Ieteikumi 01/2021 pietiekamības atsaucēm saskaņā ar Direktīvu par datu aizsardzību tiesībaizsardzības jomā

Pieņemti 2021. gada 2. februārī

Satura rādītājs

Eiropas Datu aizsardzības kolēģija,

ņemot vērā 51. panta 1. punkta b) apakšpunktu Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Direktīvā (ES) 2016/680 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI[1],

ņemot vērā sava Reglamenta 12. un 22. punktu,

IR PIEŅĒMUSI ŠOS IETEIKUMUS.

1. IEVADS

1. Darba grupa personu aizsardzībai attiecībā uz personas datu apstrādi (29. panta darba grupa) ir publicējusi darba dokumentu[2] par pietiekamības atsaucēm saskaņā ar Vispārīgo datu aizsardzības regulu (VDAR)[3]. Eiropas Datu aizsardzības kolēģija (EDAK) apstiprināja šo darba dokumentu savā pirmajā plenārsēdē.

2. Kā norādīts Lisabonas līgumam pievienotajā 21. deklarācijā, personas datu īpašo iezīmju dēļ var būt nepieciešami īpaši noteikumi par šo datu aizsardzību un par to brīvu apriti tiesu iestāžu sadarbībā krimināllietās un policijas sadarbībā, pamatojoties uz Līguma par Eiropas Savienības darbību (LESD) 16. pantu.

3. Pamatojoties uz to, ES likumdevējs pieņēma Direktīvu (ES) 2016/680 (Tiesībaizsardzības direktīva, turpmāk tekstā "TAD"), ar ko nosaka īpašus noteikumus attiecībā uz personas datu apstrādi, ko kompetentās iestādes veic, lai **novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu.**

4. TAD ir izklāstīti pamatojumi, saskaņā uz kuriem ir atļauts nosūtīt personas datus uz trešo valsti vai starptautisku organizāciju šajā kontekstā. Viens no šādas nosūtīšanas pamatojumiem ir Eiropas Komisijas lēmums, ka attiecīgā trešā valsts vai starptautiskā organizācija nodrošina pietiekamu aizsardzības līmeni.

5. Ja darba dokumenta WP254 rev.01 par pietiekamības atsaucēm mērķis ir sniegt norādījumus Eiropas Komisijai par datu aizsardzības līmeni trešās valstīs un starptautiskās organizācijās saskaņā ar VDAR, šā dokumenta mērķis ir sniegt līdzīgas vadlīnijas atbilstīgi TAD. Šajā kontekstā šajā

[1] OV L 119, 4.5.2016., 89. lpp.
[2] WP254 rev.01, kuru 29. panta darba grupa pieņēma 2017. gada 28. novembrī; jaunākā pārskatītā redakcija tika pieņemta 2018. gada 6. februārī. Ar to tiek atjaunināta I nodaļa "Personas datu nosūtīšana uz trešām valstīm: ES Datu aizsardzības direktīvas 25. un 26. panta piemērošana" darba dokumentā WP12, kuru 29. panta darba grupa pieņēma 1998. gada 24. jūlijā.
[3] Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 26. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

dokumentā ir izklāstīti datu aizsardzības pamatprincipi, kuriem ir jābūt ievērotiem trešās valsts vai starptautiskas organizācijas tiesiskajā regulējumā, lai nodrošinātu, ka tas ir pēc būtības līdzvērtīgs ES sistēmai TAD darbības jomā (proti, attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināLsodus). Turklāt tas var kalpot kā norāde trešām valstīm un starptautiskām organizācijām, kuras vēlas nodrošināt pietiekamību.

6. Šajā dokumentā uzmanība ir pievērsta tikai lēmumiem par aizsardzības līmeņa pietiekamību. Tie ir Eiropas Komisijas īstenošanas akti saskaņā ar TAD 36. panta 3. punktu.

2. PIETIEKAMĪBAS JĒDZIENS

7. TAD ir izklāstīti noteikumi saistībā ar personas datu nosūtīšanu uz trešām valstīm un starptautiskām organizācijām tiktāl, ciktāl šāda nosūtīšana ietilpst TAD darbības jomā. Noteikumi par personas datu starptautisku nosūtīšanu ir izklāstīti TAD V nodaļā, jo īpaši tās 35.–39. pantā.

8. Saskaņā ar TAD 36. pantu datu nosūtīšana uz trešo valsti vai starptautisku organizāciju var notikt, ja trešā valsts, teritorija vai viens vai vairāki konkrēti sektori trešā valstī, vai starptautiska organizācija nodrošina pietiekamu aizsardzības līmeni. No Eiropas Savienības Tiesas (EST) judikatūras[4] izriet, ka šis noteikums ir jālasa kopā ar TAD 35. pantu ar nosaukumu "Personas datu nosūtīšanas vispārīgie principi", kurā noteikts, ka "[v]isus [TAD V nodaļas] noteikumus piemēro tā, lai nodrošinātu, ka nemazinās ar šo direktīvu nodrošinātais fizisko personu aizsardzības līmenis".

9. Ja Eiropas Komisija ir nolēmusi, ka tiek nodrošināts šāds pietiekams aizsardzības līmenis, personas datus var nosūtīt uz šo trešo valsti, teritoriju, sektoru vai starptautisku organizāciju bez nepieciešamības saņemt īpašu atļauju, izņemot gadījumus, kad citai dalībvalstij, no kuras iegūti dati, ir jāsniedz atļauja nosūtīšanai, kā paredzēts TAD 35. un 36. pantā un 66. apsvērumā. Tas neskar prasību, ka attiecīgo dalībvalstu iestāžu veiktajai datu apstrādei ir jāatbilst valsts noteikumiem, kas pieņemti saskaņā ar Direktīvu (ES) 2016/680.

10. Šo jēdzienu "pietiekams aizsardzības līmenis", kas pastāvēja jau saskaņā ar Direktīvu 95/46[5] un Padomes Pamatlēmumu 2008/977/TI[6], EST ir turpinājusi attīstīt šajā kontekstā un — pēdējā laikā — VDAR ietvaros.

11. Kā noteikusi EST, lai gan aizsardzības līmenim trešā valstī būtībā ir jābūt līdzvērtīgam ES garantētajam līmenim, "līdzekļi, pie kuriem šī trešā valsts ķeras šādas aizsardzības nodrošināšanai, var atšķirties no tiem, kas tikuši likti lietā Savienībā", taču "šiem līdzekļiem tik un tā praksē būtu jābūt efektīviem"[7]. Tāpēc pietiekamības standartam nav jābūt ES tiesību aktu precīzam atspoguļojumam, bet ar to ir jānosaka šo tiesību aktu būtiskas pamatprasības.

---

[4] Tiesas 2020. gada 16. jūlija spriedums *Data Protection Commissioner* / *Facebook Ireland Limited*, *Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559, 92. punkts (*Schrems II)*.

[5] Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV L 281, 23.11.1995., 31. lpp.).

[6] Padomes Pamatlēmums 2008/977/TI (2008. gada 27. novembris) par tādu personas datu aizsardzību, ko apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās (OV L 350, 30.12.2008., 60. lpp.).

[7] Tiesas 2015. gada 6. oktobra spriedums *Maximillian Schrems* / *Data Protection Commissioner*, C−362/14, ECLI:EU:C:2015:650, 73. un 74. punkts (*Schrems I*).

12. Šajā kontekstā Tiesa arī precizēja, ka Komisijas lēmumā par aizsardzības līmeņa pietiekamību būtu jāietver secinājums par to, ka trešā valstī ir spēkā valsts tiesību akti, kuru mērķis ir ierobežot iespējamo iejaukšanos to personu pamattiesībās, kuru dati no Eiropas Savienības ir pārsūtīti uz šo trešo valsti, — iejaukšanos, ko šīs valsts publiskā sektora struktūras ir *tiesīgas* praktizēt, ja tā kalpo leģitīmam mērķim — kā valsts drošība[8].

13. Eiropas Komisijas lēmumu par aizsardzības līmeņa pietiekamību nolūks ir oficiāli apstiprināt, radot dalībvalstīm[9], tostarp to kompetentajām datu aizsardzības iestādēm[10], saistošas sekas, ka datu aizsardzības līmenis trešā valstī vai starptautiskā organizācijā būtībā ir līdzvērtīgs datu aizsardzības līmenim Eiropas Savienībā. Trešai valstij būtu jāpiedāvā garantijas, kas nodrošinātu pietiekamu aizsardzības līmeni, kurš pēc būtības ir līdzvērtīgs Savienībā nodrošinātajam, jo īpaši, ja datus apstrādā vienā vai vairākos konkrētos sektoros[11].

14. Pietiekamību var panākt, apvienojot datu subjektu tiesības un to personu pienākumus, kuras datus apstrādā vai arī kuras īsteno kontroli pār neatkarīgu struktūru veikto apstrādi un uzraudzību. Tomēr datu aizsardzības noteikumi ir efektīvi tikai tad, ja tie ir izpildāmi un tiek ievēroti praksē. Tāpēc ir jāņem vērā ne tikai to noteikumu saturs, kuri attiecas uz personas datiem, kas nosūtīti uz trešo valsti vai starptautisku organizāciju, bet arī ieviestā sistēma, kas nodrošina šādu noteikumu efektivitāti. Efektīvi izpildes mehānismi ir ārkārtīgi svarīgi, lai nodrošinātu datu aizsardzības noteikumu efektivitāti[12].

3. PIETIEKAMĪBAS KONSTATĒJUMU PROCESUĀLIE ASPEKTI SASKAŅĀ AR TAD

15. Lai EDAK varētu pildīt savu uzdevumu, sniedzot konsultācijas Eiropas Komisijai saskaņā ar TAD 51. panta 1. punkta g) apakšpunktu, EDAK būtu jāsaņem visa attiecīgā dokumentācija, tostarp attiecīgā korespondence un Eiropas Komisijas konstatējumi. Ir absolūti nepieciešams, lai visa attiecīgā dokumentācija tiktu pārsūtīta EDAK pietiekami savlaicīgi un tiktu iztulkota angļu valodā, lai varētu noturēt informētas un noderīgas apspriešanās pirms lēmumu par aizsardzības līmeņa pietiekamību galīgās pieņemšanas. Ja tiesiskais regulējums ir sarežģīts, tajā būtu jāiekļauj visi ziņojumi, kas sagatavoti par trešās valsts vai starptautiskās organizācijas datu aizsardzības līmeni. Jebkurā gadījumā Eiropas Komisijas sniegtajai informācijai vajadzētu būt izsmeļošai un tādai, lai EDAK varētu novērtēt Komisijas veikto analīzi attiecībā uz datu aizsardzības līmeni trešā valstī vai starptautiskā organizācijā.

16. EDAK savlaicīgi sniegs atzinumu par Eiropas Komisijas konstatējumiem, identificējot pietiekamības sistēmas nepilnības, ja tādas būs, un attiecīgā gadījumā sniedzot iespējamos ieteikumus.

---

[8] *Schrems I*, 88. punkts.
[9] LESD 288. panta 2. punkts.
[10] *Schrems I*, 52. punkts.
[11] TAD 67. apsvērums.
[12] *Schrems I*, 72.–74. punkts, un EST 2017. gada 26. jūlija Atzinums 1/15par nolīguma projektu starp Kanādu un Eiropas Savienību, ECLI:EU:C:2017:592 (Atzinums 1/15), 134. punkts: "Šīs tiesības uz personas datu aizsardzību it īpaši pieprasa, lai ar Savienības tiesībām piešķirto brīvību un pamattiesību augstais aizsardzības līmenis tiktu joprojām nodrošināts gadījumā, kad personas dati tiek no Savienības pārsūtīti uz kādu trešo valsti. Pat ja līdzekļi šāda aizsardzības līmeņa nodrošināšanai var atšķirties no tiem, kas ieviesti Savienībā, lai nodrošinātu no Savienības tiesībām izrietošo prasību ievērošanu, šiem līdzekļiem tik un tā praksē būtu jābūt efektīviem, lai nodrošinātu Savienībā esošajai aizsardzībai būtībā ekvivalentu aizsardzību."

17. Saskaņā ar TAD 36. panta 4. punktu Eiropas Komisijai pastāvīgi ir jāuzrauga norises, kas varētu ietekmēt lēmuma par aizsardzības līmeņa pietiekamību darbību.

18. TAD 36. panta 3. punktā ir noteikts, ka vismaz reizi četros gados ir jāveic periodiska pārskatīšana. Tomēr tas ir vispārīgs laika posms, kas ir jāpielāgo katrai trešai valstij vai starptautiskai organizācijai, pieņemot lēmumu par aizsardzības līmeņa pietiekamību. Atkarībā no konkrētajiem apstākļiem pārskatīšanas cikls var būt īsāks. Arī incidenti vai cita informācija par attiecīgās trešās valsts vai starptautiskās organizācijas tiesisko regulējumu vai tā izmaiņām var radīt vajadzību veikt pārskatīšanu pirms termiņa. Šķiet, ir arī lietderīgi pirmoreiz pārskatīt pilnīgi jaunu lēmumu par aizsardzības līmeņa pietiekamību diezgan agrā stadijā un pakāpeniski pielāgot pārskatīšanas ciklu atkarībā no rezultāta.

19. Ņemot vērā uzdevumu Eiropas Komisijai sniegt atzinumu par to, ka trešā valsts, kāda minētās trešās valsts teritorija vai viens vai vairāki konkrēti sektori vai starptautiska organizācija vairs nenodrošina pietiekamu aizsardzības līmeni, EDAK savlaicīgi ir jāsaņem jēgpilna informācija par to, kā ES Komisija uzrauga attiecīgās norises šajā trešā valstī vai starptautiskajā organizācijā. Tādējādi EDAK būtu jāsaņem informācija par jebkuru pārskatīšanas procesu un pārskatīšanas vizīti trešā valstī vai starptautiskajā organizācijā. EDAK iesaka uzaicināt to piedalīties šajos pārskatīšanas procesos un misijās, kā tas bija paredzēts lēmumā par privātuma vairogu un ir paredzēts lēmumā par Japānas nodrošinātā aizsardzības līmeņa pietiekamību.

20. Tāpat būtu jāatzīmē, ka saskaņā ar TAD 36. panta 5. punktu Eiropas Komisijai ir tiesības gadījumos, ja trešā valsts vai starptautiska organizācija vairs nenodrošina pietiekama līmeņa aizsardzību, atcelt, grozīt vai apturēt esošos lēmumus par aizsardzības līmeņa pietiekamību. Atcelšanas, grozīšanas vai apturēšanas procedūrā iesaista EDAK, pieprasot tās atzinumu saskaņā ar TAD 51. panta 1. punkta g) apakšpunktu.

21. Turklāt, neskarot kriminālvajāšanas iestāžu pilnvaras, uzraudzības iestādēm vajadzētu būt arī pilnvarām pievērst tiesu iestāžu uzmanību šīs direktīvas pārkāpumiem vai iesaistīties tiesvedībā[13]. Tas jo īpaši izriet no EST sprieduma lietā *Schrems I*, proti, ka datu aizsardzības iestādēm ir jāspēj iesaistīties tiesvedībā valsts tiesās, ja tās uzskata personas prasību attiecībā uz lēmumu par aizsardzības līmeņa pietiekamību par pamatotu[14]. Ar spriedumu lietā *Schrems II* tika apstiprināts šis vērtējums[15].

4. ES PIETIEKAMĪBAS STANDARTI, ĪSTENOJOT POLICIJAS SADARBĪBU UN TIESU IESTĀŽU SADARBĪBU KRIMINĀLLIETĀS

[13] Sk. TAD 47. panta 5. punktu un 82. apsvērumu.
[14] Sk. spriedumu lietā *Schrems I*, 65. punktu: "Šajā ziņā valsts likumdevēja ziņā ir paredzēt tiesiskās aizsardzības līdzekļus, kas valsts uzraudzības iestādei ļauj valstu tiesās izvirzīt iebildes, ko tā uzskata par pamatotām, lai šīs tiesas — ja arī tās piekrīt šīs iestādes šaubām par Komisijas lēmuma spēkā esamību — iesniegtu lūgumu sniegt prejudiciālu nolēmumu šī lēmuma spēkā esamības izvērtēšanas nolūkos."
[15] Sk. spriedumu lietā *Schrems II*, 120. punktu: "Tādējādi, pat ja pastāv Komisijas lēmums par aizsardzības līmeņa pietiekamību, kompetentajai valsts uzraudzības iestādei, kurā ir vērsusies persona ar sūdzību par tās tiesību un brīvību aizsardzību attiecībā uz personas datu apstrādi, ir jābūt iespējai pilnīgi neatkarīgi pārbaudīt, vai šo datu nodošana atbilst VDAR noteiktajām prasībām, un vajadzības gadījumā celt prasību valsts tiesās, lai pēdējās minētās, ja tās piekrīt šīs iestādes viedoklim attiecībā uz lēmuma par aizsardzības līmeņa pietiekamību spēkā esamību, iesniegtu lūgumu sniegt prejudiciālu nolēmumu nolūkā pārbaudīt šo spēkā esamību."

22. Runājot par saturu, lēmumos par aizsardzības līmeņa pietiekamību galvenā uzmanība būtu jāpievērš attiecīgās trešās valsts spēkā esošo tiesību aktu novērtēšanai kopumā, teorijā un praksē, ņemot vērā TAD 36. pantā noteiktos vērtēšanas kritērijus. Trešās valsts vai starptautiskas organizācijas sistēmā ir jāietver šādi pamata vispārīgie, procesuālie un izpildes datu aizsardzības principi un mehānismi.

23. TAD 36. panta 2. punktā ir noteikti elementi, kurus Eiropas Komisija ņem vērā, izvērtējot aizsardzības līmeņa pietiekamību trešā valstī vai starptautiskā organizācijā.

24. Komisija jo īpaši ņem vērā tiesiskumu, cilvēktiesību un pamatbrīvību ievērošanu[16], attiecīgos tiesību aktus, kā arī šādu tiesību aktu īstenošanu, efektīvas un īstenojamas datu subjektu tiesības un efektīvu administratīvo un tiesisko aizsardzību datu subjektiem, kuru personas dati tiek nosūtīti, vienas vai vairāku neatkarīgu uzraudzības iestāžu esamību un efektīvu darbību, kā arī starptautiskās saistības, ko trešā valsts vai starptautiskā organizācija ir uzņēmusies.

25. Tādēļ ir skaidrs, ka jebkurai jēgpilnai pietiekamas aizsardzības analīzei ir jāietver divi pamatelementi: piemērojamo noteikumu saturs un līdzekļi to efektīvai īstenošanai praksē. Eiropas Komisijai regulāri jāpārbauda, vai spēkā esošie noteikumi praksē ir efektīvi.

26. Datu aizsardzības vispārīgo principu un procesuālo un izpildes prasību būtība, ko varētu uzskatīt par minimālajām prasībām pietiekamam datu aizsardzības līmenim, izriet no ES Pamattiesību hartas (Harta) un TAD. Vispārīgi noteikumi par datu aizsardzību un privātumu trešā valstī nav pietiekami. Tieši pretēji, trešās valsts vai starptautiskās organizācijas tiesiskajā regulējumā ir jāiekļauj īpaši noteikumi, kas konkrēti attiecas uz datu aizsardzību tiesībaizsardzības jomā. Trešai valstij būtu jāpiedāvā garantijas, kas nodrošinātu pietiekamu aizsardzības līmeni, kurš pēc būtības ir līdzvērtīgs Savienībā nodrošinātajam. Šiem noteikumiem jābūt izpildāmiem.

27. Turklāt attiecībā uz samērīguma principu[17] EST saistībā ar dalībvalstu tiesību aktiem ir spriedusi, ka jautājums par to, vai tiesību uz privātumu un datu aizsardzību ierobežojums var būt pamatots, ir jāizvērtē, no vienas puses, izsverot **iejaukšanās**, ko rada šāds ierobežojums, **smagumu**[18] un pārbaudot, vai **vispārējo interešu mērķa nozīmīgums**, kas ir šā ierobežojuma pamats, ir atbilstošs šim smagumam, no otras puses[19].

28. Saskaņā ar EST judikatūru pašā juridiskajā pamatā, kas ļauj iejaukties pamattiesībās, lai tas atbilstu samērīguma principam, ir jānosaka attiecīgo tiesību īstenošanas ierobežojuma apjoms[20]. Atkāpes no personas datu aizsardzības un tās ierobežojumi ir jāīsteno, stingri ievērojot vajadzīgās robežas[21]. Lai izpildītu šo prasību, attiecīgajos tiesību aktos papildus skaidru un precīzu noteikumu

[16] Novērtējot trešās valsts tiesisko regulējumu, būtu jāņem vērā iespēja, ka, pamatojoties uz datiem, kas nosūtīti no ES, pastāv nāvessoda piemērošanas vai jebkāda veida nežēlīgas un necilvēcīgas izturēšanās risks. Patiešām, ja šāds sods vai izturēšanās ir paredzēti trešās valsts tiesību aktos, trešās valsts tiesiskajā regulējumā būtu jāatrod papildu aizsardzības pasākumi, lai nodrošinātu, ka no ES nosūtītos datus neizmanto nāvessoda vai jebkāda veida nežēlīgas un necilvēcīgas izturēšanās pieprasīšanai, piespriešanai vai izpildei (piem., starptautisks nolīgums, kurā noteikti nosacījumi nosūtīšanai, trešās valsts apņemšanās nepiemērot nāvessodu vai jebkāda veida nežēlīgu un necilvēcīgu izturēšanos, pamatojoties uz datiem, kas nosūtīti no ES, vai nāves soda moratorijs).
[17] Hartas 52. panta 1. punkts.
[18] Tiesa, piem., arī atzīmēja, ka "iejaukšanās, ko rada datu vākšana reāllaikā, kas ļauj noteikt galaiekārtas atrašanās vietu, ir īpaši smaga, jo šie dati kompetentajām valsts iestādēm sniedz veidu, kā precīzi un pastāvīgi uzraudzīt mobilo tālruņu lietotāju pārvietošanos (..)" (Tiesas 2020. gada 6. oktobra spriedums *La Quadrature du Net* u. c., apvienotās lietas C-511/18, C-512/18 un C-520/18, ECLI:EU:C:2020:791, 187. punkts un tajā citētā judikatūra).
[19] *La Quadrature du Net* u. c., 131. punkts.
[20] *Schrems II*, 180. punkts.
[21] *Schrems II*, 176. punkts un tajā citētā judikatūra.

noteikšanai, ar ko reglamentē attiecīgā pasākuma apjomu un piemērošanu, ir jānosaka minimālie aizsardzības pasākumi, lai personām, kuru dati ir pārsūtīti, būtu pietiekamas garantijas, ka viņu personas dati tiek efektīvi aizsargāti pret ļaunprātīgas izmantošanas risku. "Tajā it īpaši ir jānorāda, kādos apstākļos un saskaņā ar kādiem nosacījumiem šādu datu apstrādi paredzošs pasākums var tikt veikts, tādējādi garantējot, ka šāda iejaukšanās notiek tikai stingri nepieciešamajā apmērā. Šādu garantiju nepieciešamība ir vēl jo svarīgāka tādēļ, ka personas dati tiek apstrādāti automātiski.[22]"

29. EDAK ir pieņēmusi ieteikumus, kuros identificētas būtiskas garantijas, kas atspoguļo EST un Eiropas Cilvēktiesību tiesas (ECT) judikatūru novērošanas jomā un kam ir jābūt trešās valsts tiesību aktos, novērtējot šādu trešo valstu novērošanas pasākumu iejaukšanos datu subjektu tiesībās gadījumā, ja dati tiek nosūtīti uz šo trešo valsti saskaņā ar VDAR[23]. Lai novērtētu, vai ir ievēroti TAD 36. panta 2. punkta a) apakšpunktā izklāstītie nosacījumi, EDAK uzskata, ka šajos ieteikumos noteiktās garantijas ir jāņem vērā, novērtējot trešās valsts atbilstību TAD novērošanas jomā, šajā kontekstā ņemot vērā citus īpašos apstākļus novērošanas jomā.

30. Saistībā ar TAD 36. panta 2. punkta b) apakšpunktā izklāstīto prasību trešai valstij būtu ne tikai jānodrošina efektīva neatkarīga datu aizsardzības uzraudzība, bet arī jāparedz sadarbības mehānismi ar dalībvalstu datu aizsardzības iestādēm[24].

31. Saistībā ar 36. panta 2. punkta c) apakšpunktā izklāstīto prasību papildus starptautiskajām saistībām, ko trešā valsts vai starptautiskā organizācija ir uzņēmusies, ir jāņem vērā arī saistības, kas izriet no trešās valsts vai starptautiskās organizācijas dalības daudzpusējās vai reģionālās sistēmās, īpaši attiecībā uz personas datu aizsardzību, kā arī šādu saistību izpildi, jo īpaši trešai valstij pievienojoties citiem starptautiskiem nolīgumiem par datu aizsardzību, piemēram, būtu jāņem vērā Eiropas Padomes 1981. gada 28. janvāra Konvencija par personu aizsardzību attiecībā uz personas datu automātisku apstrādi un tās papildprotokols (Konvencija Nr. 108[25] un tās modernizētā versija, Konvencija Nr. 108+). Var ņemt vērā arī trešās valsts atbilstību principiem, kas iekļauti starptautiskos dokumentos, piemēram, Eiropas Padomes "Praktiskajā ceļvedī par personas datu izmantošanu policijas nozarē: kā aizsargāt personas datus, apkarojot noziedzību".

32. Lēmumam par aizsardzības līmeņa pietiekamību būtu jānodrošina, ka, pateicoties privātuma un datu aizsardzības tiesību būtībai un to efektīvai īstenošanai, uzraudzībai un izpildei, ārvalstu sistēma kopumā nodrošina nepieciešamo aizsardzības līmeni, tostarp attiecībā uz datiem, kas tiek nosūtīti uz šo trešo valsti. Kā uzsvēra EST spriedumā lietā *Schrems II*, garantētais augstais aizsardzības līmenis ir jānodrošina arī datu nosūtīšanas laikā uz trešo valsti[26].

33. Visbeidzot, pieņemot lēmumu par aizsardzības līmeņa pietiekamību tikai attiecībā uz teritoriju vai konkrētu sektoru trešā valstī, Eiropas Komisijai būtu jāņem vērā skaidri un objektīvi kritēriji, piemēram, konkrētas apstrādes darbības vai piemērojamo juridisko standartu un attiecīgajā trešā valstī spēkā esošo tiesību aktu darbības joma[27].

A. Vispārīgi principi un garantijas

[22] *Schrems II*, 176. punkts un tajā citētā judikatūra.
[23] EDAK Ieteikumi 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem, pieņemti 2020. gada 10. novembrī.
[24] TAD 67. apsvērums.
[25] TAD 68. apsvērums.
[26] Sk. 93. punktu.
[27] TAD 67. apsvērums.

a) Jēdzieni

34. Ir jāpastāv datu aizsardzības pamatjēdzieniem. Tiem nav jāatspoguļo TAD terminoloģija, bet tiem būtu jāatspoguļo Eiropas datu aizsardzības tiesību aktos ietvertie jēdzieni un būtu jāsaskan ar tiem. Piemēram, TAD ir iekļauti šādi svarīgi jēdzieni: "personas dati", "personas datu apstrāde", "kompetentās iestādes", "datu pārzinis", "datu apstrādātājs", "saņēmējs", "sensitīvi dati", "precizitāte", "profilēšana", "integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma", "uzraudzības iestāde" un "pseidonimizācija".

b) Personas datu apstrādes likumība un godprātība (4. pants, 26. apsvērums)

35. Saskaņā ar Hartas 8. panta 2. punktu personas dati citstarp ir jāapstrādā "noteiktiem mērķiem un ar attiecīgās personas piekrišanu vai ar citu likumīgu pamatojumu, kas paredzēts tiesību aktos"[28]. Tomēr tiesībaizsardzības kontekstā ir jāatzīmē, ka tādu noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas vai saukšanas pie atbildības par tiem uzdevumu veikšana, kuri ar likumu ir institucionāli uzdoti kompetentajām iestādēm, ļauj tām pieprasīt vai pavēlēt fiziskām personām izpildīt iesniegtos lūgumus. Šādā gadījumā datu subjekta piekrišanai nebūtu jākalpo par kompetentās iestādes veiktās personas datu apstrādes juridisko pamatu[29].

36. Šajā juridiskajā pamatā ir jāparedz skaidri un precīzi noteikumi attiecībā uz attiecīgo datu apstrādes darbību tvērumu un piemērošanu, un jāparedz minimālās prasības[30]. Turklāt EST atgādināja, ka "tiesiskajam regulējumam ir jābūt juridiski saistošam valsts tiesībās"[31].

37. Lai datu apstrāde būtu likumīga[32], tai ir jābūt nepieciešamai, lai izpildītu uzdevumu, kuru kompetentā iestāde veic, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu[33]. Šiem nolūkiem ir jābūt paredzētiem valsts tiesību aktos.

38. Personas dati ir jāapstrādā godprātīgi. Tāds datu aizsardzības princips kā godprātīga apstrāde ir atsevišķs jēdziens, kas atšķiras no tiesībām uz taisnīgu tiesu, kā noteikts Hartas 47. pantā un Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas (ECTK) 6. pantā[34].

c) Mērķa ierobežojuma princips (4. pants)

[28] Sk. spriedumu lietā *Schrems II*, 173. punkts.

[29] TAD 35. apsvērumā arī teikts, ka tad, "ja datu subjektam liek pildīt kādu juridisku pienākumu, datu subjektam nav reālas un brīvas izvēles, tādēļ datu subjekta reakciju nevar uzskatīt par brīvprātīgi sniegtu norādi uz viņa vēlmēm. Tam nebūtu jāliedz dalībvalstīm likumā paredzēt, ka datu subjekts var piekrist savu personas datu apstrādei šīs direktīvas nolūkos, piemēram, DNS testiem kriminālizmeklēšanā vai tā atrašanās vietas uzraudzībai ar elektroniskām ierīcēm krimināsodu izpildei".

[30] Sk. spriedumu lietā *Schrems II*, 175. un 180. punkts, un Atzinumu 1/15, 139. punkts un tajā citētā judikatūra.

[31] Sk. 2020. gada 6. oktobra spriedumu *Privacy International* / *Secretary of State for Foreign and Commonwealth Affairs* u. c., C-623/17, ECLI: EU:C:2020:790, 68. punkts; jāsaprot, ka sprieduma franču valodas versijā EST lieto vārdu "*réglementation*", kam ir plašāka nozīme nekā tikai "Parlamenta akti".

[32] Personas datu apstrāde, kas pilnībā vai daļēji veikta ar automatizētiem līdzekļiem, un tādu personas datu apstrāde, kuri veido daļu no kartotēkas vai ir paredzēti, lai veidotu daļu no kartotēkas, ja apstrādi neveic ar automatizētiem līdzekļiem.

[33] Kompetentās iestādes ir jebkura valsts iestāde, kas ir kompetenta šādiem nolūkiem, vai jebkura cita struktūra vai vienība, kam tiesību aktos uzticēts īstenot publisko varu un publiskās pilnvaras šādiem nolūkiem.

[34] TAD 26. apsvērums.

39. Konkrētajiem personas datu apstrādes nolūkiem jo īpaši vajadzētu būt nepārprotamiem, leģitīmiem un noteiktiem jau personas datu vākšanas laikā[35].

40. Dati būtu jāapstrādā konkrētam, nepārprotamam un likumīgam nolūkam, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināLsodus[36], tostarp lai pasargātu no draudiem sabiedriskajai drošībai trešā valstī un tos novērstu, un pēc tam izmantotiem jebkuram no šiem nolūkiem, ciktāl tas nav pretrunā ar apstrādes sākotnējo nolūku (piem., izmantošanai šādiem nolūkiem paralēlām izpildes procedūrām vai arhivēšanai sabiedrības interesēs, zinātniskiem, statistikas vai vēsturiskiem mērķiem) un ievērojot atbilstošus datu subjektu tiesību un brīvību aizsardzības pasākumus. Ja personas datus apstrādā tas pats vai cits pārzinis (kompetentā iestāde[37]) nolūkā novērst, izmeklēt, atklāt vai saukt pie atbildības par noziedzīgiem nodarījumiem vai izpildīt krimināLsodus, izņemot tādus, attiecībā uz kuriem dati apkopoti, šāda apstrāde būtu jāatļauj ar nosacījumu, ka šī apstrāde ir atļauta saskaņā ar piemērojamiem tiesību aktiem un ir nepieciešama un samērīga šim citam nolūkam[38]. Jāņem vērā arī tas, vai eksistē mehānisms attiecīgās dalībvalstu kompetentās iestādes informēšanai par šādu turpmāku datu apstrādi[39]. Turklāt jebkurā gadījumā nevajadzētu tikt mazinātam fizisko personu aizsardzības līmenim, ko Savienībā garantē TAD, tostarp gadījumos, kad personas datus no trešās valsts nosūta pārzinim vai apstrādātājiem tajā pašā trešā valstī[40].

d) Specifiski nosacījumi attiecībā uz turpmāku apstrādi citiem nolūkiem (9. pants)

41. Attiecībā uz tādu datu turpmāku apstrādi vai izpaušanu, kas nosūtīti no ES citiem nolūkiem, nevis tiesībaizsardzības mērķiem, piemēram, valsts drošības nolūkiem, šādai apstrādei vai izpaušanai vajadzētu būt arī paredzētai likumā un vajadzētu būt nepieciešamai un samērīgai. Būtu jāņem vērā arī tas, vai eksistē mehānisms attiecīgās dalībvalstu kompetentās iestādes informēšanai par šādu turpmāku datu apstrādi[41]. Arī šajā gadījumā, t. i., pēc turpmākas apstrādes vai izpaušanas, datiem būtu jānodrošina tāds pats aizsardzības līmenis kā tad, kad tos sākotnēji apstrādāja saņēmēja kompetentā iestāde.

e) Datu minimizēšanas princips

42. Datiem vajadzētu būt adekvātiem, atbilstīgiem un ne pārmērīgiem, ņemot vērā nolūkus, kādos tos apstrādā. Jo īpaši būtu jāņem vērā integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma piemērošana, piemēram, ierobežoti ievades lauki (strukturēta saziņa) vai automatizētas un neautomatizētas kvalitātes pārbaudes.

---

[35] TAD 26. apsvērums.

[36] Tas ietver policijas darbības bez iepriekšējām zināšanām par to, vai incidents ir noziedzīgs nodarījums. "Šādas darbības var ietvert arī varas pielietošanu, veicot piespiedu pasākumus, piemēram, policijas darbības demonstrāciju, liela mēroga sporta pasākumu un nemieru laikā. Tās ietver arī likumības un kārtības uzturēšanu kā uzdevumu, kas uzticēts policijai vai citām tiesībaizsardzības iestādēm, kad nepieciešams pasargāt no tādiem draudiem sabiedriskajai drošībai un ar likumu aizsargātām fundamentālām sabiedrības interesēm, kas varētu novest pie noziedzīga nodarījuma, un šos draudus novērst" (TAD 12. apsvērums). Tas ir jānošķir no valsts drošības mērķa vai no darbībām, kas ietilpst Līguma par Eiropas Savienību (LES) V sadaļas 2. nodaļas darbības jomā (TAD 14. apsvērums).

[37] Sk. 33. zemsvītras piezīmi.

[38] TAD 29. apsvērums.

[39] Šāds mehānisms varētu būt, piem., savstarpēji saskaņoti apstrādes kodi, informēšanas pienākums saskaņā ar starptautisku instrumentu, tostarp iespējami automatizēti paziņojumi, vai citi līdzīgi pārredzamības pasākumi.

[40] TAD 64. apsvērums.

[41] Sk. 39. zemsvītras piezīmi.

f) Datu precizitātes princips

43. Datiem vajadzētu būt precīziem un nepieciešamības gadījumā atjauninātiem. Tomēr datu precizitātes princips būtu jāpiemēro, ņemot vērā attiecīgās apstrādes raksturu un nolūkus. Jo īpaši tiesvedībā izteikumi, kas satur personas datus, balstās uz fizisko personu subjektīvu uztveri un ne vienmēr ir pārbaudāmi. Attiecīgi prasībai par precizitāti nebūtu jāattiecas uz izteikuma precizitāti, bet vienīgi uz to, ka ir izdarīts konkrēts izteikums[42].

44. Būtu jānodrošina, ka personas dati, kas ir neprecīzi, nepilnīgi vai vairs nav aktuāli, netiek nosūtīti vai darīti pieejami[43] un ka ir paredzētas procedūras neprecīzu datu labošanai vai dzēšanai. Jo īpaši būtu jāņem vērā jebkāda apstrādātās informācijas klasifikācijas sistēma attiecībā uz avota ticamību un faktu pārbaudes līmeni[44].

g) Datu saglabāšanas princips

45. Dati būtu jāglabā ne ilgāk, kā tas ir nepieciešams, nolūkiem kādiem tos apstrādā. Būtu jāizveido atbilstoši mehānismi personas datu dzēšanai; tas var būt noteikts periods vai periodiska personas datu glabāšanas nepieciešamības pārskatīšana (vai abu kombinācija: fiksēts maksimālais periods un periodiska pārskatīšana noteiktos intervālos)[45]. Attiecībā uz personas datiem, kurus glabā ilgāku laiku saistībā ar arhivēšanu sabiedrības interesēs, izmantošanu zinātniskiem, statistikas vai vēsturiskiem mērķiem, būtu jānosaka atbilstīgas garantijas (piem., attiecībā uz piekļuvi)[46].

h) Drošības un konfidencialitātes princips (29. pants, 28. un 71. apsvērums)

46. Jebkurai vienībai, kas apstrādā personas datus, būtu jānodrošina, ka dati tiek apstrādāti veidā, kas nodrošina personas datu drošību, tostarp novēršot neatļautu piekļuvi personas datiem vai to izmantošanu un neatļautu piekļuvi apstrādei izmantotajām iekārtām. Tas ietver aizsardzību pret nelikumīgu apstrādi, nejaušu nozaudēšanu, iznīcināšanu vai bojājumu un atbilstošus pasākumus, lai to novērstu, izmantojot atbilstošus tehniskos un organizatoriskos pasākumus. Nosakot drošības līmeni, būtu jāņem vērā tehnikas līmenis, ieviešanas izmaksas un apstrādes raksturs, tvērums, konteksts un nolūki, kā arī ar fizisku personu tiesībām un brīvībām saistīto risku atšķirīgā iespējamība un nopietnība.

47. Starp dalībvalstu iestādēm, kas pārsūta personas datus, un trešo valstu saņēmējām iestādēm būtu jānodrošina droši saziņas kanāli.

i) Pārredzamības princips (13. pants, 26., 39., 42., 43., 44. un 46. apsvērums)

48. Fiziskas personas būtu jāinformē par riskiem, noteikumiem, garantijām un tiesībām saistībā ar viņu personas datu apstrādi un par to, kā viņi var īstenot savas tiesības saistībā ar apstrādi[47].

49. Informācija par visiem galvenajiem personas datu apstrādes elementiem būtu jāpadara attiecīgajiem indivīdiem pieejama. Šai informācijai būtu jābūt viegli pieejamai un viegli saprotamai skaidrā un vienkāršā valodā. Šādā informācijā būtu jāiekļauj apstrādes nolūks, personas datu

[42] TAD 30. apsvērums.
[43] TAD 32. apsvērums.
[44] Piem., 4x4 režģi uzticamības novērtēšanai un apstrādes kodi.
[45] TAD 5. pants.
[46] TAD 26. apsvērums.
[47] TAD 26. apsvērums.

pārziņa identitāte, viņiem pieejamās tiesības[48] un cita informācija, ciktāl tas ir nepieciešams godprātības nodrošināšanai.

50. Šīm tiesībām uz informāciju var būt daži izņēmumi. Šādi ierobežojumi tomēr būtu jāpieļauj tiesību aktā, un tiem vajadzētu būt nepieciešamiem un samērīgiem, lai novērstu, ka tiek traucētas oficiālas vai juridiskas pārbaudes, izmeklēšana vai procedūras, lai novērstu, ka tiek ietekmēta noziedzīgu nodarījumu novēršana, izmeklēšana atklāšana vai saukšana pie atbildības par tiem vai kriminālsodu izpilde, lai pasargātu sabiedrisko drošību vai valsts drošību vai lai pasargātu citu personu tiesības un brīvības, ja vien šāds daļējs vai pilnīgs ierobežojums ir nepieciešams un samērīgs pasākums demokrātiskā sabiedrībā, pienācīgi ņemot vērā attiecīgās fiziskās personas pamattiesības un leģitīmās intereses. Šādi ierobežojumi būtu arī jāapsver un jānovērtē, ņemot vērā iespēju iesniegt sūdzību uzraudzības iestādē vai saņemt tiesisku aizsardzību. Jebkurā gadījumā jebkādam iespējamam ierobežojumam vajadzētu būt īslaicīgam un nevis vispārējam, un tajā būtu jāietver nosacījumi, aizsardzības pasākumi un ierobežojumi līdzīgi tiem, kas prasīti Hartā un ECT, kā tas interpretēts attiecīgi EST un ECT judikatūrā, un jo īpaši šo tiesību un brīvību būtības ievērošana.

j) Tiesības piekļūt, tiesības uz labošanu un dzēšanu (14. un 16. pants)

51. Datu subjektam vajadzētu būt tiesībām saņemt apstiprinājumu par to, vai tiek veikta uz viņu attiecināmu datu apstrāde, un, ja tas tā ir, viņam/viņai vajadzētu nodrošināt piekļuvi saviem datiem. Šīm tiesībām būtu jāietver vismaz noteikta informācija par apstrādi, piemēram, apstrādes nolūks un juridiskais pamats, tiesības iesniegt sūdzību uzraudzības iestādē vai attiecīgās personas datu kategorijas[49]. Tas ir īpaši svarīgi, ja pārredzamība tiek panākta ar vispārēju paziņojumu (piem., informācija iestādes tīmekļvietnē).

52. Datu subjektam vajadzētu būt tiesībām panākt savu datu labošanu noteiktu iemeslu dēļ, piemēram, ja tiek pierādīts, ka tie ir neprecīzi vai nepilnīgi. Datu subjektam vajadzētu būt arī tiesībām uz savu datu dzēšanu, ja, piemēram, to apstrāde vairs nav nepieciešama vai ir nelikumīga.

53. Šo tiesību īstenošana datu subjektam nedrīkst būt pārmērīgi apgrūtinoša.

k) Datu subjektu tiesību ierobežojumi

54. Varētu pastāvēt šo tiesību iespējami ierobežojumi, lai novērstu, ka tiek traucētas oficiālas vai juridiskas pārbaudes, izmeklēšana vai procedūras, lai novērstu, ka tiek ietekmēta noziedzīgu nodarījumu novēršana, izmeklēšana atklāšana vai saukšana pie atbildības par tiem vai kriminālsodu izpilde, lai pasargātu sabiedrisko drošību vai valsts drošību vai lai pasargātu citu personu tiesības un brīvības, ja vien šāds daļējs vai pilnīgs ierobežojums ir nepieciešams un samērīgs pasākums demokrātiskā sabiedrībā, pienācīgi ņemot vērā attiecīgās fiziskās personas pamattiesības un leģitīmās intereses. Šādi ierobežojumi būtu arī jāapsver un jānovērtē, ņemot vērā iespēju iesniegt sūdzību uzraudzības iestādē vai saņemt tiesisku aizsardzību.

l) Tālākas nosūtīšanas ierobežojumi (35. pants, 64. un 65. apsvērums)

[48] Gan materiālās tiesības (piekļuves tiesības, tiesības veikt labojumus utt.), gan tiesības uz atlīdzību.
[49] TAD 14. pants.

55. Sākotnējā saņēmēja veikta personas datu tālāka nosūtīšana uz citu trešo valsti vai starptautisku organizāciju nedrīkst apdraudēt fizisko personu, kuru dati tiek nosūtīti, Savienībā garantēto aizsardzības līmeni. Tādēļ šāda datu nosūtīšana būtu pieļaujama tikai tad, ja tiek garantēta Savienības tiesībās piedāvātā aizsardzības līmeņa turpinātība[50]. Jo īpaši nākamajam saņēmējam (proti, nosūtīšanas saņēmējam) vajadzētu būt kompetentajai iestādei tiesībaizsardzības nolūkos[51], un šāda datu tālāka nosūtīšana var notikt tikai ierobežotiem un konkrētiem mērķiem, ciktāl pastāv šādas apstrādes juridisks pamats.

56. Ir jāņem vērā arī tas, vai eksistē mehānisms attiecīgās dalībvalstu kompetentās iestādes informēšanai un tam, lai saņemtu šīs iestādes atļauju šādai tālākai datu nosūtīšanai. Sākotnējam no ES nosūtīto datu saņēmējam vajadzētu būt atbildīgam par to, ka attiecīgā dalībvalsts kompetentā iestāde ir atļāvusi tālāku nosūtīšanu[52] un ka gadījumos, ja nav pieņemts lēmums par aizsardzības līmeņa pietiekamību attiecībā uz trešo valsti, uz kuru dati tiks nosūtīti, ir paredzēti atbilstoši aizsardzības pasākumi datu tālākai nosūtīšanai[53], un būtu jāspēj to pierādīt.

m) Pārskatatbildības princips (4. panta 4. punkts)

57. Pārzinim vajadzētu būt atbildīgam par atbilstību TAD 4. pantā noteiktajiem datu aizsardzības principiem un vajadzētu spēt to pierādīt.

[50] Sk. arī Atzinumu 1/15.
[51] Sk. 33. zemsvītras piezīmi.
[52] Šajā kontekstā būtu jāņem vērā pienākums vai apņemšanās ieviest attiecīgus apstrādes kodus, kurus noteikušas nosūtītāju dalībvalstu iestādes.
[53] Iepriekš minētās prasības neskar īpašos nosacījumus attiecībā uz tālāku nosūtīšanu uz valsti ar pietiekamu aizsardzības līmeni, kā izklāstīts TAD (35. panta 1. punkta c) un e) apakšpunkts).

B. Piemēri papildu principiem, kurus piemēro konkrētiem apstrādes veidiem

a) Īpašās datu kategorijas (10. pants un 37. apsvērums)

58. Ja tiek skartas "īpašas datu kategorijas"[54], būtu jāparedz konkrēti aizsardzības pasākumi, kas vērsti uz konkrētiem iesaistītajiem riskiem[55]. Šīm kategorijām būtu jāatspoguļo TAD 10. pantā noteiktās kategorijas. Tāpēc īpašu datu kategoriju apstrādei būtu jāpiemēro īpaši aizsardzības pasākumi un tā būtu pieļaujama tikai tad, ja tas ir absolūti nepieciešams noteiktos apstākļos, piemēram, lai aizsargātu personas vitālās intereses.

b) Automatizēta lēmumu pieņemšana un profilēšana (11. pants un 38. apsvērums)

59. Lēmumus, kuru pamatā ir tikai automatizēta apstrāde (automatizēta individuālu lēmumu pieņemšana), tostarp profilēšana, kas rada nelabvēlīgas juridiskas sekas vai būtiski ietekmē datu subjektu, drīkstētu īstenot tikai ar konkrētiem nosacījumiem, kas noteikti trešās valsts tiesiskajā regulējumā[56].

60. Eiropas Savienības sistēmā šādi nosacījumi varētu būt, piemēram, īpašas informācijas sniegšana datu subjektam un tiesības panākt cilvēka iejaukšanos no pārziņa puses, jo īpaši paust savu viedokli, saņemt paskaidrojumu par lēmumu, kas pieņemts pēc šādas izvērtēšanas, un apstrīdēt lēmumu.

61. Trešās valsts tiesību aktos jebkurā gadījumā būtu jāparedz nepieciešamie pasākumi datu subjekta tiesību un brīvību aizsardzībai. Šajā sakarā būtu jāņem vērā arī tas, vai eksistē mehānisms attiecīgās dalībvalstu kompetentās iestādes informēšanai par šādu turpmāku datu apstrādi, piemēram, par nosūtīto datu izmantošanu liela mēroga profilēšanai.

c) Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma (20. pants)

62. Novērtējot pietiekamību, uzmanība būtu jāpievērš pārziņu pienākumam pieņemt iekšējo politiku un īstenot pasākumus, ar kuriem ievēro integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma principus, ņemot vērā tehnikas līmeni, ieviešanas izmaksas un apstrādes raksturu, tvērumu, kontekstu un nolūku, kā arī apstrādes radīto atšķirīgo risku iespējamību un nopietnību attiecībā uz fizisko personu tiesībām un brīvībām gan apstrādes līdzekļu noteikšanas laikā, gan pašas apstrādes laikā, pieņemt atbilstošus tehniskus un organizatoriskus pasākumus, piemēram, pseidonimizāciju, kas paredzēti, lai efektīvi ieviestu datu aizsardzības principus, piemēram, datu minimizēšanu, un integrētu apstrādē nepieciešamos aizsardzības pasākumus.

[54] Šādas īpašās kategorijas TAD 37. apsvērumā tiek sauktas arī par "sensitīviem datiem".
[55] Šādi papildu aizsardzības pasākumi var būt, piem., īpaši drošības pasākumi; ierobežotas piekļuves tiesības personālam; turpmākas apstrādes, automatizētas lēmumu pieņemšanas, kopīgošanas vai tālākas nosūtīšanas ierobežojumi.
[56] Atzinums 1/15, 173. punkts.

C. Procesuālie un izpildes mehānismi

63. Kaut arī līdzekļi, kādus trešā valsts izmanto, lai nodrošinātu pietiekamu aizsardzības līmeni, var atšķirties no tiem, kas tiek izmantoti Eiropas Savienībā[57], Eiropas sistēmai atbilstošu sistēmu raksturo šādi elementi.

a) Kompetenta neatkarīga uzraudzības iestāde (36. panta 2. punkta b) apakšpunkts un 3. punkts; 67. apsvērums)

64. Vajadzētu būt vienai vai vairākām neatkarīgām uzraudzības iestādēm, kurām ir pienākums nodrošināt un panākt atbilstību trešās valsts datu aizsardzības un privātuma noteikumiem. Uzraudzības iestāde darbojas pilnīgi neatkarīgi un objektīvi, pildot savus pienākumus un īstenojot savas pilnvaras, un, to darot, tā neprasa un nepieņem norādījumus. Šajā kontekstā uzraudzības iestādei vajadzētu būt atbilstošām izpildes panākšanas pilnvarām, lai efektīvi nodrošinātu datu aizsardzības tiesību ievērošanu, kā arī veicinātu informētību. Jāņem vērā arī uzraudzības iestādes personāls un budžets. Uzraudzības iestāde pēc savas iniciatīvas var arī veikt izmeklēšanu. Tai vajadzētu noteikt arī uzdevumu palīdzēt un konsultēt datu subjektus par viņu tiesību īstenošanu (sk. arī tālāk c) punktu). Lēmumos par aizsardzības līmeņa pietiekamību attiecīgā gadījumā būtu jāidentificē šī uzraudzības iestāde vai iestādes un sadarbības mehānismi ar dalībvalstu uzraudzības iestādēm datu aizsardzības noteikumu atbilstības panākšanai.

b) Datu aizsardzības noteikumu efektīva īstenošana

65. Trešās valsts sistēmai būtu jānodrošina augsts informētības līmenis datu pārziņu vidū un to personu vidū, kuras apstrādā personas datus viņu vārdā, attiecībā uz to pienākumiem, uzdevumiem un atbildību, kā arī datu subjektu vidū attiecībā uz viņu tiesībām un to īstenošanas līdzekļiem. Svarīga loma noteikumu ievērošanas nodrošināšanā var būt gan iedarbīgām un atturošām sankcijām, gan arī iestāžu, revidentu vai neatkarīgu datu aizsardzības amatpersonu veiktu tiešo pārbaužu sistēmām.

66. Trešās valsts datu aizsardzības sistēmā būtu jāuzliek par pienākumu datu pārziņiem vai personām, kuras apstrādā personas datus viņu vārdā, to ievērot un spēt uzskatāmi parādīt šādu atbilstību jo īpaši kompetentajai uzraudzības iestādei. Šādiem pasākumiem būtu jāietver datu apstrādes darbību uzskaites vai žurnālu ierakstu saglabāšana atbilstošā laika periodā. Tie var arī ietvert, piemēram, datu aizsardzības ietekmes novērtējumus, datu aizsardzības speciālista iecelšanu vai integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma.

c) Datu aizsardzības sistēmai ir jāatvieglo datu subjektu tiesību īstenošana (TAD 12., 17. un 46. pants)

67. Trešās valsts datu aizsardzības sistēmā datu pārziņiem būtu jānosaka pienākums atvieglot to datu subjekta tiesību īstenošanu, kas minētas iepriekš A iedaļas j) punktā, un jāparedz, ka tās uzraudzības iestāde pēc pieprasījuma informē jebkuru datu subjektu par viņa tiesību īstenošanu[58].

d) Datu aizsardzības sistēmai ir jānodrošina atbilstoši tiesiskās aizsardzības mehānismi

68. Lai gan pašlaik nav judikatūras attiecībā uz trešās valsts tiesību sistēmas pietiekamību saskaņā ar TAD, EST ir interpretējusi pamattiesības uz efektīvu tiesisko aizsardzību, kā noteikts Hartas

[57] *Schrems I*, 74. punkts.
[58] Datu subjektu tiesību īstenošana var būt tieša vai netieša.

47. pantā. Hartas 47. panta pirmajā daļā ir prasīts, lai ikvienai personai, kuras tiesības un brīvības, kas garantētas Savienības tiesībās, tikušas pārkāptas, būtu tiesības uz efektīvu tiesību aizsardzību tiesā[59], ievērojot nosacījumus, kuri paredzēti šajā pantā.

69. Saskaņā ar pastāvīgo EST judikatūru efektīvas pārskatīšanas tiesā ar mērķi nodrošināt atbilstību ES tiesību aktiem esamība pati par sevi ir raksturīga tiesiskuma pastāvēšanai. Tādējādi tiesību aktos, kuros nav paredzēta indivīda iespēja izmantot tiesiskās aizsardzības līdzekļus, lai piekļūtu uz viņu attiecināmiem personas datiem vai lai panāku šādu datu labošanu vai dzēšanu, netiek ievērota pamattiesību uz efektīvu tiesību aizsardzību būtība, kā noteikts Hartas 47. pantā[60].

70. Personai būtu jāspēj izmantot tiesiskās aizsardzības līdzekļus, lai īstenotu savas tiesības ātri un efektīvi, nepieprasot tai maksu, kas varētu atturēt personu no šo tiesību īstenošanas, kā arī lai nodrošinātu atbilstību.

71. Šim nolūkam ir jāievieš uzraudzības mehānismi, kas ļautu neatkarīgi izskatīt sūdzības un atļautu praksē identificēt un sodīt jebkādus tiesību uz datu aizsardzību un privātās dzīves neaizskaramību pārkāpumus.

72. Ja noteikumi netiek ievēroti, datu subjektam, kura personas dati tiek nosūtīti uz trešo valsti, būtu jānodrošina arī efektīva administratīvā un tiesiskā aizsardzība trešā valstī, tostarp tādu zaudējumu atlīdzināšana, kas radušies viņa/viņas personas datu nelikumīgas apstrādes rezultātā. Šis ir galvenais elements, kam jāietver neatkarīgas lietu izskatīšanas vai izšķiršanas sistēma, kura nodrošinātu kompensācijas izmaksāšanu un attiecīgos gadījumos sodu piespriešanu.

[59] EST uzskata, ka efektīvu tiesību aizsardzību var nodrošināt ne tikai tiesa, bet arī struktūra, kas piedāvā garantijas, kuras būtībā ir līdzvērtīgas tām, kas prasītas Hartas 47. pantā (sk. spriedumu *Schrems II*, 197. punkts). Tas jo īpaši varētu attiekties uz starptautiskām organizācijām.
[60] *Schrems II*, 187. un 194. punkts un tajos citētā judikatūra.