Modernizētā Konvencija Nr. 108

Konvencija par personu aizsardzību attiecībā uz personas datu apstrādi

www.coe.int/dataprotection



# Paskaidrojošais ziņojums

### I. Ievads

1. No brīža, kad pirms 35 gadiem parakstīšanai tika atvērta Konvencija par personu aizsardzību attiecībā uz personas datu automātisku apstrādi, zināma arī kā Konvencija Nr. 108 (turpmāk tekstā – Konvencija), tā ir bijusi pamats starptautiskajiem datu aizsardzības tiesību aktiem vairāk nekā 40 Eiropas valstīs. Tā ir arī ietekmējusi politiku un tiesību aktus tālu aiz Eiropas robežām. Tā kā katru dienu rodas jaunas problēmas, kas apdraud cilvēktiesības un pamatbrīvības, jo īpaši tiesības uz privāto dzīvi, kļuva skaidrs, ka Konvencija ir jāmodernizē, lai labāk risinātu jaunās ar privātumu saistītās problēmas, ko rada aizvien plašāka jauno informācijas un komunikācijas tehnoloģiju (IT) lietošana, apstrādes darbību globalizācija un aizvien pieaugošās personas datu plūsmas, un vienlaikus stiprinātu Konvencijas izvērtēšanas un uzraudzības mehānismu.

2. Tika panākta plaša vienošanās par šādiem modernizācijas procesa aspektiem: jāsaglabā Konvencijas noteikumu vispārīgums un tehnoloģiskā neitralitāte, jāsaglabā Konvencijas saskaņotība un saderība ar citiem tiesiskajiem regulējumiem un atkārtoti jāapstiprina Konvencijas atklātums, kas tai piešķir unikālu universāla standarta potenciālu. Konvencijas teksts ir vispārīgs, un to var papildināt ar detalizētākām nesaistošām nozaru tiesību normām, jo īpaši ar Ministru komitejas ieteikumiem, kas izstrādāti, piedaloties ieinteresētajām pusēm.

3. Modernizācija notika plašākā kontekstā vienlaikus ar dažādām starptautisko datu aizsardzības instrumentu reformām, pienācīgi ņemot vērā 1980. gada Ekonomiskās sadarbības un attīstības organizācijas (ESAO) Pamatnostādnes par privātās dzīves aizsardzību un personas datu pārrobežu plūsmu (pārskatītas 2013. gadā), Apvienoto Nāciju Organizācijas 1990. gada Pamatnostādnes par elektronisko personas datu datņu noteikumiem, Eiropas Savienības (ES) tiesisko regulējumu[[1]](#footnote-2) kopš 1995. gada, 2004. gada Āzijas un Klusā okeāna valstu ekonomiskās sadarbības foruma privātuma pamatnoteikumus un 2009. gada standartus “International Standards on the Protection of Privacy with regard to the processing of Personal Data” [Starptautiskie standarti privātuma aizsardzībai attiecībā uz personas datu apstrādi][[2]](#footnote-3). Darbs tika veikts paralēli jo īpaši attiecībā uz ES datu aizsardzības reformu kopumu, ļoti rūpīgi raugoties, lai tiktu nodrošināta abu tiesisko regulējumu saskaņotība. ES datu aizsardzības tiesiskajā regulējumā ir konkretizēti un pastiprināti Konvencijas Nr. 108 principi un ņemta vērā pievienošanās Konvencijai Nr. 108, jo īpaši attiecībā uz datu pārsūtīšanu starptautiskā mērogā.[[3]](#footnote-4)

4. Konsultatīvā komiteja, kas izveidota saskaņā ar Konvencijas 18. pantu, sagatavoja modernizācijas projekta priekšlikumus, kuri tika pieņemti 29. plenārsēdē (2012. gada 27.–30. novembrī) un iesniegti Ministru komitejai. Pēc tam Ministru komiteja modernizācijas priekšlikumus uzticēja pabeigt *ad hoc* komitejai datu aizsardzības jautājumos (*CAHDATA*). Tas tika izdarīts *CAHDATA* 3. sanāksmē (2014. gada 1.–3. decembrī). Papildus ES datu aizsardzības tiesiskā regulējuma pabeigšanai tika izveidota vēl viena *CAHDATA*, lai izskatītu neatrisinātos jautājumus.

Pēdējā *CAHDATA* sanāksmē (2016. gada 15.–16. jūnijā) šie priekšlikumi tika pabeigti un iesniegti Ministru komitejai izvērtēšanai un pieņemšanai.

5. Šā paskaidrojošā ziņojuma mērķis ir sniegt norādes un atbalstu Konvencijas noteikumu piemērošanā, un tajā ir izklāstīts, kā tās izstrādātāji ir paredzējuši Konvencijas darbību.

6. Ministru komiteja ir apstiprinājusi paskaidrojošo ziņojumu. Šajā ziņā paskaidrojošais ziņojums veido daļu no konteksta, kurā paskaidrota konkrētu Konvencijā lietoto terminu nozīme (piezīme: sk. Apvienoto Nāciju Organizācijas Vīnes Konvencijas par starptautisko līgumu tiesībām 31. panta 1. un 2. punktu).

Ministru komiteja Protokolu pieņēma 2018. gada 18. maijā. Protokola papildinājums ir Protokola neatņemama sastāvdaļa, un tam ir tāds pats juridiskais spēks kā pārējiem Protokola noteikumiem.

Šis protokols tika atvērts parakstīšanai 2018. gada 10. oktobrī Strasbūrā.

### II. Komentāri

7. Šā protokola mērķis ir modernizēt Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu apstrādi (EPLS Nr. 108) un tās Papildu protokolu par uzraudzības institūcijām un pārrobežu datu plūsmām (EPLS Nr. 181) un stiprināt to piemērošanu. No brīža, kad Papildu protokols stājas spēkā, to uzskata par grozītās Konvencijas neatņemamu sastāvdaļu.

8. Konvencijas Nr. 108 un tās papildu protokola paskaidrojošie ziņojumi joprojām ir aktuāli, jo tajos sniegts vēsturiskais konteksts un aprakstīta abu instrumentu attīstība, un šajā nolūkā tos var skatīt kopā ar šo dokumentu.

### Preambula

9. Preambulā atkārtoti apstiprināta parakstītājvalstu apņemšanās ievērot cilvēktiesības un pamatbrīvības.

10. Viens no Konvencijas galvenajiem mērķiem ir nodrošināt, ka personas zina, saprot un kontrolē to, kā citas personas apstrādā viņu personas datus. Tādēļ preambulā ir skaidri minētas tiesības uz personas autonomiju un personas tiesības kontrolēt savus personas datus, kas jo īpaši izriet no personas tiesībām uz privātās dzīves neaizskaramību un cieņu. Lai saglabātu cilvēka cieņu, attiecībā uz personas datu apstrādi ir jāievieš aizsardzības pasākumi, lai personas netiktu uzskatītas tikai par objektiem.

11. Ņemot vērā nozīmi, kāda sabiedrībā ir tiesībām uz personas datu aizsardzību, preambulā uzsvērts princips, ka attiecīgā gadījumā ir savstarpēji jāsaskaņo personu intereses, tiesības un pamatbrīvības. Tādēļ, lai saglabātu optimālu līdzsvaru starp dažādām interesēm, tiesībām un pamatbrīvībām, Konvencijā ir paredzēti konkrēti nosacījumi un ierobežojumi attiecībā uz informācijas apstrādi un personas datu aizsardzību. Tiesības uz datu aizsardzību, piemēram, ir jāskata kopā ar tiesībām uz vārda brīvību, kas noteiktas Eiropas Cilvēktiesību konvencijas (EPLS Nr. 5) 10. pantā un kas ietver uzskatu brīvību un tiesības netraucēti saņemt un izplatīt informāciju. Turklāt Konvencijā ir apstiprināts, ka tiesības uz datu aizsardzību, kas nav absolūtas, jo īpaši nedrīkst izmantot kā vispārēju līdzekli, lai liegtu publisku piekļuvi oficiāliem dokumentiem.[[4]](#footnote-5)

12. Konvencija Nr. 108 aizsargā personas, pamatojoties uz tajā noteiktajiem principiem un nostiprinātajām vērtībām, vienlaikus nodrošinot pamatnoteikumus attiecībā uz starptautiskām datu plūsmām. Tas ir svarīgi, jo globālo informācijas plūsmu nozīme mūsdienu sabiedrībā strauji pieaug, nodrošinot iespēju izmantot pamattiesības un pamatbrīvības, vienlaikus veicinot inovāciju un sekmējot sociālo un ekonomisko attīstību, kā arī būtiski palīdzot nodrošināt sabiedrības drošību. Informācijas un komunikācijas sabiedrībā personas datu apritei ir jānotiek, ievērojot personu pamattiesības un pamatbrīvības. Turklāt šīs tiesības ir jāievēro arī, izstrādājot un lietojot inovatīvas tehnoloģijas. Tas palīdz veidot uzticību inovācijai un jaunajām tehnoloģijām un veicināt to turpmāko attīstību.

13. Tā kā efektīvas personu aizsardzības pamatelements ir uzraudzības iestāžu starptautiskā sadarbība, Konvencijas mērķis ir stiprināt šādu sadarbību, jo īpaši nosakot, ka Pusēm ir jāsniedz savstarpēja palīdzība, un nodrošinot atbilstošu juridisko pamatu sadarbības sistēmai un informācijas apmaiņai izmeklēšanas un izpildes nolūkā.

### I nodaļa. Vispārīgi noteikumi

### 1. pants. Mērķis un nolūks

14. Konvencijas pirmajā pantā ir izklāstīts tās mērķis un nolūks. Šajā pantā norādīts uz aizsardzības priekšmetu – personas ir jāaizsargā, apstrādājot viņu personas datus.[[5]](#footnote-6) Datu aizsardzība kā pamattiesības nesen tika iekļauta ES Pamattiesību hartas 8. pantā un vairāku Konvencijas pušu konstitūcijās.

15. Konvencijā noteiktās garantijas attiecas uz visām personām neatkarīgi no pilsonības vai dzīvesvietas. Piemērojot šīs garantijas, nav atļauta trešo valstu pilsoņu diskriminācija salīdzinājumā ar pilsoņiem.[[6]](#footnote-7) Noteikumi, kas datu aizsardzību attiecina tikai uz attiecīgās valsts pilsoņiem vai ārvalstu pilsoņiem, kuri likumīgi uzturas attiecīgajā valstī, ir pretrunā Konvencijai.

### 2. pants. Definīcijas

16. Šajā konvencijā izmantoto definīciju nolūks ir nodrošināt vienādu terminu piemērošanu, lai valstu tiesību aktos izklāstītu noteiktus pamatjēdzienus.

#### a) apakšpunkts – “personas dati”

17. “Identificējama fiziska persona” ir persona, ko var tieši vai netieši identificēt. Personu neuzskata par “identificējamu”, ja tās identificēšanā jāiegulda nepieņemami ilgs laiks, centieni vai resursi. Piemēram, ja datu subjekta identificēšanai ir jāveic pārmērīgi sarežģītas, ilgstošas un dārgas darbības. Jautājums par to, kas ir “nepieņemami ilgs laiks, centieni vai resursi”, jāizvērtē katrā atsevišķā gadījumā. Piemēram, var apsvērt datu apstrādes nolūku, ņemot vērā tādus objektīvus kritērijus kā šādas identificēšanas izmaksas, ieguvumi, pārziņa veids, izmantotā tehnoloģija utt. Turklāt jēdziena “nepieņemami ilgs laiks, centieni vai resursi” nozīmi var mainīt tehnoloģiju attīstība un citi notikumi.

18. Jēdziens “identificējams” attiecas ne tikai uz personas pilsonisko vai juridisko identitāti, bet arī uz iezīmēm, kas var ļaut “individualizēt” vai atšķirt vienu personu no citām (un tādējādi ļaut atšķirīgi izturēties pret to). Šādu “individualizāciju” var veikt, piemēram, izmantojot identifikācijas numuru, pseidonīmu, biometriskos vai ģenētiskos datus, atrašanās vietas datus, IP adresi vai citu identifikatoru, lai konkrēti norādītu uz attiecīgo personu, ierīci (datoru, mobilo tālruni, kameru, spēļu ierīci utt.) vai ierīču kombināciju. Pseidonīma vai jebkura cita digitāla identifikatora / digitālās identitātes izmantošana nenodrošina datu anonimizāciju, jo datu subjektu joprojām var identificēt vai individualizēt. Tāpēc pseidonīma datus uzskata par personas datiem un uz tiem attiecas Konvencijas noteikumi. Novērtējot to aizsardzības pasākumu piemērotību, kas ieviesti, lai mazinātu riskus datu subjektiem, ir pienācīgi jāņem vērā izmantoto pseidonimizācijas metožu kvalitāte.

19. Dati ir uzskatāmi par anonīmiem tikai tik ilgi, kamēr nav iespējams atkārtoti identificēt datu subjektu vai ja šādai atkārtotai identificēšanai būtu vajadzīgs nepieņemami ilgs laiks, centieni vai resursi, ņemot vērā datu apstrādes brīdī pieejamās tehnoloģijas vai tehnoloģiju attīstību. Tomēr atsevišķos gadījumos (neieguldot nepieņemami ilgu laiku, centienus vai resursus) dati, kas šķiet anonīmi, jo tiem nav pievienoti nekādi acīmredzami identifikācijas elementi, ļauj identificēt personu. Tas var notikt, piemēram, gadījumos, kad pārzinis vai cita persona var identificēt personu, izmantojot dažādus datu veidus, piemēram, fiziskos, fizioloģiskos, ģenētiskos, finanšu vai sociālos datus (vecuma, dzimuma, profesijas, atrašanās vietas, ģimenes stāvokļa utt. datu kombināciju). Šādā gadījumā datus nevar uzskatīt par anonīmiem un uz tiem attiecas Konvencijas noteikumi.

20. Ja dati ir padarīti anonīmi, ir jāievieš atbilstoši līdzekļi, lai novērstu datu subjektu atkārtotu identificēšanu; jo īpaši ir jāizmanto visi tehniskie līdzekļi, lai garantētu, ka persona nav identificējama vai vairs nav identificējama. Tie ir regulāri jāpārskata, ņemot vērā straujo tehnoloģiju attīstības tempu.

#### b) un c) apakšpunkts – “datu apstrāde”

21. “Datu apstrāde” sākas no brīža, kad tiek vākti personas dati, un aptver visas darbības, ko daļēji vai pilnīgi automatizēti veic ar personas datiem. Ja datus neapstrādā automatizēti, datu apstrāde ir darbība vai darbību kopums, ko veic ar personas datiem šādu datu strukturētā kopumā, kas ir pieejams vai izgūstams saskaņā ar īpašiem kritērijiem un ar ko datu pārzinis vai cita persona var meklēt, kombinēt vai sasaistīt datus, kas attiecas uz konkrētu datu subjektu.

#### d) apakšpunkts – “pārzinis”

22. “Pārzinis” ir persona vai struktūra, kas ir pilnvarota pieņemt lēmumus par datu apstrādes nolūku un līdzekļiem, neatkarīgi no tā, vai šīs pilnvaras ir likumīgi noteiktas vai izriet no faktiskajiem apstākļiem, kas jānovērtē katrā atsevišķā gadījumā. Dažkārt var būt vairāki datu pārziņi vai līdzpārziņi (kas ir kopīgi atbildīgi par datu apstrādi un var būt atbildīgi par dažādiem attiecīgās apstrādes aspektiem). Novērtējot, vai persona vai struktūra ir pārzinis, īpaši jāņem vērā, vai attiecīgā persona vai iestāde nosaka apstrādes pamatojumu, proti, tās nolūkus un tai izmantotos līdzekļus. Šajā novērtējumā jāņem vērā arī tādi būtiski faktori kā tas, vai attiecīgā persona vai struktūra kontrolē apstrādes metodes, izvēlētie apstrādājamie dati un tas, kam ir atļauts piekļūt datiem. Par apstrādātājiem uzskata personas, kas nav tieši pakļautas pārzinim un veic apstrādi pārziņa vārdā un tikai saskaņā ar pārziņa norādījumiem. Datu pārzinis ir atbildīgs par datu apstrādi arī tad, ja apstrādātājs apstrādā datus viņa vārdā.

#### e) apakšpunkts – “saņēmējs”

23. “Saņēmējs” ir fiziska vai juridiska persona, kura saņem personas datus vai kurai tiek darīti pieejami personas dati. Atkarībā no apstākļiem saņēmējs var būt vai nu pārzinis, vai apstrādātājs. Piemēram, uzņēmums var nosūtīt konkrētus darbinieku datus valsts pārvaldes iestādei, kas tos kā pārzinis apstrādā nodokļu vajadzībām. Tā šos datus var nosūtīt uzņēmumam, kas sniedz glabāšanas pakalpojumus un darbojas kā apstrādātājs. Saņēmējs var būt valsts iestāde vai struktūra, kurai ir piešķirtas tiesības pildīt sabiedrisku funkciju, bet, ja iestāde vai struktūra saņemtos datus apstrādā saistībā ar konkrētu izmeklēšanu saskaņā ar piemērojamiem tiesību aktiem, šo valsts iestādi vai struktūru neuzskata par saņēmēju. Valsts iestāžu nosūtītiem informācijas pieprasījumiem vienmēr jābūt rakstveida, pamatotiem un neregulāriem, un tie nedrīkst attiekties uz visu kartotēku kopumā vai novest pie kartotēku savstarpējas sasaistīšanas. Personas datu apstrādei, ko veic minētās valsts iestādes, jāatbilst piemērojamajiem datu aizsardzības noteikumiem saskaņā ar apstrādes nolūkiem.

#### f) apakšpunkts – “apstrādātājs”

24. “Apstrādātājs” ir fiziska vai juridiska persona (kas nav datu pārziņa darbinieks), kura pārziņa vārdā un saskaņā ar pārziņa norādījumiem apstrādā personas datus. Pārziņa sniegtie norādījumi nosaka, kādas darbības apstrādātājs drīkst veikt ar personas datiem.

### 3. pants. Darbības joma

25. Saskaņā ar *1. punktu* Pusēm ir jāpiemēro šī konvencija visai to jurisdikcijā veiktajai personas datu apstrādei gan valsts, gan privātajā sektorā.

26. Aizsardzības piemērošanas joma tiek piesaistīta Pušu “jurisdikcijas” jēdzienam, lai labāk izturētu laika pārbaudi un pielāgotos nepārtrauktajai tehnoloģiju attīstībai.

27. Šā panta *2. punkts* Konvencijas darbības jomu neattiecina uz apstrādi, ko veic tikai saistībā ar personiskiem vai mājsaimnieciskiem pasākumiem. Šāds izņēmums paredzēts, lai neuzliktu nepamatotus pienākumus attiecībā uz datu apstrādi, ko fiziskas personas veic privātajā sfērā, īstenojot ar privāto dzīvi saistītas darbības. Personiski vai mājsaimnieciski pasākumi ir pasākumi, kas cieši un objektīvi ir saistīti ar personas privāto dzīvi un kas ievērojami neskar citu personu personisko sfēru. Šiem pasākumiem nav profesionālu vai komerciālu aspektu un tie ir saistīti tikai ar tādiem personiskiem vai mājsaimnieciskiem pasākumiem kā, piemēram, ģimenes vai privātu attēlu glabāšana datorā, draugu un ģimenes locekļu kontaktinformācijas saraksta izveide, sarakste utt. Datu apmaiņa privātajā sfērā jo īpaši ietver datu apmaiņu starp ģimenes locekļiem, ierobežotā draugu lokā vai lokā, kura lielums ir ierobežots un kura pamatā ir personiskas attiecības vai īpaša uzticēšanās.

28. Tas, vai pasākumi ir “tikai personiski vai mājsaimnieciski pasākumi”, ir atkarīgs no apstākļiem. Piemēram, izņēmums neattiecas uz gadījumiem, kad personas dati tiek darīti pieejami lielam skaitam personu vai personām, kas acīmredzami nepieder pie privātās sfēras, piemēram, publiskā tīmekļvietnē internetā. Tāpat kameras sistēmas darbību, kuras rezultātā personu videoieraksts tiek uzglabāts nepārtraukta ieraksta iekārtā, piemēram, cietajā diskā, un ko fiziska persona ir uzstādījusi pie savas ģimenes mājokļa ar mērķi aizsargāt mājokļa īpašnieku īpašumu, veselību un dzīvību, bet kas kaut daļēji aptver publisku telpu un attiecīgi ir vērsta ārpus personas, kura šādā veidā apstrādā datus, privātās telpas, nevar uzskatīt par tikai un vienīgi “personisku vai mājsaimniecisku” pasākumu.[[7]](#footnote-8)

29. Tomēr Konvencija attiecas uz datu apstrādi, ko veic personas, kas nodrošina personas datu apstrādes līdzekļus šādiem personiskiem vai mājsaimnieciskiem pasākumiem.

30. Lai gan Konvencija attiecas uz fizisku personu datu apstrādi, Puses valsts tiesību aktos paredzēto aizsardzību var attiecināt arī uz juridisku personu datiem, lai aizsargātu to leģitīmās intereses. Konvencija attiecas uz dzīvām personām; to nav paredzēts piemērot mirušu cilvēku personas datiem. Tomēr tas neliedz Pusēm attiecināt aizsardzību uz mirušiem cilvēkiem.

### II nodaļa. Personas datu aizsardzības pamatprincipi

**4. pants. Pušu pienākumi**

31. Kā norādīts šajā pantā, Konvencija uzliek Pusēm pienākumu ieviest tās noteikumus valsts normatīvajos aktos un nodrošināt to efektīvu piemērošanu praksē. Tas jādara, ņemot vērā piemērojamo tiesību sistēmu un pieeju attiecībā uz starptautisko līgumu iekļaušanu.

32. Termins “Pušu normatīvie akti” saskaņā ar konkrētās valsts tiesību un konstitucionālo sistēmu apzīmē visus izpildāmos noteikumus neatkarīgi no tā, vai tās ir rakstītās tiesības vai judikatūra. Tiem jāatbilst piekļūstamības un paredzamības (jeb prognozējamības) kvalitatīvajām prasībām. Tas nozīmē, ka normatīvajiem aktiem jābūt pietiekami skaidriem, lai ļautu fiziskām personām un citām struktūrām regulēt savu rīcību, ņemot vērā to darbības sagaidāmās juridiskās sekas, un ka personām, uz kurām tiesību akti varētu attiekties, jābūt piekļuvei tiem. Tie ietver noteikumus, kas uzliek pienākumus vai piešķir tiesības personām (gan fiziskām, gan juridiskām) vai kas regulē valsts iestāžu organizāciju, pilnvaras un atbildības jomas, vai nosaka procedūras. Jo īpaši tie ietver valstu konstitūcijas un visus rakstītos likumdevēju iestāžu aktus (formālā nozīmē – tiesību aktus), kā arī visus regulatīvos pasākumus (dekrētus, noteikumus, rīkojumus un administratīvās direktīvas), kuru pamatā ir šādi tiesību akti. Tie attiecas arī uz starptautiskām konvencijām, kas piemērojamas valsts tiesību aktos, tostarp ES tiesību aktos. Turklāt tie ietver visus pārējos vispārīgos publisko tiesību vai privāttiesību statūtus (ieskaitot līgumtiesības), kā arī tiesu nolēmumus valstīs, kurās ir spēkā anglosakšu tiesības, vai visās valstīs – iedibināto judikatūru, ar ko interpretē rakstītās tiesības. Tie ietver arī jebkuru profesionālas struktūras aktu, ko tā izdod saskaņā ar likumdevēja deleģētām pilnvarām un neatkarīgām likumdošanas pilnvarām.

33. Šādus “Pušu normatīvos aktus” var lietderīgi pastiprināt ar brīvprātīgiem regulēšanas pasākumiem datu aizsardzības jomā, piemēram, ar labās prakses kodeksiem vai profesionālās ētikas kodeksiem. Tomēr šādi brīvprātīgi pasākumi paši par sevi nav pietiekami, lai nodrošinātu pilnīgu atbilstību Konvencijai.

34. Attiecībā uz starptautiskām organizācijām[[8]](#footnote-9) dažos gadījumos šādu starptautisku organizāciju tiesību aktus var piemērot tieši šādu organizāciju dalībvalstu līmenī atkarībā no katras valsts tiesību sistēmas.

35. Būtiska nozīme ir to pasākumu piemērošanas efektivitātei, ar kuriem īsteno Konvencijas noteikumus. Veicot vispārēju novērtējumu par to, cik efektīvi Puse īsteno Konvencijas noteikumus, jāņem vērā uzraudzības iestādes (vai iestāžu) loma un visi datu subjektiem pieejamie tiesiskās aizsardzības līdzekļi.

36. Turklāt *2. punktā* ir noteikts, ka attiecīgās Puses veic pasākumus, ar kuriem īsteno Konvenciju, un tie stājas spēkā brīdī, kad Puse ratificē šo konvenciju vai pievienojas tai, proti, kad Konvencija kļūst juridiski saistoša Pusei. Šā noteikuma mērķis ir ļaut Konvencijas komitejai pārbaudīt, vai ir veikti visi “nepieciešamie pasākumi”, lai nodrošinātu, ka Konvencijas puses ievēro saistības un valsts tiesību aktos nodrošina sagaidāmo datu aizsardzības līmeni. Procedūrai un kritērijiem, ko izmanto šajā pārbaudē, jābūt skaidri definētiem Konvencijas komitejas reglamentā.

37. Šā panta *3. punktā* izteikta Pušu apņemšanās aktīvi iesaistīties savu saistību izpildes novērtēšanā, lai nodrošinātu regulāru Konvencijas principu īstenošanas (tostarp tās efektivitātes) novērtējumu. Šāda aktīva iesaiste var ietvert ziņojumus, ko Puses iesniedz par datu aizsardzības tiesību aktu piemērošanu.

38. Īstenojot 3. punktā piešķirtās pilnvaras, Konvencijas komiteja nevērtē, vai Puse ir veikusi efektīvus pasākumus, ciktāl tā ir izmantojusi izņēmumus un ierobežojumus saskaņā ar šo konvenciju. Proti, saskaņā ar 11. panta 3. punkta a) apakšpunktu Pusei nav jāsniedz Konvencijas komitejai slepena informācija.

39. Konvencijas komiteja vērtē Puses saistību izpildi, pamatojoties uz objektīvu, taisnīgu un pārredzamu procedūru, ko izstrādājusi Konvencijas komiteja un kas ir pilnīgi izklāstīta tās reglamentā.

### 5. pants. Datu apstrādes likumība un datu kvalitāte

40. Šā panta *1. punktā* ir noteikts, ka datu apstrādei jābūt samērīgai, proti, atbilstīgai tās leģitīmajam nolūkam, turklāt jāņem vērā datu subjekta intereses, tiesības un brīvības vai sabiedrības intereses. Šāda datu apstrāde nedrīkst izraisīt nesamērīgu iejaukšanos šādās interesēs, tiesībās un brīvībās. Proporcionalitātes princips ir jāievēro visos apstrādes posmos, arī sākuma posmā, t. i., lemjot par datu apstrādes veikšanu vai neveikšanu.

41. Šā panta *2. punktā* ir noteikti divi būtiski alternatīvi likumīgas apstrādes priekšnosacījumi – personas piekrišana vai likumā noteikts leģitīms pamats. Konvencijas 5. panta 1., 2., 3. un 4. punkts ir kumulatīvi, un tie ir jāievēro, lai nodrošinātu datu apstrādes likumību.

42. Datu subjekta piekrišanai jābūt brīvai, konkrētai, apzinātai un viennozīmīgai. Šādai piekrišanai jābūt brīvai apzinātas izvēles izpausmei, ko sniedz vai nu ar paziņojumu (kas var būt rakstisks, sniegts ar elektroniskiem saziņas līdzekļiem, vai mutisks) vai ar skaidru apstiprinošu darbību un kas attiecīgajā kontekstā skaidri norāda uz piekrišanu ierosinātajai personas datu apstrādei. Tāpēc klusēšana, atturēšanās no darbības vai iepriekš apstiprinātas veidlapas vai iepriekš atzīmēti laukumi nav uzskatāmi par piekrišanu. Piekrišanai jāatteicas uz visām apstrādes darbībām, kurām ir viens un tas pats nolūks vai nolūki (ja ir vairāki nolūki, piekrišana jāsniedz par katru nolūku atsevišķi). Iespējami gadījumi, kad piekrišanas lēmumi ir atšķirīgi (piemēram, ja nolūks ir viens, bet datu veids ir atšķirīgs, piemēram, veselības dati un atrašanās vietas dati – šādos gadījumos datu subjekts var piekrist atrašanās vietas datu apstrādei, bet ne veselības datu apstrādei). Datu subjektam jābūt informētam par sava lēmuma sekām (ko nozīmē piekrišana un uz ko tā attiecas). Datu subjektu nedrīkst ne tieši, ne netieši nepamatoti ietekmēt vai uz to izdarīt spiedienu (vai nu ekonomisku, vai cita veida), un piekrišana nav uzskatāma par brīvprātīgi sniegtu, ja datu subjektam nav patiesas vai brīvas izvēles vai ja viņš nespēj noraidīt vai atcelt piekrišanu, neradot kaitējumu.

43. Saistībā ar zinātnisko pētniecību datu vākšanas brīdī bieži vien nav iespējams pilnīgi noteikt personas datu apstrādes nolūku zinātniskās pētniecības mērķiem. Tāpēc datu subjektiem jāļauj sniegt piekrišanu noteiktām zinātniskās pētniecības jomām, ievērojot atzītas zinātniskās pētniecības ētikas normas. Datu subjektiem jābūt iespējai sniegt piekrišanu tikai attiecībā uz noteiktām pētniecības jomām vai pētniecības projektu daļām, ciktāl to pieļauj paredzētais nolūks.

44. Piekrišana neatceļ nepieciešamību ievērot personas datu aizsardzības pamatprincipus, kas izklāstīti Konvencijas II nodaļā, un joprojām ir jāievēro, piemēram, apstrādes samērīgums.

45. Datu subjektam ir tiesības jebkurā brīdī atsaukt piekrišanu (kas jānošķir no atsevišķām tiesībām iebilst pret apstrādi). Tas neietekmē tādas datu apstrādes likumību, kas notikusi, pirms datu pārzinis ir saņēmis piekrišanas atsaukumu, taču neļauj turpināt datu apstrādi, izņemot gadījumus, kad šādu apstrādi pamato cits likumā noteikts leģitīms pamats.

46. Šā panta *2. punktā* minētais jēdziens “likumā noteikts leģitīms pamats” *inter alia* ietver datu apstrādi, kas nepieciešama, lai izpildītu līgumu (vai pēc datu subjekta pieprasījuma īstenotu pasākumus pirms līguma noslēgšanas), kura puse ir datu subjekts; datu apstrādi, kas nepieciešama, lai aizsargātu datu subjekta vai citas personas vitālās intereses; datu apstrādi, kas nepieciešama, lai izpildītu uz pārzini attiecināmu juridisku pienākumu un datu apstrādi, ko veic, pamatojoties uz sabiedrības interesēm vai primārajām pārziņa vai trešās personas leģitīmajām interesēm.

47. Datu apstrādei, ko veic sabiedrības interesēs, jābūt noteiktai tiesību aktos, un to *inter alia* veic saistībā ar monetāriem, budžeta un nodokļu jautājumiem, sabiedrības veselību un sociālo nodrošinājumu, noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu un saukšanu pie atbildības par tiem, kriminālsodu izpildi, valsts drošības aizsardzību, aizstāvību, reglamentētu profesiju ētikas kodeksu pārkāpumu novēršanu, izmeklēšanu, atklāšanu un saukšanu pie atbildības par tiem, civilprasību izpildi un tiesu varas neatkarības un tiesvedības aizsardzību. Datu apstrādes pamatā var būt gan sabiedrības intereses, gan datu subjekta vitālās intereses, piemēram, ja dati tiek apstrādāti humānos nolūkos, tostarp dzīvību apdraudošu epidēmiju un to izplatīšanās monitoringam vai humānās ārkārtas situācijās. Pēdējā no minētajām situācijām var būt saistīta ar dabas katastrofām, kad uz noteiktu laiku saistībā ar ārkārtas situāciju var būt nepieciešama bezvēsts pazudušu cilvēku personas datu apstrāde, kas jāizvērtē katrā atsevišķā gadījumā. Tā var rasties arī bruņotu konfliktu vai citas vardarbības gadījumos.[[9]](#footnote-10) Personas datu apstrādi, ko oficiālās iestādes veic, lai sasniegtu konstitucionālajās tiesībās vai starptautiskajās publiskajās tiesībās noteiktos mērķus attiecībā uz oficiāli atzītām reliģiskajām apvienībām, arī var uzskatīt par veiktu sabiedrības interesēs.

48. Šā panta *3. un 4. punktā* ir izklāstīti likumīgas apstrādes nosacījumi. Personas dati ir jāapstrādā likumīgi, taisnīgi un pārredzami. Personas dati arī ir jāvāc skaidros, konkrētos un leģitīmos nolūkos, un attiecīgie dati ir jāapstrādā atbilstīgi minētajiem nolūkiem vai vismaz ar tiem saderīgā veidā. Atsauce uz “konkrētiem” nolūkiem norāda, ka datus nav atļauts apstrādāt nedefinētiem, neprecīziem vai neskaidriem nolūkiem. Leģitīmu nolūku nosaka atbilstīgi apstākļiem, jo mērķis ir nodrošināt, ka katrā atsevišķā gadījumā tiek ievērots visu tiesību, brīvību un interešu līdzsvars – tiesības uz personas datu aizsardzību, no vienas puses, un citu tiesību aizsardzība, no otras puses, piemēram, datu subjekta intereses un datu pārziņa vai sabiedrības intereses.

49. Saderīgas izmantošanas jēdziens nedrīkst negatīvi ietekmēt apstrādes pārredzamību, juridisko noteiktību, paredzamību vai godīgumu. Personas datu turpmāku apstrādi nedrīkst veikt tādā veidā, ko datu subjekts var uzskatīt par neparedzētu, neatbilstošu vai citādi apstrīdamu. Lai pārliecinātos, vai turpmākas apstrādes nolūks ir saderīgs ar nolūku, kādā personas dati ir sākotnēji vākti, pārzinim – pēc tam, kad ir izpildītas visas prasības attiecībā uz sākotnējās apstrādes likumīgumu, – *inter alia* jāņem vērā jebkura saikne starp minētajiem nolūkiem un paredzētās turpmākās apstrādes nolūkiem; konteksts, kādā personas dati ir vākti, jo īpaši pamatotas datu subjektu gaidas, kuru pamatā ir to attiecības ar pārzini, attiecībā uz datu turpmāku izmantošanu; personas datu veids; sekas, ko paredzētā turpmākā apstrāde rada datu subjektiem un atbilstošas garantijas gan sākotnējās, gan paredzētajās turpmākajās apstrādes darbībās.

50. Šā panta *4. punkta b) apakšpunktā* minētā turpmākā personas datu apstrāde arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēsturiskās pētniecības nolūkos vai statistikas nolūkos *a priori* tiek uzskatīta par saderīgu, ja ir ieviesti citi aizsardzības pasākumi (piemēram, datu anonimizācija vai datu pseidonimizācija, izņemot gadījumus, kad ir jāsaglabā identificējama forma; dienesta noslēpuma noteikumi; noteikumi, kas reglamentē ierobežotu piekļuvi datiem un datu paziņošanu iepriekš minētajos nolūkos, jo īpaši saistībā ar statistiku un valsts arhīviem, kā arī citi tehniski un organizatoriski datu drošības pasākumi) un ja šīs darbības principā nepieļauj iespēju iegūto informāciju izmantot lēmumu pieņemšanai vai pasākumu īstenošanai attiecībā uz konkrēto personu. Jēdziens “statistikas nolūki” attiecas uz statistikas pārskatu sagatavošanu vai sagrupētu statistikas rezultātu sagatavošanu. Statistikas mērķis ir analizēt un raksturot masveida vai kolektīvas parādības attiecīgajā populācijā.[[10]](#footnote-11) Statistikas nolūkus var īstenot gan valsts, gan privātais sektors. “Zinātniskās pētniecības nolūkos” datus apstrādā, lai sniegtu pētniekiem informāciju, kas palīdz izprast parādības dažādās zinātnes jomās (epidemioloģijā, psiholoģijā, ekonomikā, socioloģijā, lingvistikā, politikas zinātnēs, kriminoloģijā utt.), lai izstrādātu pastāvīgus principus, uzvedības likumsakarības vai cēloņsakarības modeļus, kas aptver visas personas, uz kurām tie attiecas.[[11]](#footnote-12) “Vēsturiskās pētniecības nolūki” ietver ģenealoģisku izpēti. Gadījumos, kas ietver sabiedrības intereses, “arhivēšanas nolūki sabiedrības interesēs” var ietvert arī privātu uzņēmumu arhīvus.

51. Personas datiem, kurus apstrādā, jābūt adekvātiem, atbilstīgiem un nav jābūt pārmērīgiem. Turklāt datiem jābūt precīziem un vajadzības gadījumā tie regulāri jāatjaunina.

52. Šā panta *4. punkta c) apakšpunktā* minētā prasība, ka datiem “nav jābūt pārmērīgiem”, pirmkārt, nozīmē to, ka datu apstrādē jāietver tikai tas, kas nepieciešams apstrādes nolūkos. Tie jāapstrādā tikai tad un tik ilgi, kamēr apstrādes nolūku nav iespējams pienācīgi sasniegt, apstrādājot informāciju, kas nav saistīta ar personas datiem. Turklāt šī prasība attiecas ne tikai uz personas datu kvantitāti, bet arī uz personas datu kvalitāti. Personas dati, kas ir adekvāti un atbilstīgi, bet kas radītu nesamērīgu iejaukšanos attiecīgajās pamattiesībās un pamatbrīvībās, jāuzskata par pārmērīgiem un nav jāapstrādā.

53. Šā panta *4. punkta e) apakšpunktā* minētā prasība par personas datu glabāšanas termiņu nozīmē, ka dati jādzēš, tiklīdz ir sasniegts nolūks, kādam tie tika apstrādāti, vai ka tie jāglabā tādā veidā, kas neļauj tieši vai netieši identificēt datu subjektu.

54. Saskaņā ar 11. panta 1. punktu ir pieļaujami ierobežoti 5. panta 4. punkta piemērošanas izņēmumi.

### 6. pants. Īpašas datu kategorijas

55. Noteiktu datu veidu apstrāde vai noteiktu datu apstrāde, iegūstot sensitīvu informāciju, ko tie atklāj, var radīt interešu, tiesību un brīvību aizskārumu. Tas var notikt, piemēram, gadījumos, kad pastāv diskriminācijas vai kaitējuma risks personas cieņai vai fiziskajai neaizskaramībai, kad ir skarta datu subjekta intīmākā dzīves joma, piemēram, viņa seksuālā dzīve vai seksuālā orientācija, vai kad datu apstrāde var ietekmēt nevainīguma prezumpciju. Tā ir jāatļauj tikai tad, ja tiesību aktos ir paredzēti pienācīgi aizsardzības līdzekļi, kas papildina citus Konvencijā paredzētos aizsardzības noteikumus. Prasība nodrošināt pienācīgus aizsardzības līdzekļus, kas papildina Konvencijas noteikumus, neizslēdz 11. pantā paredzēto iespēju pieļaut izņēmumus un ierobežojumus attiecībā uz datu subjektu tiesībām, kas piešķirtas saskaņā ar 9. pantu.

56. Lai nepieļautu nelabvēlīgu ietekmi uz datu subjektu, sensitīvu datu apstrāde leģitīmos nolūkos jāpapildina ar pienācīgiem aizsardzības līdzekļiem (kas pielāgoti attiecīgajiem riskiem un aizsargājamajām interesēm, tiesībām un brīvībām), piemēram, ar kādu no tālāk minētajiem vai visiem minētajiem: datu subjekta skaidri izteikta piekrišana; tiesību akti, kuri attiecas uz paredzēto apstrādes nolūku un līdzekļiem vai kuros norādīti izņēmuma gadījumi, kad šāda apstrāde ir atļauta; dienesta noslēpuma glabāšanas pienākums; pasākumi, ko veic pēc riska analīzes; konkrēts un atbilstīgs organizatorisks vai tehnisks drošības pasākums (piemēram, datu šifrēšana).

57. Konkrēti datu apstrādes veidi var ietvert īpašu risku datu subjektiem neatkarīgi no apstrādes konteksta. Tas, piemēram, attiecas uz tādu ģenētisko datu apstrādi, kas var būt iegūti no personām un kas var atklāt informāciju par attiecīgās personas, kā arī trešo personu veselību vai izcelsmi. Ģenētiskie dati ir visi dati, kas attiecas uz personas ģenētiskajām īpašībām, kuras ir iedzimtas vai iegūtas agrīnās prenatālās attīstības posmā, jo tos iegūst no attiecīgās personas bioloģiskā parauga, veicot hromosomu, DNS vai RNS analīzi vai jebkuru citu elementu analīzi, kas ļauj iegūt līdzvērtīgu informāciju. Līdzīgi riski rodas, apstrādājot datus, kuri saistīti ar noziedzīgiem nodarījumiem (kas ietver aizdomas par noziedzīgiem nodarījumiem), notiesājošiem spriedumiem krimināllietās (pamatojoties uz krimināllikumu un saistībā ar tiesvedību krimināllietās) un saistītiem drošības pasākumiem (piemēram, saistībā ar brīvības atņemšanu) un kuru apstrādei jānodrošina atbilstoši datu subjektu tiesību un brīvību aizsardzības pasākumi.

58. Arī biometrisko datu – datu, ko iegūst, ar īpašiem tehniskiem paņēmieniem apstrādājot datus par personas fiziskajām, bioloģiskajām vai psiholoģiskajām īpašībām, un kas ļauj unikāli identificēt vai autentificēt personu – apstrādi uzskata par sensitīvu, ja to tieši izmanto datu subjekta unikālai identificēšanai.

59. Lai noteiktu, vai dati ir sensitīvi, svarīgs ir attēlu apstrādes konteksts. Attēlu apstrāde parasti neietver sensitīvu datu apstrādi, jo biometrisko datu definīcija uz attēliem attiecas tikai tad, ja tos apstrādā ar īpašu tehnisko līdzekli, kas ļauj unikāli identificēt vai autentificēt personu. Turklāt, ja attēlu apstrādi veic, lai noteiktu ar rasi, etnisko piederību vai veselību saistītu informāciju (sk. nākamo punktu), šādu apstrādi uzskata par sensitīvu datu apstrādi. Toties tādu attēlu apstrādi, ko drošības nolūkos iepirkšanās zonā veic videonovērošanas sistēma, parasti neuzskata par sensitīvu datu apstrādi.

60. Ja sensitīvu datu apstrādi veic, lai iegūtu konkrētu informāciju, ko tie ietver, tā var nelabvēlīgi ietekmēt datu subjektu tiesības. Lai gan daudzos gadījumos uzvārdu apstrāde nevar radīt risku fiziskām personām (piemēram, vienotā algu izmaksas sarakstā), dažkārt šāda apstrāde var ietvert sensitīvus datus, piemēram, ja apstrādes nolūks ir atklāt personu etnisko izcelsmi vai reliģisko piederību, pamatojoties uz uzvārdu lingvistisko izcelsmi. Informācija par veselību ietver informāciju, kas attiecas uz personas pagātnes, tagadnes un nākotnes fizisko vai mentālo veselību un kas var norādīt uz to, vai personai ir veselības traucējumi, vai tā ir vesela. Tādu attēlu apstrādi, kuros redzamas personas, kas valkā brilles ar bieziem stikliem, personas ar lauztu kāju, ādas apdegumiem vai citām redzamām pazīmēm, kas saistītas ar personas veselību, var uzskatīt par sensitīvu datu apstrādi tikai tad, ja apstrādi veic, pamatojoties uz informāciju par veselību, ko var iegūt no attēliem.

61. Apstrādājot sensitīvus datus statistikas nolūkiem, tie jāvāc tā, lai datu subjekts nebūtu identificējams. Sensitīvu datu vākšana bez identifikācijas datiem ir aizsardzības pasākums 6. panta izpratnē. Ja ir likumīga vajadzība vākt sensitīvus datus identificējamā veidā statistikas nolūkiem (piemēram, lai varētu veikt atkārtotu vai longitudinālu pētījumu), ir jāievieš atbilstoši aizsardzības pasākumi.[[12]](#footnote-13)

### 7. pants. Datu drošība

62. Datu pārzinim un attiecīgā gadījumā apstrādātājam ir jāveic noteikti tehniski un organizatoriski drošības pasākumi saistībā ar katru apstrādi, ņemot vērā iespējamās nelabvēlīgās sekas personai, personas datu veidu, apstrādāto personas datu apjomu, apstrādei izmantotās tehniskās arhitektūras ievainojamības pakāpi, nepieciešamību ierobežot piekļuvi datiem, prasības attiecībā uz ilgstošu glabāšanu utt.

63. Veicot drošības pasākumus, jāņem vērā jaunākie sasniegumi attiecībā uz datu drošības metodēm un paņēmieniem datu apstrādes jomā. To izmaksām jābūt samērīgām ar potenciālo risku nopietnību un iespējamību. Drošības pasākumi ir jāpārskata un vajadzības gadījumā jāatjaunina.

64. Lai gan drošības pasākumu mērķis ir novērst virkni risku, *2. punktā* ir paredzēts īpašs pienākums gadījumos, kad tomēr ir noticis datu aizsardzības pārkāpums, kas var nopietni ietekmēt personas pamattiesības un pamatbrīvības. Piemēram, par “nopietnu” pārkāpumu var uzskatīt tādu datu izpaušanu, uz kuriem attiecas profesionālās konfidencialitātes pienākums vai kuri var radīt finansiālu kaitējumu, kaitējumu reputācijai vai fizisku kaitējumu, vai pazemojumu.

65. Ja ir noticis šāds datu aizsardzības pārkāpums, pārzinim par incidentu ir jāpaziņo attiecīgajām uzraudzības iestādēm, ievērojot 11. panta 1. punktā pieļauto izņēmumu. Tā ir minimālā prasība. Pārzinim ir jāziņo uzraudzības iestādēm arī par jebkādiem pasākumiem, kas veikti un/vai ierosināti, lai atrisinātu pārkāpumu un novērstu tā iespējamās sekas.

66. Paziņojums, ko pārzinis sniedz uzraudzības iestādēm, neliedz sniegt citus papildu paziņojumus. Piemēram, pārzinis var atzīt, ka ir nepieciešams informēt arī datu subjektus, jo īpaši tad, ja datu aizsardzības pārkāpums var būtiski apdraudēt personu tiesības un brīvības, piemēram, radīt diskrimināciju, identitātes zādzību vai viltošanu, finanšu zaudējumus, kaitējumu reputācijai, ar dienesta noslēpumu aizsargātu datu konfidencialitātes zaudēšanu vai jebkādu citu īpaši nelabvēlīgu ekonomisko vai sociālo situāciju, un jāsniedz tiem atbilstīga un lietderīga informācija, proti, par kontaktpunktiem un par iespējamiem pasākumiem, kurus tie var veikt, lai mazinātu pārkāpuma nelabvēlīgo ietekmi. Ja pārzinis pēc savas iniciatīvas neinformē datu subjektu par datu aizsardzības pārkāpumu, ir jāļauj uzraudzības iestādei pēc pārkāpuma iespējamo nelabvēlīgo seku izvērtēšanas pieprasīt, lai pārzinis to izdara. Var būt vēlams paziņot arī citām attiecīgajām iestādēm, piemēram, par datorsistēmu drošību atbildīgajām iestādēm.

### 8. pants. Apstrādes pārredzamība

67. Apstrādājot datus, pārzinim ir jārīkojas pārredzami, lai nodrošinātu godīgu apstrādi un datu subjektiem ļautu izprast un tādējādi pilnīgi izmantot tiesības saistībā ar šādu datu apstrādi.

68. Pārzinim, tieši vai netieši (nevis ar datu subjekta, bet ar trešās personas starpniecību) vācot datu subjektu datus, ir pienākums proaktīvi sniegt konkrētu būtisku informāciju datu subjektiem, ņemot vērā iespēju piemērot izņēmumus saskaņā ar 11. panta 1. punktu. Informāciju par pārziņa (vai līdzpārziņu) vārdu, uzvārdu vai nosaukumu un adresi, datu apstrādes juridisko pamatu un nolūkiem, apstrādāto datu kategorijām un saņēmējiem, kā arī par tiesību izmantošanas līdzekļiem var sniegt jebkādā piemērotā formātā (vai nu izmantojot tīmekļvietni, tehnoloģiskus rīkus personiskajās ierīcēs utt.), ja vien informācija datu subjektam tiek sniegta godīgi un efektīvi. Sniegtajai informācijai jābūt viegli pieejamai, salasāmai, saprotamai un pielāgotai attiecīgajiem datu subjektiem (piemēram, vajadzības gadījumā bērniem saprotamā valodā). Jāsniedz arī jebkāda papildu informācija, kas nepieciešama, lai nodrošinātu godīgu datu apstrādi, vai kas ir noderīga šādam nolūkam, piemēram, datu glabāšanas ilgums, datu apstrādes pamatojums vai informācija par datu nosūtīšanu citai Pusei vai trešajām pusēm (arī par to, vai attiecīgā trešā puse nodrošina pienācīgu datu aizsardzības līmeni, vai par pasākumiem, ko pārzinis veic, lai garantētu šādu pienācīgu datu aizsardzības līmeni).

69. Pārzinim šī informācija nav jāsniedz, ja datu subjekts to jau ir saņēmis, vai netiešas datu vākšanas gadījumā ar trešo pušu starpniecību, ja apstrāde ir skaidri paredzēta tiesību aktos vai ja tas nav iespējams vai ir saistīts ar nesamērīgi lielām pūlēm, jo datu subjekts nav tieši identificējams, vai ja pārzinim nav iespējas sazināties ar datu subjektu. Šāda neiespējamība var būt gan juridiska (piemēram, saistībā ar kriminālizmeklēšanu), gan praktiska (piemēram, ja pārzinis apstrādā tikai attēlus un nezina datu subjektu vārdus, uzvārdus un kontaktinformāciju).

70. Datu pārzinis var izmantot visus līdzekļus, kas ir pieejami, tostarp pieejami arī izmaksu ziņā, un pamatoti, lai informētu datu subjektus kopīgi (tīmekļvietnē vai ar publisku paziņojumu) vai atsevišķi. Ja tas nav iespējams apstrādes sākumā, to var darīt apstrādes gaitā, piemēram, kad pārzinim kāda jauna iemesla dēļ jāsazinās ar datu subjektu.

### 9. pants. Datu subjekta tiesības

71. Šajā pantā uzskaitītas tiesības, kuras ikvienai fiziskai personai jāspēj īstenot saistībā ar tās personas datu apstrādi. Katra Puse atbilstīgi tās tiesiskajam regulējumam nodrošina, ka visas šīs tiesības ir pieejamas ikvienam datu subjektam kopā ar nepieciešamajiem juridiskajiem un praktiskajiem, atbilstīgajiem un efektīvajiem līdzekļiem to īstenošanai.

72. Šīs tiesības ir:

* ikvienas fiziskas personas tiesības nebūt tāda lēmuma subjektam, kas to ievērojami ietekmē un kā pamatā ir tikai automatizēta apstrāde, neņemot vērā attiecīgās personas viedokli (*a) apakšpunkts*);
* ikvienas fiziskas personas tiesības saņemt apstiprinājumu par tās datu apstrādi un piekļūt datiem pieņemamos intervālos bez pārmērīgas kavēšanās vai izdevumiem (*b) apakšpunkts*);
* ikvienas fiziskas personas tiesības pēc pieprasījuma saņemt informāciju par datu apstrādes pamatojumu, ja minētās apstrādes rezultātus piemēro attiecīgajai personai (*c) apakšpunkts*);
* ikvienas fiziskas personas tiesības, pamatojoties uz tās stāvokli, iebilst pret personas datu apstrādi, ja vien pārzinis nepierāda leģitīmu apstrādes pamatojumu, kas ir svarīgāks par šīs personas interesēm, tiesībām un pamatbrīvībām (*d) apakšpunkts*);
* ikvienas fiziskas personas tiesības labot vai dzēst neprecīzus, nepareizus vai nelikumīgi apstrādātus datus (*e) apakšpunkts*);
* ikvienas fiziskas personas tiesības uz tiesiskās aizsardzības līdzekļiem, ja tiek pārkāptas minētās tiesības (*f) apakšpunkts*);
* ikvienas fiziskas personas tiesības izmantot uzraudzības iestādes palīdzību (*g) apakšpunkts*).

73. Šīs tiesības var būt jāsaskaņo ar citām tiesībām un leģitīmajām interesēm. Saskaņā ar 11. pantu tās var ierobežot tikai tad, ja tas paredzēts tiesību aktos un ir nepieciešams un samērīgs pasākums demokrātiskā sabiedrībā. Piemēram, tiesības uz personas datu dzēšanu var ierobežot, ciktāl apstrāde ir nepieciešama, lai izpildītu tiesību aktos paredzētu uz pārzini attiecināmu juridisku pienākumu vai lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras.

74. Lai gan Konvencijā nav noteikts, no kā datu subjekts var saņemt apstiprinājumu, paziņojumu, labošanu utt. vai kam var paust iebildumus vai viedokli, vairumā gadījumu tas ir pārzinis vai apstrādātājs pārziņa uzdevumā. Izņēmuma gadījumos līdzekļi piekļuves, labošanas un dzēšanas tiesību izmantošanai var būt saistīti ar uzraudzības iestādi kā starpnieku. Attiecībā uz veselības datiem tiesības var īstenot citā veidā, ne tikai ar tiešu piekļuvi. Tās var īstenot, piemēram, piesaistot veselības aprūpes speciālistu, ja tas ir datu subjekta interesēs, jo īpaši, lai palīdzētu personai saprast datus vai nodrošinātu, ka, sniedzot informāciju, tiek pienācīgi izvērtēts datu subjekta psiholoģiskais stāvoklis – protams, ievērojot ētikas principus.

75. *a) apakšpunkts.* Ir būtiski, lai personai, uz kuru var attiekties lēmums, kā pamatā ir tikai automatizēta apstrāde, būtu tiesības apstrīdēt šādu lēmumu, jēgpilni izsakot savu viedokli un argumentus. Proti, datu subjektam jābūt iespējai pirms datu izmantošanas pamatot iespējamo personas datu neprecizitāti, viņa konkrētajai situācijai neatbilstīga profila piemērošanu vai citus faktorus, kas ietekmē automatizētā lēmuma rezultātu. Tas jo īpaši attiecas uz gadījumiem, kad personas tiek stigmatizētas, piemērojot algoritmisku pamatojumu, kā rezultātā tiek ierobežotas tiesības, atteikts sociālais pabalsts vai personas kredītspēja tiek novērtēta tikai ar programmatūras palīdzību. Tomēr personas nevar izmantot šīs tiesības, ja automatizētā lēmuma pamatā ir tiesību akts, kurš pārzinim ir jāievēro un kurā noteikti piemēroti pasākumi datu subjekta tiesību, brīvību un leģitīmo interešu aizsardzībai.

76. *b) apakšpunkts.* Datu subjektiem jābūt tiesīgiem zināt, ka viņu personas dati tiek apstrādāti. Piekļuves tiesībām principā jābūt bez maksas. Tomēr *b) apakšpunkts* ir formulēts tā, lai pārzinis noteiktos apstākļos, kad pieprasījumi ir pārmērīgi, varētu piemērot saprātīgu maksu un lai aptvertu dažādas pieejas, ko Puse varētu pieņemt attiecīgos gadījumos. Šāda maksa jāpiemēro izņēmuma gadījumos un jebkurā gadījumā tai ir jābūt saprātīgai, turklāt tā nedrīkst liegt datu subjektam izmantot tiesības vai atturēt viņu no to izmantošanas. Pārzinis vai apstrādātājs var atteikties izpildīt acīmredzami nepamatotus un pārmērīgus pieprasījumus, jo īpaši tad, ja šādi pieprasījumi regulāri atkārtojas. Jebkurā gadījumā pārzinim šāds atteikums ir jāpamato. Lai nodrošinātu godīgu piekļuves tiesību izmantošanu, saziņa “saprotamā veidā” attiecas gan uz standarta digitālās saziņas saturu, gan veidu.

77. *c) apakšpunkts.* Datu subjektiem jābūt tiesīgiem zināt datu apstrādes pamatojumu, kā arī šāda pamatojuma sekas, kas ietekmējušas gūtos secinājumus, jo īpaši gadījumos, kas saistīti ar algoritmu izmantošanu automatizētai lēmumu pieņemšanai, tostarp profilēšanai. Piemēram, kredītvērtējuma noteikšanas gadījumā datu subjektiem jābūt tiesībām zināt loģiku, kas ir bijusi viņu datu apstrādes pamatā un kā rezultātā ir pieņemts pozitīvs vai negatīvs lēmums, nevis tikai informāciju par pašu lēmumu. Šo elementu izpratne palīdz efektīvi izmantot citus svarīgus aizsardzības pasākumus, piemēram, tiesības iebilst un tiesības iesniegt sūdzību kompetentajai iestādei.

78. *d) apakšpunkts.* Attiecībā uz tiesībām iebilst pārzinim var būt leģitīms datu apstrādes pamatojums, kas ir svarīgāks par datu subjekta interesēm vai tiesībām un brīvībām. Piemēram, likumīgu prasību celšanu, īstenošanu vai aizstāvēšanu vai sabiedrības drošības apsvērumus var uzskatīt par primāru leģitīmu pamatu, kas pamato apstrādes turpināšanu. Tas ir jāpierāda katrā atsevišķā gadījumā, un šāda pārliecinoša leģitīma pamatojuma nesniegšanu, vienlaikus turpinot apstrādi, var uzskatīt par nelikumīgu. Tiesības iebilst ir atšķirīgas un tiek nošķirtas no tiesībām pieprasīt datu labošanu vai dzēšanu (*e) apakšpunkts*).

79. Ja tiek izteikti iebildumi pret apstrādi tirgvedības nolūkos, bez nosacījumiem ir jādzēš personas dati, uz kuriem attiecas iebildums.

80. Tiesības iebilst var ierobežot saskaņā ar tiesību aktiem, piemēram, noziedzīgu nodarījumu izmeklēšanas vai kriminālvajāšanas nolūkā. Šādā gadījumā datu subjekts var attiecīgā gadījumā apstrīdēt pamatā esošās apstrādes likumību. Ja datu apstrāde ir balstīta uz derīgu datu subjekta piekrišanu, tiesību iebilst vietā var izmantot tiesības atsaukt piekrišanu. Datu subjekts var atsaukt savu piekrišanu un pēc tam uzņemties sekas, kas, iespējams, izriet no citiem tiesību aktiem, piemēram, pienākumu izmaksāt pārzinim kompensāciju. Tāpat, ja datu apstrādes pamatā ir līgums, datu subjekts var attiecīgi rīkoties, lai to atceltu.

81. *e) apakšpunkts.* Ja labošana vai dzēšana ir pamatota, tā jāveic bez maksas. Ja labošana un dzēšana ir panākta saskaņā ar *e) apakšpunktā* noteikto principu, par šiem labotajiem vai dzēstajiem datiem, ja iespējams, ir jāinformē sākotnējās informācijas saņēmēji, izņemot gadījumus, kad tas nav iespējams vai ir saistīts ar nesamērīgi lielām pūlēm.

82. Šā punkta *g) apakšpunkta* mērķis ir nodrošināt efektīvu datu subjektu aizsardzību, nodrošinot tiem tiesības uz uzraudzības iestādes palīdzību Konvencijā paredzēto tiesību īstenošanā. Ja datu subjekts dzīvo citas Puses teritorijā, tas var iesniegt pieprasījumu ar šīs citas Puses norādītās iestādes starpniecību. Palīdzības pieprasījumā jāiekļauj pietiekama informācija, lai būtu iespējams identificēt attiecīgo datu apstrādi. Šīs tiesības var ierobežot saskaņā ar 11. pantu vai pielāgot, lai nodrošinātu notiekoša tiesas procesa intereses.

83. Saskaņā ar 11. panta 1. punktu ir atļauti ierobežoti 9. panta piemērošanas izņēmumi.

### 10. pants. Papildu pienākumi

84. Lai nodrošinātu, ka tiesības uz personas datu aizsardzību ir efektīvas, pārzinim un attiecīgā gadījumā apstrādātājam(-iem) tiek noteikti papildu pienākumi.

85. Saskaņā ar *1. punktu* pārziņa pienākums nodrošināt pietiekamu datu aizsardzību ir saistīts ar pienākumu pārbaudīt un spēt pierādīt, ka datu apstrāde atbilst piemērojamajiem tiesību aktiem. Konvencijā noteiktie datu aizsardzības principi, kas jāpiemēro visos apstrādes posmos, ieskaitot izstrādes posmu, ir paredzēti datu subjektu aizsardzībai un vienlaikus veicina to uzticēšanos. Piemēroti pasākumi, kas pārzinim un apstrādātājam var būt jāveic atbilstības nodrošināšanai, ietver darbinieku mācības, piemērotu paziņošanas procedūru izveidi (piemēram, lai norādītu, kad dati jādzēš no sistēmas), apstrādes deleģēšanas gadījumā – konkrētu līguma noteikumu izstrādi, lai īstenotu Konvenciju, kā arī iekšēju procedūru izveidi, lai nodrošinātu verifikāciju un atbilstības pierādīšanu.

86. Ja saskaņā ar 11. panta 3. punktu Puse, atsaucoties uz apstrādes darbībām valsts drošības un aizsardzības nolūkos, izvēlas ierobežot uzraudzības iestādes pilnvaras 15. panta izpratnē, pārzinim nav pienākuma pierādīt šādai uzraudzības iestādei datu aizsardzības prasību izpildi attiecībā uz darbībām, kurām piemēro minēto izņēmumu.

87. Lai atvieglotu šādu pārbaudi un atbilstības pierādīšanu, pārzinis var izraudzīties “datu aizsardzības speciālistu”, kam uztic līdzekļus, kas vajadzīgi viņa pilnvaru īstenošanai. Datu aizsardzības speciālists, par kura iecelšanu ir jāinformē uzraudzības iestāde, var būt vai nu saistīts ar pārzini, vai neatkarīgs.

88. Šā panta *2. punktā* paskaidrots, ka pirms datu apstrādes pārzinim ir jāpārbauda tās iespējamā ietekme uz datu subjekta tiesībām un pamatbrīvībām. Šo pārbaudi var veikt bez pārmērīgām formalitātēm. Turklāt, pamatojoties uz visaptverošu paredzētās apstrādes pārskatu, tajā jānovērtē arī proporcionalitātes principa ievērošana. Dažās situācijās, kad papildus pārzinim ir iesaistīts apstrādātājs, arī apstrādātājam ir jānovērtē riski. Risku novērtēšanā var iesaistīties IT sistēmu izstrādātāji, tostarp drošības speciālisti vai projektētāji, kā arī lietotāji un tiesību eksperti.

89. Šā panta *3. punktā* noteikts, ka, lai labāk nodrošinātu efektīvu aizsardzības līmeni, pārziņiem un attiecīgā gadījumā apstrādātājiem jānodrošina, ka datu aizsardzības prasības datu apstrādes darbībās tiek integrētas pēc iespējams agrāk, proti, ideālā gadījumā – arhitektūras un sistēmas izstrādes posmā, izmantojot tehniskus un organizatoriskus pasākumus (integrēta datu aizsardzība). Datu aizsardzības prasības jāievieš ne tikai attiecībā uz datu apstrādei izmantoto tehnoloģiju, bet arī attiecībā uz saistītajiem darba un pārvaldības procesiem. Jāievieš viegli lietojamas funkcijas, kas veicina atbilstību piemērojamajiem tiesību aktiem. Piemēram, ja iespējams, attiecīgā gadījumā datu subjektiem jāpiedāvā droša tiešsaistes piekļuve to datiem. Jāievieš arī viegli lietojami rīki, kas ļauj datu subjektiem nodot savus datus citam izvēlētam pakalpojuma sniedzējam vai pašiem saglabāt datus (datu pārnesamības rīki). Nosakot noklusējuma iestatījumu tehniskās prasības, pārziņiem un apstrādātājiem jāizvēlas uz privātumu vērstas standarta konfigurācijas, lai lietotņu un programmatūras lietošana nepārkāptu datu subjektu tiesības (datu aizsardzība pēc noklusējuma), jo īpaši, lai nepieļautu, ka tiek apstrādāts vairāk datu nekā nepieciešams leģitīmā nolūka sasniegšanai. Piemēram, sociālie tīkli pēc noklusējuma jākonfigurē tā, lai ieraksti vai attēli tiktu kopīgoti tikai ierobežotā izvēlētu personu lokā, nevis visā internetā.

90. Šā panta *4. punkts* nosaka, ka Pusēm ir atļauts pielāgot 1.–3. punktā minētos papildu pienākumus, ņemot vērā riskus, kas apdraud datu subjektu intereses, tiesības un pamatbrīvības. Šāda pielāgošana jāveic, ņemot vērā apstrādāto datu veidu un apjomu, datu apstrādes veidu, darbības jomu un nolūkus un dažos gadījumos – vienības, kas apstrādā datus, lielumu. Pienākumus var pielāgot, piemēram, tā, lai neradītu pārmērīgi augstas izmaksas maziem un vidējiem uzņēmumiem (MVU), kuri no klientiem saņemtos nesensitīvos personas datus apstrādā tikai komercdarbību ietvaros un neizmanto tos atkārtoti citiem nolūkiem. Noteiktām datu apstrādes kategorijām, piemēram, apstrādei, kas nerada riskus datu subjektiem, var pat nepiemērot dažus no šajā pantā paredzētajiem papildu pienākumiem.

### 11. pants. Izņēmumi un ierobežojumi

91. Nav pieļaujami nekādi izņēmumi attiecībā uz II nodaļas noteikumiem, izņemot ierobežotu skaitu noteikumu (5. panta 4. punkts, 7. panta 2. punkts, 8. panta 1. punkts un 9. pants), ja šādi izņēmumi ir paredzēti tiesību aktos, ja tajos ir ievērota pamattiesību un brīvību būtība un tie ir nepieciešami demokrātiskā sabiedrībā 11. panta 1. punkta *a)* un *b) apakšpunktā* minēto iemeslu dēļ. Pasākumam, kas ir “nepieciešams demokrātiskā sabiedrībā”, ir jāsasniedz leģitīms mērķis, un tādējādi tam ir jānodrošina neatliekama sabiedriska vajadzība, kuru nevar īstenot ar mazāk traucējošiem līdzekļiem. Turklāt šādam pasākumam jābūt samērīgam ar sasniedzamo leģitīmo mērķi, un iemesliem, ar kuriem valsts iestādes to pamato, jābūt atbilstīgiem un pieņemamiem. Šāds pasākums ir jānosaka pieejamā un paredzamā tiesību aktā, kam jābūt pietiekami detalizētam.

92. Personas datu apstrādei vienmēr jābūt likumīgai, godīgai un pārredzamai attiecībā pret datu subjektiem, un dati jāapstrādā tikai konkrētiem nolūkiem. Tas neliedz tiesībaizsardzības iestādēm veikt tādas darbības kā slepena izmeklēšana vai videonovērošana. Šādas darbības var veikt, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus, sauktu pie atbildības par tiem un izpildītu kriminālsodus, tostarp lai nodrošinātu aizsardzību pret draudiem valsts drošībai un sabiedriskajai drošībai un tos novērstu, ja šādas darbības ir paredzētas tiesību aktos un ir nepieciešams un samērīgs pasākums demokrātiskā sabiedrībā, pienācīgi ņemot vērā datu subjektu leģitīmās intereses.

93. Šādu izņēmumu nepieciešamība ir jāpārbauda katrā atsevišķā gadījumā un ņemot vērā svarīgos vispārējo sabiedrības interešu mērķus, kā izklāstīts pirmā punkta *a)* un b) apakšpunktā. Šā punkta *a) apakšpunktā* uzskaitīti daži valsts vai starptautiskas organizācijas vispārējo sabiedrības interešu mērķi, kuru dēļ var būt nepieciešami izņēmumi.

94. Jēdziens “valsts drošība” jāinterpretē, pamatojoties uz attiecīgo Eiropas Cilvēktiesību tiesas judikatūru.[[13]](#footnote-14)

95. Termins “svarīgas ekonomiskās un finansiālās intereses” jo īpaši attiecas uz nodokļu iekasēšanas prasībām un valūtas maiņas kontroli. Termins “noziedzīgu nodarījumu novēršana, izmeklēšana un saukšana pie atbildības par tiem un kriminālsodu izpilde” šajā *a) apakšpunktā* ietver kriminālvajāšanu un ar noziedzīgiem nodarījumiem saistītu sankciju piemērošanu. Termins “citi svarīgi vispārējo sabiedrības interešu mērķi” *inter alia* attiecas uz reglamentēto profesiju ētikas pārkāpumu novēršanu, izmeklēšanu, atklāšanu un saukšanu pie atbildības par tiem, kā arī civilprasību izpildi.

96. Šā punkta *b) apakšpunkts* attiecas uz fizisku personu, piemēram, datu subjekta tiesībām un pamatbrīvībām (piemēram, ja datu subjekta vitālās intereses ir apdraudētas tāpēc, ka viņš ir pazudis bez vēsts) vai trešās personas tiesībām un pamatbrīvībām, piemēram, vārda brīvību, tostarp žurnālistikas, akadēmiskās, mākslinieciskās vai literārās izpausmes brīvību, un tiesībām saņemt un izplatīt informāciju, saziņas un korespondences konfidencialitāti, kā arī komercnoslēpumu vai citiem juridiski aizsargātiem noslēpumiem. Tas jo īpaši jāatiecina uz datu apstrādi audiovizuālajā jomā, ziņu arhīvos un preses bibliotēkās. Lai vārda brīvības īpaši svarīgā loma katrā demokrātiskā sabiedrībā būtu pietiekami ņemta vērā, jēdzieni, kas saistīti ar šo brīvību, piemēram, jēdziens “žurnālistika”, ir jāinterpretē plaši.

97. Šā panta *otrajā punktā* pieļauta iespēja ierobežot 8. un 9. panta noteikumus attiecībā uz konkrētu datu apstrādi, ko veic arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos vai statistikas nolūkos, kuri nerada ievērojamu datu subjektu tiesību un pamatbrīvību pārkāpuma risku. Piemēram, tā varētu attiekties uz datu izmantošanu statistikas datu apstrādei valsts un privātajā jomā, ja šie dati tiek publicēti sagrupētā veidā un ar nosacījumu, ka ir ieviesti atbilstoši datu aizsardzības pasākumi (sk. 50. punktu).

98. Papildu izņēmumi, kas pieļaujami attiecībā uz 4. panta 3. punktu, 14. panta 5. un 6. punktu un 15. panta 2. punkta *a)*, *b)*, *c)* un *d)* apakšpunktu par datu apstrādi valsts drošības un aizsardzības nolūkos, neskar piemērojamās prasības saistībā ar pārskatīšanas un uzraudzības mehānismu neatkarību un efektivitāti.[[14]](#footnote-15)

### 12. pants. Sankcijas un tiesiskās aizsardzības līdzekļi

99. Lai Konvencija garantētu efektīvu datu aizsardzības līmeni, pārziņa un apstrādātāja pienākumi un datu subjektu tiesības jāatspoguļo Pušu tiesību aktos, nosakot attiecīgas sankcijas un tiesiskās aizsardzības līdzekļus.

100. Katra puse var noteikt tiesas un ārpustiesas sankciju veidu (civiltiesiskas, administratīvas, kriminālsankcijas). Sankcijām ir jābūt iedarbīgām, samērīgām un atturošām. Tas pats attiecas uz tiesiskās aizsardzības līdzekļiem – datu subjektiem jābūt iespējai apstrīdēt lēmumu vai praksi tiesā, procesa kārtību nosakot Pusēm. Datu subjektu rīcībā jābūt arī ārpustiesas aizsardzības līdzekļiem. Attiecīgā gadījumā var apsvērt arī iespēju noteikt finansiālu kompensāciju par materiālu vai nemateriālu kaitējumu, kas radies datu apstrādes un kolektīvas rīcības dēļ.

### 13. pants. Paplašinātā aizsardzība

101. Šā panta pamatā ir līdzīgs noteikums – Eiropas Cilvēktiesību konvencijas 53. pants. Konvencijā ir apstiprināti datu aizsardzības tiesību principi, ko visas Puses ir gatavas pieņemt. Tekstā uzsvērts, ka šie principi ir tikai pamats, uz kura Puses var veidot progresīvāku aizsardzības sistēmu. Tādēļ jēdziens “plašāks aizsardzības pasākums” attiecas uz aizsardzības standartu, kas ir augstāks, nevis zemāks par Konvencijā noteikto.

### III nodaļa. Personas datu pārrobežu plūsmas[[15]](#footnote-16)

**14. pants. Personas datu pārrobežu plūsmas**

102. Šā panta mērķis ir veicināt brīvu informācijas apriti neatkarīgi no robežām (kā norādīts preambulā), vienlaikus nodrošinot personu atbilstošu aizsardzību attiecībā uz personas datu apstrādi. Pārrobežu datu nosūtīšana notiek, kad personas dati tiek izpausti vai darīti pieejami saņēmējam, kurš ir citas valsts vai starptautiskas organizācijas jurisdikcijas subjekts.

103. Pārrobežu datu plūsmas režīma mērķis ir nodrošināt, ka personas datus, kas sākotnēji apstrādāti Puses jurisdikcijā (piemēram, dati tur ir iegūti vai glabāti) un kas pēc tam nonāk tādas valsts jurisdikcijā, kura nav Konvencijas puse, apstrādā, ievērojot atbilstošus aizsardzības pasākumus. Ir svarīgi, lai datus, ko apstrādā Puses jurisdikcijā, vienmēr aizsargātu attiecīgie Konvencijas datu aizsardzības principi. Lai gan aizsardzības sistēmas var būt ļoti dažādas, paredzētajai aizsardzībai jābūt tādas kvalitātes, lai nodrošinātu, ka globalizācija un pārrobežu datu plūsmas neietekmē cilvēktiesības.

104. Konvencijas 14. pants attiecas tikai uz izejošajiem datiem, nevis ienākošajiem datiem, uz kuriem attiecas saņēmējas Puses datu aizsardzības režīms.

105. Šā panta *1. punktu* piemēro datu plūsmām starp Konvencijas pusēm. Datu plūsmas nevar aizliegt vai pakļaut īpašai atļaujai “tikai tāpēc, lai aizsargātu personas datus”. Tomēr Konvencija neierobežo Puses brīvību ierobežot personas datu nosūtīšanu citai Pusei citu iemeslu dēļ, tostarp, piemēram, valsts drošības, aizsardzības, sabiedrības drošības vai citu svarīgu sabiedrības interešu dēļ (tostarp valsts noslēpuma aizsardzībai).

106. Šā panta *1. punkta* noteikuma pamatojums ir tāds, ka no visām Pusēm, kas parakstījušās par Konvencijā izklāstītajiem kopējiem datu aizsardzības pamatnoteikumiem, sagaida, ka tās nodrošinās tādu aizsardzības līmeni, kas uzskatāms par atbilstošu un kas tādējādi principā atļauj brīvu datu apriti. Tomēr ir iespējami izņēmumi, kad pastāv reāls un nopietns risks, ka šāda brīva personas datu aprite var novest pie Konvencijas noteikumu apiešanas. Izņēmuma kārtā šis noteikums ir jāinterpretē ierobežojoši, un Puses nevar uz to atsaukties gadījumos, kad risks ir hipotētisks vai neliels. Tāpēc Puse var piemērot izņēmumu konkrētā gadījumā tikai tad, ja tai ir skaidri un ticami pierādījumi, ka datu nosūtīšana citai Pusei var ievērojami apdraudēt aizsardzību, kas šiem datiem piešķirta saskaņā ar Konvenciju, un ka šāda notikuma iespējamība ir ļoti augsta. Tas var notikt, piemēram, gadījumos, kad otra Puse vairs negarantē noteiktu aizsardzības līmeni, kas paredzēts Konvencijā (piemēram, tāpēc, ka tās uzraudzības iestāde vairs nespēj efektīvi pildīt savas funkcijas), vai kad citai Pusei nosūtītie dati, iespējams, tiks pārsūtīti tālāk (tālāka nosūtīšana), nenodrošinot pienācīgu aizsardzības līmeni. Vēl vienu starptautiskajās tiesībās atzītu izņēmumu piemēro gadījumos, kad Pusēm ir saistoši saskaņoti aizsardzības noteikumi, kas ir kopīgi valstīm, kuras pieder pie reģionālām (ekonomiskām) organizācijām, kas cenšas panākt dziļāku integrācijas līmeni.

107. Cita starpā tas attiecas uz ES dalībvalstīm. Tomēr, kā skaidri noteikts Vispārīgajā datu aizsardzības regulā (ES) 2016/679, trešās valsts pievienošanās Konvencijai Nr. 108 un tās īstenošana ir svarīgs faktors, piemērojot ES starptautisko datu nosūtīšanas režīmu, jo īpaši novērtējot, vai trešā valsts nodrošina pietiekamu aizsardzības līmeni (kas savukārt ļauj nodrošināt personas datu brīvu apriti).

108. Šā panta *2. punktā* paredzēts pienākums principā nodrošināt, ka “tiek garantēts atbilstošs aizsardzības līmenis, kas balstīts uz šīs konvencijas noteikumiem”. Vienlaikus 4. punktā ir noteikts, ka Puses var nosūtīt datus pat tad, ja nav nodrošināts pienācīgs aizsardzības līmenis, ja nosūtīšanu cita starpā pamato “prevalējošas leģitīmās intereses, jo īpaši svarīgas sabiedrības intereses”, tādā apmērā, kādā tas paredzēts tiesību aktos, un ja šāda nosūtīšana ir vajadzīgs un samērīgs pasākums demokrātiskā sabiedrībā (*c) apakšpunkts*). Tādējādi personas datus var nosūtīt tādu iemeslu dēļ, kas ir līdzīgi 11. panta 1. un 3. punktā minētajiem. Visos gadījumos Puses drīkst saskaņā ar Konvenciju brīvi ierobežot datu nosūtīšanu trešajām pusēm vai nu datu aizsardzības nolūkā, vai citu iemeslu dēļ.

109. Šā panta *2. punkts* attiecas uz personas datu pārrobežu plūsmām saņēmējam, kas nav Puses jurisdikcijas subjekts. Attiecībā uz visiem personas datiem, ko nosūta ārpus valsts robežām, ir jānodrošina atbilstošs aizsardzības līmenis. Ja saņēmējs nav Konvencijas puse, Konvencijā ir paredzēti divi mehānismi, lai nodrošinātu, ka datu aizsardzības līmenis patiešām ir atbilstošs – vai nu ar tiesību aktiem, vai ar *ad hoc* vai apstiprinātiem standarta aizsardzības pasākumiem, kas ir juridiski saistoši un izpildāmi, kā arī tiek pienācīgi īstenoti.

110. Šā panta *2. un 3. punkts* attiecas uz visiem atbilstošas aizsardzības veidiem, ko nodrošina vai nu ar tiesību aktiem, vai ar standarta aizsardzības pasākumiem. Tiesību aktos jāiekļauj attiecīgie datu aizsardzības elementi, kā noteikts šajā konvencijā. Aizsardzības līmenis jānovērtē attiecībā uz katru datu nosūtīšanu vai nosūtīšanas kategoriju. Jānovērtē dažādi nosūtīšanas elementi, piemēram, datu veids, apstrādes, kuras ietvaros dati tiek nosūtīti, nolūks un ilgums, tiesiskuma ievērošana galamērķa valstī, vispārējās un nozaru tiesību normas, kā arī profesionālie un drošības noteikumi, kas piemērojami attiecīgajā valstī vai organizācijā.

111. *Ad hoc* vai standarta aizsardzības pasākumu saturā jāiekļauj attiecīgie datu aizsardzības elementi. Turklāt līguma noteikumi var ietvert nosacījumu, piemēram, ka datu subjektam par datu nosūtīšanu atbildīgās personas darbinieku vidū tiek nodrošināta kontaktpersona, kuras pienākums ir nodrošināt atbilstību būtiskajiem aizsardzības standartiem. Datu subjekts jebkurā laikā bez maksas var sazināties ar šo personu par datu apstrādi vai nosūtīšanu un attiecīgā gadījumā saņemt palīdzību saistībā ar tiesību īstenošanu.

112. Novērtējot, vai aizsardzības līmenis ir atbilstošs, jāņem vērā Konvencijas principi, tas, cik lielā mērā tie tiek ievēroti saņēmējā valstī vai organizācijā – ciktāl tie attiecas uz konkrēto datu nosūtīšanas gadījumu – un kā datu subjekts var aizstāvēt savas intereses neatbilstības gadījumā. Novērtējumā jāņem vērā datu subjektu tiesību īstenojamība un efektīva aizsardzības nodrošināšana administratīvā kārtā vai tiesā tiem datu subjektiem, kuru personas datus nosūta. Tāpat novērtējumu var veikt attiecībā uz visu valsti vai organizāciju, tādējādi atļaujot visa veida datu nosūtīšanu uz šādu galamērķi.

113. Šā panta *4. punkts* nosaka, ka Pusēm ir atļauts atkāpties no principa par atbilstošu aizsardzības līmeni un nosūtīt datus saņēmējam, kas šādu aizsardzību nenodrošina. Šādas atkāpes ir atļautas tikai dažās situācijās: ar datu subjekta piekrišanu vai konkrētās datu subjekta interesēs un/vai tad, ja tiesību aktos ir paredzētas prevalējošas leģitīmas intereses un/vai datu nosūtīšana ir nepieciešams un samērīgs pasākums demokrātiskā sabiedrībā, lai nodrošinātu vārda brīvību. Piemērojot šādas atkāpes, jāievēro nepieciešamības un proporcionalitātes princips.

114. Šā panta *5. punktā* ir noteikts papildu aizsardzības pasākums, proti, ka kompetentajai uzraudzības iestādei tiek sniegta visa attiecīgā informācija par 3. punkta b) apakšpunktā minēto datu pārsūtīšanu un pēc pieprasījuma par 4. panta b) un c) apakšpunktā minēto datu pārsūtīšanu. Iestādei ir jābūt tiesībām pieprasīt attiecīgo informāciju par šādas nosūtīšanas apstākļiem un pamatojumu. Saskaņā ar 11. panta 3. punktu, ir atļauts piemērot izņēmumus attiecībā uz 14. panta 5. punktu.

115. Kā noteikts *6. punktā*, uzraudzības iestādei jābūt tiesībām pieprasīt pierādījumus par veikto pasākumu efektivitāti vai par prevalējošām leģitīmām interesēm un aizliegt, apturēt datu nosūtīšanu vai izvirzīt nosacījumus attiecībā uz to, ja tas ir nepieciešams, lai aizsargātu datu subjektu tiesības un pamatbrīvības. Saskaņā ar 11. panta 3. punktu ir atļauts piemērot izņēmumus attiecībā uz 14. panta 6. punktu.

116. Datu plūsmas nepārtraukti pieaug un līdz ar to ir jāpaaugstina personas datu aizsardzība, radot nepieciešamību palielināt arī kompetento uzraudzības iestāžu starptautisko sadarbību izpildes jomā.

### IV nodaļa. Uzraudzības iestādes[[16]](#footnote-17)

### 15. pants. Uzraudzības iestādes

117. Šā panta mērķis ir nodrošināt personu efektīvu aizsardzību, nosakot, ka Pusēm ir jānodrošina viena vai vairākas neatkarīgas un objektīvas valsts uzraudzības iestādes, kas veicina personu tiesību un brīvību aizsardzību saistībā ar personas datu apstrādi. Šāda iestāde var būt komisārs vai kolēģija. Lai datu aizsardzības uzraudzības iestādes varētu nodrošināt atbilstošu tiesiskās aizsardzības līdzekli, tām nepieciešamas efektīvas pilnvaras un funkcijas, kā arī tām jābūt patiesi neatkarīgām, pildot tām uzticētos pienākumus. Tās ir svarīgs datu aizsardzības uzraudzības sistēmas elements demokrātiskā sabiedrībā.Ciktāl piemērojams 11. panta 3. punkts, Puses var nodrošināt citus atbilstošus mehānismus neatkarīgai un efektīvai apstrādes darbību pārskatīšanai un uzraudzībai valsts drošības un aizsardzības nolūkos.

118. Šā panta *1. punktā* ir paskaidrots, ka, ņemot vērā dažādu tiesību sistēmu (piemēram, federālo valstu) konkrētos apstākļus, var būt nepieciešamas vairākas iestādes. Var izveidot arī īpašas uzraudzības iestādes, kas darbojas noteiktā nozarē (elektronisko sakaru nozarē, veselības nozarē, publiskajā sektorā utt.). Tas attiecas arī uz personas datu apstrādi žurnālistikas vajadzībām, ja tiesības uz personas datu aizsardzību ir jāsaskaņo ar tiesībām uz vārda brīvību. Lai ātri un efektīvi rīkotos, uzraudzības iestāžu rīcībā jābūt nepieciešamajai infrastruktūrai un finanšu, tehniskajiem resursiem un cilvēkresursiem (juristiem, IT speciālistiem). Resursu piemērotība ir pastāvīgi jāpārskata. Konvencijas 11. panta 3. punktā attiecībā uz uzraudzības iestāžu pilnvarām ir pieļauti izņēmumi saistībā ar apstrādes darbībām valsts drošības un aizsardzības nolūkos (nosakot šādus izņēmumus, var nebūt piemērojami vai nebūt atbilstīgi citi šā panta punkti). Tomēr tas neskar piemērojamās prasības attiecībā uz pārskatīšanas un uzraudzības mehānismu objektivitāti un efektivitāti.[[17]](#footnote-18)

119. Pusēm ir noteikta rīcības brīvība attiecībā uz to, kā izveidot iestādes, lai tās varētu veikt tām uzticēto uzdevumu. Tomēr *2. punktā* ir noteikts, ka, ņemot vērā iespēju piemērot izņēmumus saskaņā ar 11. panta 3. punktu, tām ir jābūt pilnvarotām veikt izmeklēšanu, iejaukties un izdot lēmumus par šīs konvencijas noteikumu pārkāpumiem. Šādos gadījumos var tikt piemērotas administratīvas sankcijas, tostarp naudas sodi. Ja Puses tiesību sistēma neparedz administratīvās sankcijas, 2. punktu var piemērot tā, ka sankcijas ierosina kompetentā uzraudzības iestāde un tās piemēro kompetentā valsts tiesa. Jebkurā gadījumā visām piemērotajām sankcijām ir jābūt efektīvām, samērīgām un atturošām.

120. Iestādei jābūt pilnvarotai veikt izmeklēšanu ar nosacījumu, ka ir iespējams piemērot izņēmumus saskaņā ar 11. panta 3. punktu, piemēram, iespēju lūgt pārzinim un apstrādātājam informāciju par personas datu apstrādi un iegūt to. Kā noteikts 15. pantā, šāda informācija jāsniedz jo īpaši tad, ja uzraudzības iestādē vēršas datu subjekts, kas vēlas īstenot 9. pantā paredzētās tiesības. Attiecībā uz šīm tiesībām piemēro 11. panta 1. punktā minētos izņēmumus.

121. Pilnvaras iejaukties, kas piešķirtas uzraudzības iestādei un kas paredzētas 1. punktā, Pušu tiesību aktos var būt noteiktas dažādos veidos. Piemēram, iestāde var būt pilnvarota noteikt pārzinim pienākumu labot, dzēst vai iznīcināt nepareizi vai nelikumīgi apstrādātus datus uz pārziņa rēķina vai gadījumos, kad datu subjekts nespēj īstenot šīs tiesības. Īpaši efektīva iejaukšanās pilnvaru izpausme ir arī pilnvaras vērsties pret pārziņiem, kuri nevēlas sniegt prasīto informāciju piemērotā termiņā. Šīs pilnvaras var ietvert arī iespēju izdot atzinumus pirms datu apstrādes darbību veikšanas (ja apstrāde īpaši apdraud tiesības un pamatbrīvības, pārziņiem ar uzraudzības iestādi jākonsultējas jau, sākot ar procesu izstrādes sākotnējo posmu) vai attiecīgā gadījumā nodot lietas attiecīgajām kompetentajām iestādēm.

122. Turklāt saskaņā ar *4. punktu* katram datu subjektam jābūt iespējai pieprasīt, lai uzraudzības iestāde izmeklē prasību attiecībā uz viņa tiesībām un brīvībām saistībā ar personas datu apstrādi. Tas palīdz atbilstīgi 9. un 12. pantam garantēt tiesības uz atbilstošu tiesiskās aizsardzības līdzekli. Jānodrošina šā pienākuma izpildei nepieciešamie resursi. Ņemot vērā pieejamos resursus, uzraudzības iestādēm jādod iespēja noteikt prioritātes datu subjektu iesniegto pieprasījumu un sūdzību izskatīšanai.

123. Pusēm jāpiešķir uzraudzības iestādei pilnvaras vai nu iesaistīties tiesvedībā, vai vērsties tiesu iestādēs saistībā ar jebkādiem datu aizsardzības noteikumu pārkāpumiem ar nosacījumu, ka ir iespējams piemērot izņēmumus saskaņā ar 11. panta 3. punktu. Minētās pilnvaras izriet no pilnvarām veikt izmeklēšanu, kurā iestāde var atklāt, ka ir pārkāptas personas tiesības uz aizsardzību. Puses var izpildīt pienākumu piešķirt šīs pilnvaras iestādei, ļaujot tai pieņemt lēmumus.

124. Ja administratīvam lēmumam ir tiesiskas sekas, katrai skartajai personai ir tiesības uz efektīvu tiesiskās aizsardzības līdzekli saskaņā ar piemērojamajiem valsts tiesību aktiem.

125. Šā panta *2. punkta e) apakšpunktā* aplūkota uzraudzības iestāžu izpratnes veidošanas loma. Šajā kontekstā šķiet īpaši svarīgi, lai uzraudzības iestāde proaktīvi nodrošinātu savu darbību, uzdevumu un pilnvaru redzamību. Tādēļ uzraudzības iestādei ir jāinformē sabiedrība, sniedzot periodiskus ziņojumus (sk. 131. punktu). Tā var arī publicēt atzinumus, sniegt vispārīgus ieteikumus par datu aizsardzības noteikumu pareizu piemērošanu vai izmantot citus saziņas līdzekļus. Turklāt tai jāinformē personas, datu pārziņi un apstrādātāji par viņu tiesībām un pienākumiem saistībā ar datu aizsardzību. Veidojot izpratni par datu aizsardzības jautājumiem, iestādēm īpaša uzmanība jāpievērš bērniem un neaizsargātām fiziskām personām, izmantojot pielāgotas metodes un valodu.

126. Kā noteikts *3. punktā*, uzraudzības iestādēm saskaņā ar piemērojamajiem valsts tiesību aktiem ir tiesības izdot atzinumus par visiem likumdošanas vai administratīvajiem pasākumiem, kuros paredzēta personas datu apstrāde. Minētās konsultatīvās pilnvaras attiecas tikai uz vispārīgiem, nevis atsevišķiem pasākumiem.

127. Papildus 3. punktā paredzētajām konsultācijām iestādei var lūgt sniegt atzinumu arī tad, ja tiek gatavoti citi pasākumi attiecībā uz personas datu apstrādi, piemēram, rīcības kodeksi vai tehniskie noteikumi.

128. Konvencijas 15. pants neliedz piešķirt uzraudzības iestādēm citas pilnvaras.

129. Šā panta *5. punktā* paskaidrots, ka uzraudzības iestādes var efektīvi nodrošināt personas tiesības un brīvības tikai tad, ja tās pilda savas funkcijas pilnīgi neatkarīgi. Uzraudzības iestādes neatkarību, pildot tās funkcijas, palīdz nodrošināt vairāki elementi, tostarp iestādes sastāvs, tās locekļu iecelšanas metode, tās funkciju īstenošanas ilgums un to izbeigšanas nosacījumi, iespēja bez pārmērīgiem ierobežojumiem piedalīties attiecīgās sanāksmēs, iespēja konsultēties ar tehniskiem vai citiem ekspertiem vai rīkot neatkarīgas konsultācijas, pietiekamu resursu pieejamība, iespēja nolīgt darbiniekus vai pieņemt lēmumus bez tiešas vai netiešas ārējas ietekmes.

130. Aizliegums lūgt vai pieņemt norādījumus attiecas uz uzraudzības iestādes pienākumu izpildi. Tas neliedz uzraudzības iestādēm vajadzības gadījumā lūgt speciālistu ieteikumus, ja vien uzraudzības iestādes pašas pieņem neatkarīgu spriedumu.

131. Šā panta *7. punktā* ir noteikts, ka uzraudzības iestāžu darba un darbību pārredzamību nodrošina, piemēram, publicējot gada darbības pārskatus, kur *inter alia* iekļauj informāciju par iestādes izpildes darbībām.

132. Neskarot šo neatkarību, jābūt iespējai pārsūdzēt uzraudzības iestāžu lēmumus tiesā saskaņā ar tiesiskuma principu, kā noteikts *9. punktā*.

133. Turklāt, lai gan uzraudzības iestādēm jābūt tiesībspējīgām rīkoties tiesā un pieprasīt izpildi, uzraudzības iestādes iejaukšanās (vai neiejaukšanās) nedrīkst liegt skartajai personai izmantot tiesiskās aizsardzības līdzekļus (sk. 124. punktu).

134. Konvencijas 15. panta *10. punktā* noteikts, ka uzraudzības iestāžu kompetencē neietilpst apstrāde, ko veic neatkarīgas iestādes, kas pilda tiesas funkciju. Šāds atbrīvojums no uzraudzības pilnvarām ir stingri jāattiecina tikai uz reālām tiesas darbībām saskaņā ar valsts tiesību aktiem.

### V nodaļa. Sadarbība un savstarpēja palīdzība

**16. pants. Uzraudzības iestāžu izraudzīšana**

135. Konvencijas V nodaļa (16.–21. pants) ietver noteikumu kopumu par Pušu sadarbību un savstarpējo palīdzību ar dažādu iestāžu starpniecību, lai īstenotu datu aizsardzības tiesību aktus, kas ieviesti saskaņā ar Konvenciju. Šie noteikumi ir obligāti, izņemot 20. pantā minētos gadījumus. Saskaņā ar 16. pantu Puses izraugās vienu vai vairākas iestādes un paziņo Eiropas Padomes ģenerālsekretāram to kontaktinformāciju, kā arī attiecīgā gadījumā to būtiskās un teritoriālās kompetences. Turpmākajos pantos ir izklāstīta detalizēta sadarbības un savstarpējās palīdzības sistēma.

136. Lai gan Pušu sadarbību galvenokārt īsteno uzraudzības iestādes, kas izveidotas saskaņā ar 15. pantu, Puse 16. panta noteikumu izpildei var izraudzīties citu iestādi.

137. Sadarbība un vispārīgā palīdzība attiecas gan uz kontroles pasākumiem *a priori*, gan uz kontroles pasākumiem *a posteriori* (piemēram, lai pārbaudītu konkrēta datu pārziņa darbības). Informācija, ar kuru apmainās, var būt juridiska vai faktiska.

### 17. pants. Sadarbības veidi

138. Saskaņā ar 17. pantu uzraudzības iestādes 15. panta izpratnē savstarpēji sadarbojas, ciktāl tas ir nepieciešams, lai izpildītu pienākumus un īstenotu pilnvaras. Tā kā 17. pantā ir noteikts, ka uzraudzības iestāžu sadarbība notiek “ciktāl tas ir nepieciešams, lai izpildītu pienākumus un īstenotu pilnvaras”, un tā kā uzraudzības iestāžu spēja sadarboties ir atkarīga no to pilnvarām, šo noteikumu nepiemēro tādā apmērā, kādā Puse izmanto 11. panta 3. punktu, kas ietver uzraudzības iestāžu pilnvaru ierobežošanu saskaņā ar 15. panta 2. punkta *a)*–*d) apakšpunktu*.

139. Var būt vairāki sadarbības veidi – gan “stingri”, piemēram, datu aizsardzības tiesību aktu īstenošana, izmantojot savstarpēju palīdzību, kurā katras uzraudzības iestādes rīcības likumība ir neapstrīdama, gan “maigi”, piemēram, izpratnes veidošana, mācības un darbinieku apmaiņa.

140. Iespējamo sadarbības veidu saraksts nav stingri noteikts. Pirmkārt, uzraudzības iestādes sniedz viena otrai savstarpēju palīdzību, jo īpaši apmainoties ar jebkādu būtisku un noderīgu informāciju. Šī informācija var būt divējāda: “informācija un dokumentācija par to normatīvo un administratīvo praksi saistībā ar datu aizsardzību” (kas parasti nerada nekādas problēmas; ar šādu informāciju var brīvi apmainīties un publiskot to), kā arī konfidenciāla informācija, tostarp personas dati.

141. Ar personas datiem var apmainīties tikai tad, ja tiem ir būtiska nozīme sadarbībā, proti, ja, nesniedzot šādus datus, sadarbība nebūtu efektīva vai ja “attiecīgais datu subjekts ir devis skaidru, konkrētu, brīvu un apzinātu piekrišanu”. Jebkurā gadījumā personas dati jānosūta, ievērojot Konvencijas noteikumus, jo īpaši II nodaļu (sk. arī 20. pantu, kur paredzēti atteikuma iemesli).

142. Papildus būtiskas un noderīgas informācijas sniegšanai sadarbības mērķus var sasniegt, koordinējot izmeklēšanas vai iejaukšanās, kā arī veicot kopīgas darbības. Attiecībā uz piemērojamajām procedūrām uzraudzības iestādes atsaucas uz piemērojamajiem valsts tiesību aktiem, piemēram, administratīvā procesa, civilprocesa vai kriminālprocesa kodeksiem vai starpvalstu vai starptautiskām saistībām, kas ir juridiski saistošas to jurisdikcijām, piemēram, savstarpējās tiesiskās palīdzības līgumiem, izvērtējot savu tiesībspēju iesaistīties šāda veida sadarbībā.

143. Šā panta *3. punktā* minēts uzraudzības iestāžu tīkls kā līdzeklis, lai veicinātu sadarbības procesa racionalizāciju un tādējādi uzlabotu personas datu aizsardzības efektivitāti. Ir svarīgi norādīt, ka Konvencijā “tīkls” minēts vienskaitlī. Tas neliedz Pušu izveidotajām uzraudzības iestādēm piedalīties citos attiecīgos tīklos.

### 18. pants. Palīdzība datu subjektiem

144. Šā panta *1. punktā* noteikts, ka datu subjekti neatkarīgi no dzīvesvietas vai pilsonības var izmantot 9. pantā noteiktās tiesības vai nu Konvencijas puses, vai trešās valsts teritorijā.

145. Kā noteikts *2. punktā*, ja datu subjekts dzīvo citas Puses teritorijā, tas var izmantot tiesības vai nu tieši valstī, kurā informācija attiecībā uz datu subjektu tiek apstrādāta, vai netieši ar izraudzītās iestādes starpniecību.

146. Turklāt datu subjekti, kas dzīvo ārvalstīs, tiesības var izmantot ar savas valsts diplomātiskā vai konsulārā dienesta pārstāvju palīdzību.

147. Šā panta *3. punktā* noteikts, ka palīdzības pieprasījumiem jābūt, cik vien iespējams, precīziem, lai paātrinātu procedūru.

### 19. pants. Aizsardzības pasākumi

148. Šajā pantā noteikts, ka uzraudzības iestādēm ir juridiski saistošs pienākums ievērot diskrētumu un konfidencialitāti arī attiecībā uz citu Pušu datu aizsardzības iestādēm un datu subjektiem, kas dzīvo ārvalstīs.

149. Uzraudzības iestāde var sniegt palīdzību datu subjekta vārdā tikai pēc attiecīgā datu subjekta pieprasījuma. Iestādei ir jāsaņem pilnvarojums no datu subjekta, un tā nedrīkst rīkoties autonomi viņa vārdā. Šim noteikumam ir būtiska nozīme savstarpējās uzticēšanās nodrošināšanā, kas ir savstarpējās palīdzības pamatā.

### 20. pants. Pieprasījumu izpildes atteikums

150. Šajā pantā noteikts, ka Pusēm ir jāizpilda sadarbības un savstarpējās palīdzības pieprasījumi. Atteikuma iemesli, kas jāievēro, ir izsmeļoši uzskaitīti.

151. Termins “atbilstība”, kas lietots *c) apakšpunktā*, jāsaprot plašākā nozīmē, proti, ka tas ietver ne tikai pieprasījuma izpildi, bet arī rīcību līdz tā saņemšanai. Piemēram, pieprasījuma saņēmēja iestāde var atteikties rīkoties gan tad, ja pieprasītās informācijas nosūtīšana pieprasījuma iesniedzējai iestādei var kaitēt personas tiesībām un pamatbrīvībām, gan arī tad, ja pats informācijas pieprasīšanas fakts var ietekmēt personas tiesības un pamatbrīvības. Turklāt saskaņā ar piemērojamajiem valsts tiesību aktiem pieprasījuma saņēmējai iestādei var būt pienākums nodrošināt citu sabiedriskās kārtības interešu aizsardzību (piemēram, nodrošināt policijas izmeklēšanas konfidencialitāti). Tādēļ uzraudzības iestādei var būt pienākums atbildē uz pieprasījumu neiekļaut noteiktu informāciju vai dokumentus.

### 21. pants. Izmaksas un procedūras

152. Šā panta noteikumi ir līdzīgi citu starptautisku instrumentu noteikumiem.

153. Lai Konvenciju nepārslogotu ar daudziem īstenošanas elementiem, šā panta *3. punktā* ir noteikts, ka attiecīgās Puses var vienoties par izmantojamo procedūru, veidiem un valodu. Šā punkta tekstā nav noteiktas formālas procedūras, taču ir atļautas administratīvas vienošanās, ko var pat attiecināt uz konkrētiem gadījumiem. Turklāt ir ieteicams Puses kompetentajām uzraudzības iestādēm uzticēt pilnvaras noslēgt šādas vienošanās. Katrā atsevišķā gadījumā sadarbības un palīdzības veidi var būt atšķirīgi. Ir skaidrs, ka, nosūtot pieprasījumu par piekļuvi sensitīvai medicīniskai informācijai, tiks noteiktas prasības, kas atšķirsies no tām, ko piemēro attiecībā uz parastiem pieprasījumiem par ierakstiem iedzīvotāju reģistrā.

### VI nodaļa. Konvencijas komiteja

154. Konvencijas 22., 23. un 24. panta nolūks ir veicināt Konvencijas efektīvu piemērošanu un vajadzības gadījumā to pilnveidot. Konvencijas komiteja ir vēl viens līdzeklis Pušu sadarbībai, lai īstenotu saskaņā ar Konvenciju ieviestos datu aizsardzības tiesību aktus.

155. Konvencijas komitejas sastāvā ir visu Pušu pārstāvji no valsts uzraudzības iestādēm vai no valdības.

156. Konvencijas komitejas būtība un iespējamā izmantotā procedūra var būt līdzīga tām, kas izveidotas saskaņā ar citu Eiropas Padomē noslēgto konvenciju noteikumiem.

157. Tā kā Konvencijā aplūkotais temats pastāvīgi attīstās, var sagaidīt, ka radīsies jautājumi gan par Konvencijas praktisko piemērošanu (23. panta *a) apakšpunkts*), gan par tās nozīmi (tas pats pants, *d) apakšpunkts*).

158. Konvencijas komitejas reglamentā ir ietverti noteikumi par Pušu balsstiesībām un šo tiesību īstenošanas kārtību, un tie ir ietverti Grozījumu protokola papildinājumā.

159. Jebkurus reglamenta grozījumus pieņem ar divu trešdaļu balsu vairākumu, izņemot grozījumus noteikumos par balsstiesībām un attiecīgo kārtību, kam piemēro Konvencijas 25. pantu.

160. ES pēc pievienošanās sniedz paziņojumu, precizējot kompetenču sadalījumu starp ES un tās dalībvalstīm attiecībā uz personas datu aizsardzību saskaņā ar Konvenciju. Pēc tam ES informē ģenerālsekretāru par jebkādām būtiskām kompetenču sadalījuma izmaiņām.

161. Saskaņā ar 25. pantu Konvencijas komitejai ir tiesības ierosināt Konvencijas grozījumus un izvērtēt citus grozījumu priekšlikumus, ko formulējusi kāda Puse vai Ministru komiteja (23. panta *b) un c) apakšpunkts*).

162. Lai garantētu Konvencijā noteikto datu aizsardzības principu īstenošanu, Konvencijas komitejas galvenais uzdevums ir novērtēt atbilstību Konvencijai, vai nu sagatavojot pievienošanās kandidātvalsts nodrošinātā datu aizsardzības līmeņa novērtējumu (23. panta *e) apakšpunkts*), vai regulāri izvērtējot, kā Puses īsteno Konvenciju (23. panta *h) apakšpunkts*). Konvencijas komiteja ir arī pilnvarota novērtēt valsts vai starptautiskas organizācijas datu aizsardzības sistēmas atbilstību Konvencijai, ja valsts vai starptautiska organizācija to pieprasa (23. panta *f) apakšpunkts*).

163. Sniedzot šādus atzinumus par atbilstību Konvencijai, Konvencijas komiteja piemēro godīgu, pārredzamu un publisku procedūru, kas detalizēti izklāstīta tās reglamentā.

164. Turklāt Konvencijas komiteja var apstiprināt standarta datu nosūtīšanas aizsardzības pasākumu paraugus (23. panta *g) apakšpunkts*).

165. Visbeidzot, Konvencijas komiteja var risināt starp Pusēm radušās grūtības (23. panta *i) apakšpunkts*). Strīdu gadījumos Konvencijas komiteja centīsies tos atrisināt sarunu ceļā vai citiem izlīguma līdzekļiem.

### VII nodaļa. Grozījumi

### 25. pants. Grozījumi

166. Ministru komiteja, kas pieņēmusi šīs konvencijas sākotnējo tekstu, ir tiesīga apstiprināt arī jebkādus tā grozījumus.

167. Saskaņā ar *1. punktu* grozījumus var ierosināt Ministru komiteja, Konvencijas komiteja vai Puse (neatkarīgi no tā, vai tā ir vai nav Eiropas Padomes dalībvalsts).

168. Visi grozījumu priekšlikumi, kurus nav ierosinājusi Konvencijas komiteja, saskaņā ar *3. punktu* ir jāiesniedz tai atzinuma sniegšanai.

169. Principā jebkurš grozījums stājas spēkā trīsdesmitajā dienā pēc tam, kad visas Puses ir informējušas Eiropas Padomes ģenerālsekretāru par tā pieņemšanu. Tomēr noteiktos apstākļos Ministru komiteja pēc apspriešanās ar Konvencijas komiteju var vienprātīgi nolemt, ka šādi grozījumi stājas spēkā, beidzoties trīs gadu periodam, ja vien kāda Puse nepaziņo ģenerālsekretāram par iebildumiem. Šī procedūra, kuras mērķis ir paātrināt grozījumu stāšanos spēkā, vienlaikus saglabājot visu Pušu piekrišanas principu, ir paredzēta nelielu un tehnisku grozījumu piemērošanai.

### VIII nodaļa. Nobeiguma noteikumi

### 26. pants. Stāšanās spēkā

170. Tā kā Konvencijas efektīvai īstenošanai ir svarīga plaša ģeogrāfiskā darbības joma, *2. punktā* ir noteikts, ka, lai Konvencija stātos spēkā, tā ir jāratificē piecām Eiropas Padomes dalībvalstīm.

171. Konvencija ir atvērta parakstīšanai Eiropas Savienībā.[[18]](#footnote-19)

### 27. pants. Valstu, kas nav dalībvalstis, un starptautisku organizāciju pievienošanās

172. Konvencijai, kas sākotnēji tika izstrādāta ciešā sadarbībā ar ESAO un vairākām valstīm ārpus Eiropas, var pievienoties jebkura no pasaules valstīm, kura ievēro tās noteikumus. Konvencijas komitejai ir uzticēts uzdevums novērtēt šādu atbilstību un sagatavot atzinumu Ministru komitejai par pievienošanās kandidātvalsts datu aizsardzības līmeni.

173. Ņemot vērā datu plūsmu pārrobežu specifiku, ir vēlama visu pasaules valstu un starptautisko organizāciju pievienošanās. Konvencijai var pievienoties tikai starptautiskās organizācijas, kuras definētas kā organizācijas, ko pārvalda saskaņā ar starptautiskajām publiskajām tiesībām.

### 28. pants. Teritoriālā piemērošana

174. Konvencijas piemērošanai attālām teritorijām, kuras ir Pušu jurisdikcijā vai kuru vārdā Puses var uzņemties saistības, ir praktiska nozīme, ņemot vērā to, ka attālas valstis datu apstrādes darbībām tiek izmantotas izmaksu un darbaspēka dēļ, vai arī lai izmantotu datu apstrādes iespējas pārmaiņus nakts un dienas laikā.

### 29. pants. Atrunas

175. Šīs konvencijas noteikumi ir svarīgākie un būtiskākie efektīvas datu aizsardzības elementi. Tādēļ Konvencijā nav atļautas atrunas attiecībā uz tās noteikumiem, kas turklāt ir pietiekami elastīgi, ņemot vērā dažos pantos pieļautos izņēmumus un ierobežojumus.

### 30. pants. Denonsēšana

176. Jebkura Puse var jebkurā laikā denonsēt šo konvenciju.

### 31. pants. Paziņojumi

177. Šie noteikumi atbilst parastajiem noslēguma noteikumiem, kas iekļauti citās Eiropas Padomes konvencijās.

1. Vispārīgā datu aizsardzības regula (ES) 2016/679 (VDAR) un Direktīva (ES) 2016/680 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes (Policijas direktīva). [↑](#footnote-ref-2)
2. Atzinīgi novērtēti 31. Starptautiskajā datu aizsardzības un privātuma komisāru konferencē, kas 2009. gada 4.–6. novembrī notika Madridē. [↑](#footnote-ref-3)
3. Sk. jo īpaši VDAR 105. apsvērumu. [↑](#footnote-ref-4)
4. Sk. Eiropas Padomes Konvenciju par piekļuvi oficiāliem dokumentiem (EPLS Nr. 205). [↑](#footnote-ref-5)
5. “Personas datu aizsardzībai ir būtiska nozīme, lai persona varētu izmantot 8. pantā garantētās tiesības uz privātās un ģimenes dzīves neaizskaramību”, ECT 1997. gada sprieduma lietā “MS pret Zviedriju” (pieteikums Nr. 20837/92) 41. punkts. [↑](#footnote-ref-6)
6. Sk. Council of Europe Commissioner on Human Rights, The rule of law on the Internet and in the wider digital world, Issue Paper, CommDH/IssuePaper(2014)1, 8 December 2014, p. 48, point 3.3 ’Everyone’ without discrimination. [↑](#footnote-ref-7)
7. Sk. ES Tiesas 2014. gada 11. decembra spriedumu lietā C212/13k “Františeks Rinešs [*František Ryneš*] pret “Úřad””. [↑](#footnote-ref-8)
8. Par starptautiskām organizācijām uzskata organizācijas, ko pārvalda saskaņā ar starptautiskajām publiskajām tiesībām. [↑](#footnote-ref-9)
9. Gadījumos, kad piemēro četras 1949. gada Ženēvas Konvencijas, to 1977. gada papildprotokolus un Starptautiskā Sarkanā Krusta un Sarkanā Pusmēness kustības statūtus. [↑](#footnote-ref-10)
10. Ministru komitejas 1997. gada 30. septembra Ieteikuma R(97)18 dalībvalstīm par tādu personas datu aizsardzību, kas vākti un apstrādāti statistikas mērķiem, papildinājuma 1. punkts. [↑](#footnote-ref-11)
11. Ministru komitejas Ieteikuma R(97)18 dalībvalstīm par tādu personas datu aizsardzību, kas vākti un apstrādāti statistikas mērķiem paskaidrojuma raksta 11. un 14. punkts. [↑](#footnote-ref-12)
12. Sk. Ministru komitejas Ieteikumu Nr. (97)18, *op. cit.* [↑](#footnote-ref-13)
13. Attiecīgā judikatūra jo īpaši ietver valsts drošības un konstitucionālās demokrātijas aizsardzību *inter alia* pret spiegošanu, terorismu, terorisma atbalstīšanu un separātismu. Valsts drošības apdraudējuma gadījumā jānodrošina aizsardzības pasākumi pret neierobežotu varu. Attiecīgos Eiropas Cilvēktiesību tiesas lēmumus var skatīt tās tīmekļvietnē (hudoc.echr.coe.int). [↑](#footnote-ref-14)
14. Attiecībā uz Pusēm, kas ir Eiropas Padomes dalībvalstis, šādas prasības ir izstrādātas Eiropas Cilvēktiesību tiesas judikatūrā saskaņā ar ECTK 8. pantu (sk. jo īpaši ECT 2015. gada 4. decembra sprieduma lietā “Romāns Zaharovs [*Roman Zakharov*] pret Krieviju” (pieteikums Nr. 47143/06) 233. punktu; 2016. gada 12. janvāra sprieduma lietā “Zabo [*Szabó*] un Visija [*Vissy*] pret Ungāriju” (pieteikums Nr. 37138/14) 75. punktu *et seq.*). [↑](#footnote-ref-15)
15. No brīža, kad Grozījumu protokols stājas spēkā, Papildu protokolu par uzraudzības institūcijām un pārrobežu datu plūsmām (EPLS Nr. 181) uzskata par grozītās Konvencijas neatņemamu sastāvdaļu. [↑](#footnote-ref-16)
16. No brīža, kad Grozījumu protokols stājas spēkā Papildu protokolu par uzraudzības institūcijām un pārrobežu datu plūsmām (EPLS Nr. 181) uzskata par grozītās Konvencijas neatņemamu sastāvdaļu. [↑](#footnote-ref-17)
17. Skat. 14. zemsvītras piezīmi. [↑](#footnote-ref-18)
18. Konvencijas grozījumi, ko Ministru komiteja apstiprināja 1999. gada 15. jūnijā, zaudē nozīmi no brīža, kad Protokols stājas spēkā. [↑](#footnote-ref-19)