieteikumā ir paskaidrots datu likumīgas ievākšanas un izmantošanas tvērums saistībā ar maksājumiem, jo īpaši maksājumu kartēm. Tālāk tas ierosina valstu likumdevējiem sīki izstrādātus regulējumus par maksājuma datu paziņošanas trešām personām ierobežojumiem, par datu saglabāšanas termiņiem, par caurskatāmību, datu drošību un pārrobežu datu plūsmām un, visbeidzot, par uzraudzību un tiesiskās aizsardzības līdzekļiem. Ierosinātie risinājumi atbilst tam, kas vēlāk tika paredzēts ES vispārīgajā datu aizsardzības regulējumā datu aizsardzības direktīvā.

Ir izveidoti vairāki juridiskie instrumenti, lai regulētu finanšu instrumentu tirgus un kredītiestāžu un ieguldījumu sabiedrību darbību.[317] Citi juridiskie instrumenti palīdz cīnīties pret iekšējās informācijas ļaunprātīgu izmantošanu un tirgus manipulācijām.[318] Kritiskākie jautājumi šajās jomās, kas ietekmē datu aizsardzību, ir šādi:

- uzskaites saglabāšana par finanšu darījumiem;
- personas datu nodošana trešām valstīm;
- telefona sarunu vai elektroniskās komunikācijas ierakstīšana, tostarp kompetento iestāžu pilnvaras pieprasīt telefona un datplūsmas ierakstus;

316 EP, Ministru komiteja (1990), Ieteikums Nr. R Rec(90) 19 par personas datu aizsardzību, ko izmanto maksājumiem un citām saistītajām darbībām, 1990. gada 13. septembrī.

317 Eiropas Komisija (2011), *Priekšlikums Eiropas Parlamenta un Padomes direktīvai par finanšu instrumentu tirgiem, ar kuru atceļ Eiropas Parlamenta un Padomes Direktīvu 2004/39/EK*, COM(2011) 656 final, Briselē, 2011. gada 20. oktobrī; Eiropas Komisija (2011), *Priekšlikums Eiropas Parlamenta un Padomes direktīvai par finanšu instrumentu tirgiem, ar ko groza Regulu [EMIR] par ārpusbiržas atvasinātiem finanšu instrumentiem, centrālajiem darījumu partneriem un tirdzniecības reģistriem*, COM(2011) 652 final, Briselē, 2011. gada 20. oktobrī; Eiropas Komisija (2011), *Priekšlikums Eiropas Parlamenta un Padomes direktīvai par piekļuvi kredītiestāžu darbībai un kredītiestāžu un ieguldījumu sabiedrību konsultatīvo uzraudzību un par grozījumiem Eiropas Parlamenta un Padomes Direktīvā 2002/87/EK par papildu uzraudzību kredītiestādēm, apdrošināšanas uzņēmumiem un ieguldījumu sabiedrībām finanšu konglomerātos*, COM(2011) 453 final, Briselē, 2011. gada 20. jūlijā.

318 Eiropas Komisija (2011), *Priekšlikums Eiropas Parlamenta un Padomes regulai par iekšējās informācijas ļaunprātīgu izmantošanu un tirgus manipulācijām (tirgus ļaunprātīgu izmantošanu)*, COM(2011) 651 final, Briselē, 2011. gada 20. oktobrī; Eiropas Komisija (2011), *Priekšlikums Eiropas Parlamenta un Padomes direktīvai par krimināl sankcijām iekšējās informācijas ļaunprātīgas izmantošanas un tirgus manipulāciju gadījumā*, COM(2011) 654 final, Briselē, 2011. gada 20. oktobrī.

- personīgas informācijas atklāšana, tostarp sankciju publicēšana;
- kompetento iestāžu uzraudzības un izmeklēšanas pilnvaras, tostarp inspekcijas uz vietas un iekļūšana privātās telpās dokumentu konfiscēšanai;
- pārkāpumu paziņošanas mehānisms, proti, ziņošanas sistēmas; un
- sadarbība starp dalībvalstu kompetentajām iestādēm un Eiropas Vērtspapīru un tirgu iestādi (*ESMA*).

Šajās jomās ir arī citi jautājumi, kas tiek konkrēti risināti, tostarp datu ievākšana par datu subjektu finansiālo stāvokli[319] vai pārrobežu maksājumi, ko veic ar bankas pārvedumiem, kas nenovēršami rada personas datu plūsmas.[320]

319 Eiropas Parlamenta un Padomes 2009. gada 16. septembra Regula (EK) Nr. 1060/2009 par kredītreitingu aģentūrām, OV 2009 L 302; Eiropas Komisija, *Priekšlikums Eiropas Parlamenta un Padomes regulai par Regulas (EK) Nr. 1060/2009 par kredītreitingu aģentūrām grozīšanu*, COM(2010) 289 final, Briselē, 2010. gada 2. jūnijā.

320 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.

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.

EDRi, *An introduction to data protection*, Brussels, pieejams: www.edri.org/files/paper06_datap.pdf.

Frowein, J., Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. and 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., 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., Brandeis, L. (1890), 'The right to privacy', *Harvard Law Review,* 4. sēj., Nr. 5, 193.–220. lpp., pieejams: www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R., Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

2. nodaļa

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

Morgan, R., 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.

Tinnefeld, M., Buchner, B., 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*, pieejams: www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

3.–5. 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., 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*, Saarbrücken, Éditions universitaires européennes.

Dammann, U., Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (European Union Agency for Fundamental Rights) (2010), *Data Protection in the European Union: the role of National Data Protection 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.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, pieejams: www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

6. nodaļa

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C., 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.

7. nodaļa

Europol (2012), *Data Protection at Europol*, Luxembourg, Publications Office, pieejams: www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, The Hague, Eurojust.

Drewer, D., 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.

Gutwirth, S., Poullet, Y., De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P., 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, pieejams: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

8. nodaļa

Büllesbach, A., Gijrath, S., Poullet, Y., Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P., Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P., 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., Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

Tiesu prakse

Atlasīti Eiropas Cilvēktiesību tiesas prakses piemēri

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
Odièvre pret Franciju [GC], Nr. 42326/98, 2003. gada 13. februāris

Datu aizsardzības līdzsvarošana ar vārda brīvību

Axel Springer AG pret Vāciju [GC], Nr. 39954/08, 2012. gada 7. februāris
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

Datu aizsardzības tiešsaistē izaicinājumi

K.U. pret Somiju, Nr. 2872/02, 2008. gada 2. decembris

Korespondence

Amann pret Šveici [GC], Nr. 27798/95, 2000. gada 16. februāris
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
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, 1985. gada 26. aprīlis
McMichael pret Apvienoto Karalisti, Nr. 16424/90, 1995. gada 24. februāris
M.G. pret Apvienoto Karalisti, Nr. 39393/98, 2002. gada 24. septembris
Rotaru pret Rumāniju [GC], Nr. 28341/95, 2000. gada 4. maijs
S. un Marper pret Apvienoto Karalisti, Nr. 30562/04 un Nr. 30566/04, 2008. gada 4. decembris
Shimovolos pret Krieviju, Nr. 30194/09, 2011. gada 21. jūnijs
Turek pret Slovākiju, Nr. 57986/00, 2006. gada 14. februāris

Kriminālas tiesājamības datu bāzes

B.B. pret Franciju, Nr. 5335/06, 2009. gada 17. decembris
M.M. pret Apvienoto Karalisti, Nr. 24029/07, 2012. gada 13. novembris

DNS datu bāzes

S. un Marper pret Apvienoto Karalisti, 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

Biriuk pret Lietuvu, Nr. 23373/03, 2008. gada 25. novembris
I. pret Somiju, Nr. 20511/03, 2008. gada 17. jūlijs
L.L. pret Franciju, Nr. 7508/02, 2006. gada 10. oktobris
M.S. pret Zviedriju, Nr. 34209/96, 2002. gada 2. jūlijs
Szuluk pret Apvienoto Karalisti, Nr. 36936/05, 2009. gada 2. jūnijs
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 profesionālām darbībām

Michaud pret Franciju, Nr. 12323/11, 2012. gada 6. decembris
Niemietz pret Vāciju, Nr. 13710/88, 1992. gada 16. decembris

Komunikācijas pārtveršana

Amann pret Šveici [GC], Nr. 27798/95, 2000. gada 16. februāris
Copland pret Apvienoto Karalisti, Nr. 62617/00, 2007. gada 3. aprīlis
Cotlet pret Rumāniju, Nr. 38565/97, 2003. gada 3. jūnijs
Kruslin pret Franciju, Nr. 11801/85, 1990. gada 24. aprīlis
Lambert pret Franciju, Nr. 23618/94, 1998. gada 24. augusts
Liberty un citi pret Apvienoto Karalisti, Nr. 58243/00, 2008. gada 1. jūlijs
Malone pret Apvienoto Karalisti, Nr. 8691/79, 1985. gada 26. aprīlis
Halford pret Apvienoto Karalisti, Nr. 20605/92, 1997. gada 25. jūnijs
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

Fotogrāfijas

Sciacca pret Itāliju, Nr. 50774/99, 2005. gada 11. janvāris
Von Hannover pret Vāciju, Nr. 59320/00, 2004. gada 24. jūnijs

Tiesības būt aizmirstam

Segerstedt-Wiberg un citi pret Zviedriju, Nr. 62332/00, 2006. gada 6. jūnijs

Iebilduma tiesības

Leander pret Zviedriju, Nr. 9248/81, 1987. gada 26. marts
Mosley pret Apvienoto Karalisti, Nr. 48009/08, 2011. gada 10. maijs
M.S. pret Zviedriju, Nr. 34209/96, 2002. gada 2. jūlijs
Rotaru pret Rumāniju [GC], Nr. 28341/95, 2000. gada 4. maijs

Sensitīvas datu kategorijas

I. pret Somiju, Nr. 20511/03, 2008. gada 17. jūlijs
Michaud pret Fanciju, Nr. 12323/11, 2012. gada 6. decembris
S. un Marper pret Apvienoto Karalisti, Nr. 30562/04 un Nr. 30566/04, 2008. gada 4. decembris

Uzraudzība un piespiedu izpilde (dažādu dalībnieku, tostarp datu aizsardzības iestāžu loma)

I. pret Somiju, Nr. 20511/03, 2008. gada 17. jūlijs
K.U. pret Somiju, prasības pieteikums 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

Uzraudzības metodes

Allan pret Apvienoto Karalisti, Nr. 48539/99, 2002. gada 5. novembris
Association „21 Décembre 1989" un citi pret Rumāniju, Nr. 33810/07 un Nr. 18817/08, 2011. gada 24. maijs
Bykov pret Krieviju [GC], Nr. 4378/02, 2009. gada 10. marts
Kennedy pret Apvienoto Karalisti, Nr. 26839/05, 2010. gada 18. maijs
Klass un citi pret Vāciju, Nr. 5029/71, 1978. gada 6. septembris
Rotaru pret Rumāniju [GC], Nr. 28341/95, 2000. gada 4. maijs
Taylor-Sabori pret Apvienoto Karalisti, Nr. 47114/99, 2002. gada 22. oktobris
Uzun pret Vāciju, Nr. 35623/05, 2010. gada 2. septembris
Vetter pret Franciju, Nr. 59842/00, 2005. gada 31. maijs

Videonovērošana

Köpke pret Vāciju, Nr. 420/07, 2010. gada 5. oktobris
Peck pret Apvienoto Karalisti, Nr. 44647/98, 2003. gada 28. janvāris

Balss paraugi

P.G. un J.H. pret Apvienoto Karalisti, Nr. 44787/98, 2001. gada 25. septembris
Wisse pret Franciju, Nr. 71611/01, 2005. gada 20. decembris

Atlasīti Eiropas Savienības Tiesas prakses piemēri

Judikatūra saistībā ar datu aizsardzības direktīvu

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) un Federación de Comercio Electrónico y Marketing Directo (FECEMD) pret Administración del Estado, apvienotajās lietās C-468/10 un C-469/10, 2011. gada 24. novembris
[Datu aizsardzības direktīvas 7. panta f) punkta – „citu likumīgas intereses" – pareiza īstenošana valsts tiesībās]

Bodil Lindqvist, C-101/01, 2003. gada 6. novembris
[Datu par citu personu privāto dzīvi publicēšanas internetā, ko veic kāda privāta persona, likumība]

College van burgemeester en wethouders van Rotterdam pret M.E.E. Rijkeboer, C-553/07, 2009. gada 7. maijs
[Datu subjekta piekļuves tiesības]

Deutsche Telekom AG pret Bundesrepublik Deutschland, C-543/09, 2011. gada 5. maijs
[Vajadzība pēc atjaunotas piekrišanas]

Digital Rights Ireland un Seitling un citi, apvienotajās lietā C-293/12 un C-594/12, 2014. gada 8. aprīlis
[ES primāro tiesību pārkāpšana ar datu saglabāšanas direktīvu]

Eiropas Komisija pret Austrijas Republiku, C-614/10, 2012. gada 16. oktobris
[Valsts uzraudzības iestādes neatkarība]

Eiropas Komisija pret Ungāriju, C-288/12, 2014. gada 8. aprīlis
[Valsts datu aizsardzības uzraudzītāja atbrīvošanas no amata likumība]

Eiropas Komisija pret Vācijas Federatīvā Republiku, C-518/07, 2010. gada 9. marts
[Valsts uzraudzības iestādes neatkarība]

Eiropas Komisija pret Zviedrijas Karalisti, C-270/1, 2013. gada 30. maijs
[Sods par direktīvas neīstenošanu]

Google Spain, S.L., Google Inc. pret Agencia Española de Protección de Datos, Mario Costeja González. Audiencia Nacional, C 131/12, Lūgums sniegt prejudiciālu nolēmumu, ko 2012. gada 9. martā iesniedza *Audiencia Nacional* (Spānija), 2012. gada 25. maijs, tiek izskatīta

[Meklētājprogrammu pakalpojumu sniedzēju pienākums pēc datu subjekta lūguma atturēties no personas datu uzrādīšanas meklēšanas rezultātos]

Huber pret Vācijas Federatīvā Republiku, C-524/06, 2008. gada 16. decembris

[Datu par ārvalstniekiem turēšanas statistikas reģistrā likumība]

Michael Schwarz pret Stadt Bochum, ģenerāladvokāta secinājumi, C-291/12, 2013. gada 13. jūnijs

[ES primāro tiesību pārkāpšana ar Regulu (EK) Nr. 2252/2004, ar kuru paredz, ka pasēs jāuzglabā pirkstu nospiedumi]

Tietosuojavaltuutettu pret Satakunnan Markkinapörssi Oy un Satamedia Oy, C-73/07, 2008. gada 16. decembris

[„Žurnālistikas darbības" jēdziens Datu aizsardzības direktīvas 9. panta nozīmē]

Productores de Música de España (Promusicae) pret Telefónica de España SAU, C-275/06, 2008. gada 29. janvāris

[Interneta piekļuves sniedzēju pienākums atklāt intelektuālā īpašuma aizsardzības asociācijai KaZaA tīmekļa datņu koplietošanas platformas lietotāju identitāti]

Rechnungshof pret Österreichischer Rundfunk un citi un Neukomm un Lauermann pret Österreichischer Rundfunk, apvienotajās lietās C-465/00, C-138/01 un C-139/01, 2003. gada 20. maijs

[Juridiskā pienākuma publicēt personas datus par noteiktu ar publisko sektoru saistītu iestāžu kategoriju darbinieku algām samērīgums]

SABAM pret Netlog N.V., C-360/10, 2012. gada 16. februāris

[Sociālo tīklu pakalpojumu sniedzēju pienākums novērst, ka tīkla lietotāji nelikumīgi izmanto mūzikas un audiovizuālos darbus]

Volker un Markus Schecke GbR un Hartmut Eifert pret Land Hessen, apvienotajās lietās C-92/09 un C-93/09, 2010. gada 9. novembris

[Juridiskā pienākuma publicēt personas datus par dažu ES lauksaimniecības fondu atbalsta saņēmējiem samērīgums]

Judikatūra saistībā ar Regulu par aizsardzību attiecībā uz personas datu apstrādi ES iestādēs

Eiropas Komisija pret The Bavarian Lager Co. Ltd., C-28/08 P, 2010. gada 29. jūnijs
[Piekļuve dokumentiem]

Interporc Im- und Export GmbH pret Eiropas Kopienu Komisiju, C-41/00 P, 2003. gada 6. marts
[Piekļuve dokumentiem]

Pachtitis pret Komisiju un EPSO, F35/08, 2010. gada 15. jūnijs
[Personas datu izmantošana saistībā ar nodarbinātību ES iestādēs]

V pret Parlamentu, F46/09, 2011. gada 5. jūlijs
[Personas datu izmantošana saistībā ar nodarbinātību ES iestādēs]

Rādītājs

Eiropas Kopienu Tiesas judikatūra

Eiropas Cilvēktiesību tiesas judikatūra

Valsts tiesu judikatūra

Eiropas Savienības Pamattiesību aģentūra
Eiropas Padome — Eiropas Cilvēktiesību tiesa

Rokasgrāmata par Eiropas tiesību aktiem datu aizsardzības jomā

2015 — 194 lpp. — 14,8 × 21 cm

ISBN 978-92-871-9942-3 (Eiropas Padome)
ISBN 978-92-9239-337-3 (*FRA*)
doi:10.2811/54847

Liela daļa informācijas par Eiropas Savienības Pamattiesību aģentūru ir pieejama internetā. Tai var piekļūt *FRA* mājas lapā (http://fra.europa.eu).

Plašāka informācija par Eiropas Padomi ir pieejama internetā http://hub.coe.int

Plašāka informācija par Eiropas Cilvēktiesību tiesas judikatūru ir pieejama tiesas tīmekļa vietnē http://echr.coe.int. *HUDOC* meklēšanas portāls nodrošina piekļuvi spriedumiem un lēmumiem angļu un/vai franču valodā, kā arī satur tulkojumus papildu valodās, ikmēneša informatīvas piezīmes par judikatūru, preses relīzes un citu informāciju par tiesas darbu.

10.2811/54847 TK-01-13-772-LV-C

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Informācijas un komunikācijas tehnoloģiju straujā attīstība uzsver aizvien pieaugošo vajadzību pēc stingras personas datu aizsardzības – šīs tiesības garantē gan Eiropas Savienības (ES), gan Eiropas Padomes (EP) instrumenti. Tehnoloģiskā attīstība paplašina, piemēram, uzraudzības, komunikāciju pārtveršanas un datu uzglabāšanas robežas, kas arī rada ievērojamus izaicinājumus tiesībām uz datu aizsardzību. Šī rokasgrāmata ir izstrādāta tā, lai iepazīstinātu praktizējošus juristus, kuri nav specializējušies datu aizsardzības jomā, ar šo tiesību jomu. Tajā ir sniegts pārskats par ES un EP piemērojamajiem tiesiskajiem regulējumiem. Tajā ir paskaidrota galvenā judikatūra, apkopojot galvenos Eiropas Cilvēktiesību tiesas (ECT) un Eiropas Savienības Tiesas (Tiesas) nolēmumus. Tur, kur šādas prakses nav, rokasgrāmatā ir praktiskas ilustrācijas ar hipotētiskiem scenārijiem. Vispārīgos vilcienos, šī rokasgrāmata palīdz nodrošināt, ka tiesības uz datu aizsardzību tiek atbalstītas enerģiski un noteikti.

EIROPAS SAVIENĪBAS PAMATTIESĪBU AĢENTŪRA
Schwarzenbergplatz 11, 1040 Vīne – Austrija
Tālr. +43 (1) 580 30-60 – Fakss +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

EIROPAS PADOME
EIROPAS CILVĒKTIESĪBU TIESA
67075 Strasbūra Cedex – Francija
Tālr. +33 (0) 3 88 41 20 00 – Fakss +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Publikāciju birojs
ISBN 978-92-871-9942-3 (Eiropas Padome)
ISBN 978-92-9239-337-3 (FRA)