
# Ieteikumi 02/2020 attiecībā uz Eiropas būtiskajām garantijām uzraudzības pasākumiem

**Pieņemti 2020. gada 10. novembrī**

# Satura rādītājs

**Eiropas Datu aizsardzības kolēģija,**

ņemot vērā 70. panta 1. punkta e) apakšpunktu Eiropas Parlamenta un Padomes Regulā (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (turpmāk — "VDAR"),[1]

ņemot vērā EEZ līgumu un jo īpaši tā XI pielikumu un 37. protokolu, kas grozīts ar EEZ Apvienotās komitejas 2018. gada 6. jūlija Lēmumu Nr. 154/2018[2],

ņemot vērā tās Reglamenta 12. un 22. pantu,

ņemot vērā 29. panta darba grupas darba dokumentu par pamatojumu, saskaņā ar kuru aizskar pamattiesības uz privātumu un datu aizsardzību, izmantojot novērošanas pasākumus personas datu nosūtīšanas laikā (Eiropas būtiskās garantijas, turpmāk — "*EEG*"), WP237,

**IR PIEŅĒMUSI ŠĀDUS IETEIKUMUS.**

# 1. IEVADS

1. Pēc sprieduma lietā *Schrems I* ES datu aizsardzības iestādes, kas piedalās 29. panta darba grupā, izmantoja judikatūru, lai identificētu Eiropas būtiskās garantijas, kuras jāievēro, lai nodrošinātu, ka ar uzraudzības palīdzību īstenota iejaukšanās tiesībās uz privāto dzīvi un personas datu aizsardzība, nosūtot personas datus, nepārsniedz to, kas nepieciešams un samērīgs demokrātiskā sabiedrībā.

2. EDAK vēlas uzsvērt, ka Eiropas būtisko garantiju pamatā ir Eiropas Savienības Tiesas (turpmāk — EST) judikatūra, kas saistīta ar ES Pamattiesību hartas (turpmāk — Harta) 7., 8., 47. un 52. pantu un, attiecīgā gadījumā, Eiropas Cilvēktiesību tiesas (turpmāk — ECT) judikatūra saistībā ar Eiropas Cilvēktiesību konvencijas (turpmāk — ECTK) 8. pantu, kurā apskatīti uzraudzības jautājumi ECTK dalībvalstīs.[3]

3. Šī dokumenta atjauninājums ir paredzēts, lai turpinātu attīstīt Eiropas būtiskās garantijas; sākotnēji tas tika izstrādāts, reaģējot uz spriedumu lietā *Schrems I*[4], atspoguļojot EST (un ECT) sniegtos skaidrojumus kopš tā pirmreizējās publicēšanas, jo īpaši Tiesas nozīmīgā sprieduma lietā *Schrems II.*[5]

[1] Šajā dokumentā nav aplūkotas nosūtīšanas vai turpmākas apmaiņas situācijas, uz kurām attiecas Tiesībaizsardzības direktīvas (Direktīva (ES) 2016/680) darbības joma.

[2] Šajā dokumentā atsauces uz "dalībvalstīm" būtu jāsaprot kā atsauces uz "EEZ dalībvalstīm".

[3] Šajos ieteikumos termins "pamattiesības" ir atvasināts no ES Pamattiesību hartas. Tomēr tas izmantots arī, lai aptvertu "cilvēktiesības" Eiropas Cilvēktiesību konvencijas izpratnē.

[4] EST spriedums (2015. gada 6. oktobris), *Maximillian Schrems / Datu aizsardzības komisija*, lieta C-362/14, EU:C:2015:650 (turpmāk — *Schrems I).*

[5] EST spriedums (2020. gada 16. jūlijs), *Datu aizsardzības komisija / Facebook Ireland Ltd, Maximillian Schrems*, lieta C-311/18, ECLI:EU:C:2020:559 (turpmāk — *Schrems II).*

4. Savā spriedumā lietā *Schrems II* EST paziņoja, ka, pārbaudot Komisijas Lēmumu 2010/87/ES par līguma standartklauzulām personas datu nosūtīšanai trešās valstīs reģistrētiem apstrādātājiem, ņemot vērā Hartas 7., 8. un 47. pantu, nav konstatēts nekas, kas varētu ietekmēt šī lēmuma spēkā esību, taču tā atcēla lēmumu par privātuma vairogu. EST uzskatīja, ka lēmums par privātuma vairogu nav savietojams ar VDAR 45. panta 1. punktu, ņemot vērā Hartas 7., 8. un 47. pantu. Tādējādi spriedums var kalpot par piemēru gadījumos, kad uzraudzības pasākumi trešā valstī (šajā gadījumā ASV saskaņā ar *FISA* 702. pantu un Rīkojumu 12333) nav pietiekami ierobežoti un datu subjektiem nav pieejami efektīvi tiesiskās aizsardzības līdzekļi, lai viņi varētu īstenot savas tiesības atbilstīgi ES tiesību aktiem, ļaujot uzskatīt aizsardzības līmeni trešā valstī par "būtībā līdzvērtīgu" tam, kas garantēts Eiropas Savienībā VDAR 45. panta 1. punkta nozīmē.

5. Privātuma vairoga pasludināšanas par spēkā neesošu iemesli ietekmē arī citus nosūtīšanas rīkus.[6] Lai arī Tiesa interpretēja VDAR 46. panta 1. punktu saistībā ar līguma standartklauzulu (turpmāk — *SCC*) spēkā esību, tās interpretācija piemērojama jebkurai nosūtīšanai uz trešām valstīm, atsaucoties uz jebkuru no VDAR 46. pantā minētajiem rīkiem.[7]

6. Galu galā EST vērtē, vai iejaukšanās pamattiesībās ir attaisnojama. Tomēr, ja šāda sprieduma nav un piemērojot pastāvīgo judikatūru, datu aizsardzības iestādēm ir pienākums izvērtēt atsevišķus gadījumus *ex officio* vai uz sūdzības pamata un vai nu nodot lietu izskatīšanai valsts tiesā, ja tām ir aizdomas, ka nosūtīšana neatbilst 45. pantam gadījumos, kad ir pieņemts lēmums par atbilstību, vai apturēt vai aizliegt nosūtīšanu, ja tās uzskata, ka VDAR 46. panta prasības nav iespējams ievērot un ES tiesību aktos prasīto nosūtīto datu aizsardzību nevar nodrošināt ar citiem līdzekļiem.

7. Atjaunināto Eiropas būtisko garantiju mērķis ir sniegt elementus pārbaudei, vai uzraudzības pasākumus, ar ko trešā valstī esošām valsts iestādēm, kas ir valsts drošības aģentūras vai tiesībaizsardzības iestādes, ļauj piekļūt personas datiem, var uzskatīt par attaisnojamu iejaukšanos.

8. Patiešām, Eiropas būtiskās garantijas ietilpst novērtējumā, kas veicams, lai noteiktu, vai trešā valstī ir nodrošināts aizsardzības līmenis, kurš būtībā ir līdzvērtīgs ES garantētajam, taču pašas par sevi tās netiecas definēt visus elementus, kas nepieciešami, lai uzskatītu, ka trešā valstī ir nodrošināts šāds aizsardzības līmenis saskaņā ar VDAR 45. pantu. Tāpat to mērķis nav patstāvīgi definēt visus elementus, kas varētu būt jāņem vērā, novērtējot, vai trešās valsts tiesiskais režīms traucē datu nosūtītājam un datu saņēmējam nodrošināt atbilstošus aizsardzības pasākumus saskaņā ar VDAR 46. pantu.

9. Tāpēc šajā dokumentā sniegtie elementi būtu jāuzskata par būtiskām garantijām, kuras ir jānosaka trešā valstī, novērtējot iejaukšanos tiesībās uz privātumu un datu aizsardzību saistībā ar trešās valsts uzraudzības pasākumiem, nevis elementu saraksts, ko izmantot, lai pierādītu, ka trešās valsts tiesiskais regulējums kopumā nodrošina būtībā līdzvērtīgu aizsardzības līmeni.

10. Līguma par Eiropas Savienību 6. panta 3. punktā noteikts, ka ECTK nostiprinātās pamattiesības ir ES tiesību vispārēji principi. Tomēr, kā EST atgādina savā judikatūrā, konvencija, kamēr Eiropas Savienība nav tai pievienojusies, nav ES tiesību aktos formāli integrēts juridisks instruments.[8] Tādējādi VDAR 46. panta 1. punktā prasītais pamattiesību aizsardzības līmenis ir jānosaka, pamatojoties uz šīs regulas

[6] Skatīt 105. punktu *Schrems II.*
[7] Skatīt 92. punktu *Schrems II.*
[8] Skatīt 98. punktu *Schrems II.*

noteikumiem, ko lasa, ņemot vērā Hartā nostiprinātās pamattiesības. Tas nozīmē, ka saskaņā ar Hartas 52. panta 3. punktu tajā ietvertajām tiesībām, kas atbilst ECTK garantētajām tiesībām, ir tāda pati nozīme un piemērošanas joma kā konvencijā noteiktajām, un līdz ar to, kā atgādināja EST, jāņem vērā ECT judikatūra attiecībā uz tiesībām, kas paredzētas arī ES Pamattiesību hartā, kā minimālais aizsardzības slieksnis attiecīgo Hartā paredzēto tiesību interpretācijai.[9] Tomēr saskaņā ar Hartas 52. panta 3. punkta pēdējo teikumu "[š]is noteikums neliedz Savienības tiesībās paredzēt plašāku aizsardzību".

11. Tāpēc būtisko garantiju būtība arī turpmāk daļēji balstīsies ECT judikatūrā, ciktāl Hartā, kā to interpretē EST, nav paredzēts augstāks aizsardzības līmenis, ar ko nosaka atšķirīgas prasības nekā ECT judikatūrā.

12. Šajā dokumentā ir izskaidrots četru Eiropas būtisko garantiju pamatojums un sīkāka informācija.

## 2. IEJAUKŠANĀS PAMATTIESĪBĀS

13. Pamattiesības uz privāto un ģimenes dzīvi, tostarp saziņu, un personas datu aizsardzības ievērošanu ir noteiktas Hartas 7. un 8. pantā, un tās attiecas uz visām personām. Turklāt 8. pantā ir izklāstīti nosacījumi, lai personas datu apstrāde būtu likumīga, un tiek atzītas piekļuves un labošanas tiesības, kā arī noteikts, ka šie nosacījumi ir pakļauti neatkarīgas iestādes kontrolei.

14. "(D)arbība, kas ietver personas datu nosūtīšanu no dalībvalsts uz trešo valsti kā tāda ir personas datu apstrāde"[10]. Tādējādi Hartas 7. un 8. pants attiecas uz šo konkrēto darbību, un tajos noteiktā aizsardzība attiecas uz nosūtītajiem datiem, tāpēc datu subjektiem, kuru personas dati tiek nosūtīti uz trešo valsti, ir jānodrošina tāds aizsardzības līmenis, kas būtībā ir līdzvērtīgs Eiropas Savienībā garantētajam.[11]

15. EST uzskata, ka gadījumos, kad tiek skartas Hartas 7. pantā noteiktās pamattiesības uz privātās dzīves neaizskaramību, apstrādājot indivīda personas datus, tiek skartas arī tiesības uz datu aizsardzību, jo šāda apstrāde ietilpst Hartas 8. panta tvērumā, un attiecīgi tai obligāti jāatbilst šajā pantā noteiktajai datu aizsardzības prasībai.[12]

16. Tādēļ attiecībā uz iespējamo iejaukšanos pamattiesībās saskaņā ar ES tiesību aktiem elektronisko sakaru pakalpojumu sniedzējiem uzliktais pienākums (…) saglabāt plūsmas datus, lai vajadzības gadījumā padarītu tos pieejamus kompetentajām valsts iestādēm, rada jautājumus par saderību ar Hartas 7. un 8. pantu[13]. Tas pats attiecas uz citiem datu apstrādes veidiem, piemēram, datu nosūtīšanu personām, kuras nav lietotāji, vai piekļuvi šiem datiem nolūkā tos izmantot[14], kas tādējādi rada iejaukšanos minētajās pamattiesībās. Turklāt saskaņā ar pastāvīgo judikatūru valsts iestādes piekļuve datiem ir papildu iejaukšanās.[15]

---

[9] Skatīt 124. punktu apvienotajās lietās C-511/18, C-512/18 un C-520/18, *La Quadrature du Net u. c*. (turpmāk — *La Quadrature du Net u. c*).

[10] EST, *Schrems II*, 83. punkts.

[11] EST, *Schrems II*, 96. punkts.

[12] EST, *Schrems II*, 170.–171. punkts.

[13] EST, lieta C-623/17, *Privacy International* (turpmāk — *Privacy International*), 60. punkts.

[14] EST, *Privacy International*, 61. punkts.

[15] ECT, *Leander*, 48. punkts; ECT, *Rotaru*, 46. punkts; EST, *Digital Rights Ireland*, 35. punkts.

17. Lai konstatētu iejaukšanos, nav svarīgi, "vai attiecīgajai informācijai par privāto dzīvi ir vai nav sensitīvs raksturs un vai ieinteresētajām personām ir vai nav radītas iespējamas neērtības šīs iejaukšanās dēļ".[16] EST arī uzsvēra, ka nav nozīmes tam, vai saglabātie dati tikuši izmantoti vēlāk.[17]

18. Tomēr Hartas 7. un 8. pantā ietvertās tiesības nav absolūtas, bet tās ir jāapskata saistībā ar to funkciju sabiedrībā.[18]

19. Harta paredz nepieciešamības un proporcionalitātes pārbaudi, lai noteiktu ierobežojumus tās aizsargātajām tiesībām. Hartas 52. panta 1. punktā precizēta iespējamo 7. un 8. panta ierobežojumu piemērošanas joma, nosakot, ka "visiem šajā Hartā atzīto tiesību un brīvību izmantošanas ierobežojumiem ir jābūt noteiktiem tiesību aktos, un tajos jārespektē šo tiesību un brīvību būtība. Ievērojot proporcionalitātes principu, ierobežojumus drīkst uzlikt tikai tad, ja tie ir nepieciešami un patiešām atbilst vispārējas nozīmes mērķiem, ko atzinusi Savienība, vai vajadzībai aizsargāt citu personu tiesības un brīvības".

20. EST atkārtoti ir uzsvērusi, ka ES tiesību aktos, kas skar Hartas 7. un 8. pantā garantēto pamattiesību iejaukšanos, "ir jāparedz skaidri un precīzi noteikumi, kas reglamentē attiecīgā pasākuma tvērumu un piemērošanu un paredz minimālās prasības, lai tā rezultātā personām, kuru personas dati tikuši pārsūtīti, būtu pietiekamas garantijas, kas ļautu šos datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku", jo īpaši, ja personas dati tiek apstrādāti automātiski un "pastāv ievērojams nelikumīgas piekļuves risks šiem datiem".[19]

21. EST uzskata, ka tiesību uz privātumu aizsardzība prasa, lai atkāpes no tiesībām uz datu aizsardzību un to ierobežojumi tiktu "īstenoti absolūti nepieciešamā ietvaros". Turklāt vispārējas nozīmes mērķis ir jāsaskaņo ar pamattiesībām, kuras skar šis pasākums, "pienācīgi līdzsvarojot" mērķi ar attiecīgajām tiesībām.[20]

22. Līdz ar to valsts iestāžu piekļuve personas datiem, to saglabāšana un turpmāka izmantošana uzraudzības pasākumu ietvaros nedrīkst pārsniegt noteikti nepieciešamā robežas, vērtējumā ņemot vērā Hartu, pretējā gadījumā tā "nevar tikt uzskatīta par pamatotu demokrātiskā sabiedrībā".[21]

23. Četrās Eiropas būtiskajās garantijās, kas sīkāk apskatītas nākamajā nodaļā, ir paredzēts precizēt, kā novērtēt iejaukšanās līmeni pamattiesībās uz privātumu un datu aizsardzību saistībā ar uzraudzības pasākumiem, ko veic valsts iestādes trešā valstī, nosūtot personas datus, un kādas juridiskās prasības attiecīgi jāpiemēro, novērtējot, vai šāda iejaukšanās būtu pieņemama saskaņā ar Hartu.

[16] EST, *Schrems II,* 171. punkts, tostarp minētā judikatūra.
[17] EST, *Schrems II,* 171. punkts, tostarp minētā judikatūra.
[18] EST, *Privacy International*, 63. punkts.
[19] EST, *Privacy International,* 68. punkts un tajā minētā judikatūra.
[20] EST, *Privacy International,* 68. punkts un tajā minētā judikatūra.
[21] EST, *Privacy International*, 81. punkts.

# 3. EIROPAS BŪTISKĀS GARANTIJAS

24. Pēc judikatūras analīzes EDAK uzskata, ka piemērojamās juridiskās prasības Hartā atzīto datu aizsardzības un privātuma tiesību ierobežojumu pamatojumam var apkopot četrās Eiropas būtiskajās garantijās:

A. apstrādei jābūt balstītai skaidros, precīzos un pieejamos noteikumos;
B. nepieciešamība un proporcionalitāte attiecībā uz izvirzītajiem likumīgajiem mērķiem ir jāpierāda;
C. jāpastāv neatkarīgam uzraudzības mehānismam;
D. indivīdam jābūt pieejamiem efektīviem līdzekļiem.

25. Garantiju pamatā ir pamattiesības uz privātumu un datu aizsardzību, kas attiecas uz visiem, neatkarīgi no viņu valstspiederības.

## A garantija — apstrādei jābūt balstītai skaidros, precīzos un pieejamos noteikumos

26. Saskaņā ar Hartas 8. panta 2. punktu personas dati cita starpā jāapstrādā "noteiktiem mērķiem, ar attiecīgās personas piekrišanu vai ar citu likumīgu pamatojumu, kas paredzēts tiesību aktos",[22] kā EST atgādināja spriedumā lietā *Schrems II.* Turklāt saskaņā ar Hartas 52. panta 1. punktu visiem Hartā atzīto tiesību un brīvību izmantošanas ierobežojumiem ES ir jābūt "noteiktiem tiesību aktos". Tādējādi attaisnojama iejaukšanās jāīsteno saskaņā ar tiesību aktiem.

27. Šajā juridiskajā pamatā būtu jāparedz skaidri un precīzi noteikumi, kas reglamentē attiecīgā pasākuma darbības jomu un piemērošanu un nosaka minimālos aizsardzības pasākumus.[23] Turklāt Tiesa atgādināja, ka "tiesiskajam regulējumam ir jābūt juridiski saistošam valsts tiesībās".[24] Šajā sakarā EST precizēja, ka piemērojamo trešo valstu tiesību aktu novērtējumā galvenā uzmanība būtu jāpievērš tam, vai personas uz to var atsaukties un uz to var paļauties tiesā.[25] Tādēļ Tiesa norāda, ka attiecībā uz datu subjektiem piešķirtajām tiesībām var iesniegt prasību; ja indivīdiem netiek nodrošinātas īstenojamas tiesības pret valsts iestādēm, piešķirto aizsardzības līmeni nevar uzskatīt par būtībā līdzvērtīgu no Hartas izrietošajam, pretēji VDAR 45. panta 2. punkta a) apakšpunkta prasībai.[26]

28. Turklāt Tiesa uzsvēra, ka piemērojamajos tiesību aktos ir jānorāda, kādos apstākļos un ar kādiem nosacījumiem var tikt pieņemts pasākums, ar ko nodrošina šādu datu apstrādi[27] (šīs garantijas saistību ar nepieciešamības un proporcionalitātes principu skatīt tālāk B garantijas sadaļā).

[22] Skatīt 173. punktu *Schrems II.*

[23] Skatīt 175. un 180. punktu *Schrems II*, un 2017. gada 26. jūlija Atzinumu 1/15 (ES un Kanādas PDR nolīgums), 139. punkts, un tajā minēto judikatūru.

[24] Skatīt 68. punktu *Privacy International*; jāprecizē arī, ka sprieduma franču valodas versijā Tiesa lieto vārdu "*réglementation*", kam ir plašāka nozīme nekā tikai Parlamenta izdotie akti.

[25] Skatīt 181. punktu *Schrems II*; šajā punktā EST atsaucas uz ASV Prezidenta politikas direktīvu Nr. 28.

[26] Skatīt 181. punktu *Schrems II.*

[27] Skatīt 68. punktu *Privacy International* saistībā ar dalībvalstu tiesību aktiem.

29. Turklāt EST ir arī norādījusi, ka "prasība, saskaņā ar kuru jebkuram pamattiesību izmantošanas ierobežojumam ir jābūt noteiktam tiesību aktos, nozīmē, ka pašā juridiskajā pamatā ir jānosaka attiecīgo tiesību īstenošanas ierobežojuma apjoms".[28]

30. Visbeidzot, Eiropas Cilvēktiesību tiesa "neuzskata, ka ir pamats piemērot dažādus principus attiecībā uz noteikumu, kas reglamentē individuālās saziņas pārtveršanu, pieejamību un skaidrību, no vienas puses, un vispārīgākām uzraudzības programmām".[29] Arī ECT ir skaidrojusi, ka juridiskajā pamatā būtu jāiekļauj vismaz to cilvēku kategoriju definīcija, kurām var piemērot uzraudzību, pasākuma ilguma ierobežojums, procedūra, kas jāievēro, pārbaudot, izmantojot un uzglabājot iegūtos datus, un piesardzības pasākumi, kas jāievēro, paziņojot datus citām pusēm.[30]

31. Visbeidzot, iejaukšanās procesam jābūt paredzamam attiecībā uz tā ietekmi uz indivīdu, lai viņam/viņai nodrošinātu pietiekamu un efektīvu aizsardzību pret patvaļīgu iejaukšanos un ļaunprātīgas izmantošanas risku. Rezultātā apstrādei jābalstās precīzā, skaidrā, taču arī pieejamā (t. i., publiskā) juridiskajā pamatā.[31] ECT attiecībā uz šo jautājumu lietā *Zakharov* atgādināja, ka "atsauce uz "paredzamību" saziņas pārtveršanas kontekstā nevar būt tāda pati kā daudzās citās jomās". Tajā precizēts, ka saistībā ar slepeniem uzraudzības pasākumiem, piemēram, saziņas pārtveršanu, "paredzamība nenozīmē, ka indivīdam jāspēj paredzēt, kad iestādes varētu pārtvert viņa saziņu, lai viņš varētu attiecīgi pielāgot savu rīcību". Tomēr, ņemot vērā, ka šāda veida situācijās ir acīmredzami patvaļas riski, "ir svarīgi, lai būtu skaidri, sīki izstrādāti noteikumi par tālruņa sarunu pārtveršanu, jo īpaši tāpēc, ka lietošanai pieejamā tehnoloģija nepārtraukti kļūst sarežģītāka. Vietējiem tiesību aktiem jābūt formulētiem pietiekami skaidri, lai sniegtu pilsoņiem pienācīgu norādi uz apstākļiem, kādos publiskās iestādes ir pilnvarotas izmantot šādus pasākumus".[32]

## B garantija — nepieciešamība un proporcionalitāte attiecībā uz izvirzītajiem likumīgajiem mērķiem ir jāpierāda

32. Saskaņā ar pirmo teikumu Hartas 52. panta 1. punktā visiem Hartā atzīto tiesību un brīvību izmantošanas ierobežojumos ir "jārespektē šo tiesību un brīvību būtība". Atbilstīgi Hartas 52. panta 1. punkta otrajam teikumam, ievērojot proporcionalitātes principu, šo tiesību un brīvību ierobežojumus drīkst uzlikt tikai tad, ja tie ir nepieciešami un patiešām atbilst vispārējas nozīmes mērķiem, ko atzinusi Savienība, vai vajadzībai aizsargāt citu personu tiesības un brīvības.[33]

33. Saistībā ar **proporcionalitātes principu** Tiesa attiecībā uz dalībvalstu tiesību aktiem nosprieda, ka jautājums par to, vai tiesību uz privātumu un datu aizsardzību ierobežojums var būt pamatots, ir jānovērtē, no vienas puses, mērot **iejaukšanās būtiskumu**, ko rada šāds ierobežojums,[34] un, no otras

[28] Skatīt 175. punktu *Schrems II* un tajā minēto judikatūru, kā arī 65. punktu *Privacy International*.

[29] ECT, *Liberty*, 63. punkts.

[30] ECT, *Weber and Saravia*, 95. punkts.

[31] ECT, *Malone*, 65., 66. punkts.

[32] ECT, *Zakharov*, 229. punkts.

[33] *Schrems II*, 174. punkts.

[34] Šajā saistībā Tiesa, piemēram, 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 (...) " (*La Quadrature du Net u. c.*, 187. punkts, tostarp minētā judikatūra).

puses, pārbaudot, vai **sabiedrības interešu mērķa**, ko sasniedz šis ierobežojums, nozīme ir samērīga attiecībā pret šo būtiskumu.[35]

34. Lietā *La Quadrature du net u. c.* var atzīmēt, ka EST saistībā ar dalībvalsts tiesību aktiem, nevis ar trešās valsts tiesību aktiem, nolēma, ka valsts drošības aizsardzības mērķis savas nozīmes dēļ var attaisnot pasākumus, ar ko paredz būtiskāku iejaukšanos pamattiesībās, nekā tādus, ko varētu pamatot ar citiem mērķiem, piemēram, noziedzības apkarošanu. Tomēr tā konstatēja, ka tas tā ir, ja ir pietiekami nopietns pamats uzskatīt, ka attiecīgā valsts saskaras ar nopietniem draudiem valsts drošībai, kuri ir patiesi un faktiski vai paredzami, un tie atbilst citām Hartas 52. panta 1. punktā noteiktajām prasībām.[36]

35. Šajā sakarā saskaņā ar pastāvīgo Tiesas judikatūru atkāpes no personas datu aizsardzības un to ierobežojumi jāpiemēro tikai tiktāl, ciktāl tas ir absolūti nepieciešams.[37] Lai izpildītu šo prasību, attiecīgajiem tiesību aktiem papildus skaidriem un precīziem noteikumiem, kas reglamentē attiecīgā pasākuma darbības jomu un piemērošanu, jāparedz minimālās prasības, lai tā rezultātā personām, kuru personas dati tikuši nosūtīti, būtu pietiekamas garantijas, kas ļautu šos datus efektīvi aizsargāt 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".[38]

36. Lietā *Schrems II* EST ir uzsvērusi, ka trešās valsts tiesību akti, kuros nav norādīti nekādi ierobežojumi attiecībā uz pilnvarām, ko piešķir, īstenojot uzraudzības programmas ārvalstu izlūkdatu vajadzībām, nevar nodrošināt aizsardzības līmeni, kas būtībā ir līdzvērtīgs Hartā garantētajam. Patiešām, saskaņā ar judikatūru juridiskajam pamatam, kas pieļauj iejaukšanos pamattiesībās, jānosaka attiecīgo tiesību izmantošanas ierobežojuma piemērošanas joma, lai izpildītu proporcionalitātes principa prasības.[39]

37. Attiecībā uz **nepieciešamības principu** EST ir skaidri norādījusi, ka tiesiskais regulējums, "saskaņā ar kuru vispārīgi tiek pieļauta visu to personu personas datu saglabāšana, kuru dati no Savienības ir pārsūtīti (...), nešķirojot, bez ierobežojumiem vai izņēmumiem saistībā ar mērķi, kam tie kalpo, vai neparedzot objektīvus kritērijus, kas valsts iestāžu piekļuvi datiem un to vēlāku izmantošanu ļauj ierobežot precīziem, strikti ierobežotiem un tādiem mērķiem, kas pamato gan piekļuvi šiem datiem, gan arī to izmantošanu", neatbilst šim principam[40]. Jo īpaši tiesību akti, kas atļauj valsts iestādēm vispārīgi

[35] *La Quadrature du Net u. c.*, 131. punkts.

[36] 136. un 137. punkts. Skatīt *Privacy International*; kā Tiesa norādīja, šādus draudus pēc to rakstura un īpašas nopietnības var nošķirt no vispārējā riska, ka radīsies pat nopietna spriedze vai traucējumi, kas ietekmē sabiedrības drošību. 75. punkts. Piemēram, lietā *La Quadrature du Net u. c.* Tiesa atzīmēja, ka automatizēta plūsmas un atrašanās vietas datu analīze, kas visaptveroši un nediferencēti attiecas uz to personu datiem, kuras izmanto elektronisko komunikāciju sistēmas, ir īpaši smaga iejaukšanās, lai šāds pasākums var atbilst samērīguma prasībai tikai situācijās, kad dalībvalsts saskaras ar nopietniem draudiem valsts drošībai, kas izrādās patiesi un faktiski vai paredzami, un ar nosacījumu, ka šīs glabāšanas ilgums ir ierobežots ar absolūti nepieciešamo (174.–177. punkts).

[37] EST, *Schrems II,* 176. punkts, tostarp minētā judikatūra.

[38] *Schrems II*, 175. punkts.

[39] *Schrems II*, 180. punkts.

[40] *Schrems I,* 93. punkts ar turpmākām atsaucēm. Skatīt tomēr šoreiz attiecībā uz dalībvalsts tiesību aktiem, nevis uz trešo valstu tiesību aktiem, *Privacy International*, 71. punkts, tostarp minēto judikatūru. Šajā gadījumā Tiesa paziņoja, ka dalībvalsts tiesību akti, kas pieprasa elektronisko sakaru pakalpojumu sniedzējiem atklāt plūsmas datus un atrašanās vietas datus drošības dienestiem un izlūkdienestiem visaptverošā un nediferencētā veidā,

piekļūt elektronisko komunikāciju saturam, uzskatāmi par tādiem, kas apdraud pašu Hartas 7. pantā garantēto pamattiesību uz privātās dzīves neaizskaramību būtību.[41]

38. Tomēr šoreiz, novērtējot dalībvalsts, nevis trešās valsts tiesību aktus, EST lietā *La Quadrature du Net u. c.* apgalvoja, ka "tiesiskajam regulējumam, kurā ir paredzēta personas datu saglabāšana, vienmēr ir jāatbilst objektīviem kritērijiem, kas veido saikni starp saglabājamajiem datiem un sasniedzamo mērķi".[42] Tajā pašā saistībā lietā *Privacy International* tā arī nosprieda, ka likumdevējam "ir jābalstās uz objektīviem kritērijiem, lai definētu apstākļus un nosacījumus, saskaņā ar kuriem kompetentajām valsts iestādēm ir jāpiešķir piekļuve aplūkotajiem datiem".[43]

## C garantija — neatkarīgs uzraudzības mehānisms

39. EDAK atgādina, ka iejaukšanās notiek ne tikai datu vākšanas laikā, bet arī brīdī, kad valsts iestāde piekļūst datiem to turpmākai apstrādei. ECT vairākas reizes ir norādījusi, ka jebkura iejaukšanās tiesībās uz privātumu un datu aizsardzību būtu jāpakļauj efektīvai, neatkarīgai un objektīvai uzraudzības sistēmai, ko nodrošina vai nu tiesnesis, vai cita neatkarīga struktūra[44] (piemēram, administratīva iestāde vai parlamentāra struktūra). Neatkarīgu uzraudzības pasākumu īstenošanas pārraudzību EST ņēma vērā arī spriedumā lietā *Schrems II*.[45]

40. ECT precizē, ka, lai gan iepriekšēja (tiesas) atļauja īstenot uzraudzības pasākumus ir svarīga aizsardzība pret patvaļīgu rīcību, ir jāņem vērā arī pārtveršanas sistēmas faktiskā darbība, tostarp varas izmantošanas pārraudzība, kā arī faktiskas ļaunprātīgas izmantošanas esība vai trūkums.[46] Lietā *Schrems II* EST ņēma vērā arī pārraudzības mehānisma, kas neattiecās uz atsevišķiem uzraudzības pasākumiem, uzraudzības lomas tvērumu.[47]

41. Attiecībā uz dalībvalstu tiesību aktiem EST identificēja vairākus pasākumus, kas atbilst ES tiesību aktiem, tikai tad, ja tos efektīvi pārbauda tiesa vai neatkarīga administratīva iestāde, kuras lēmums ir saistošs. Šādas pārbaudes mērķis ir pārbaudīt, vai pastāv situācija, kas attaisno pasākumu, un vai tiek

---

pārsniedz absolūti nepieciešamā robežas un nevar tikt uzskatīts par pamatotu demokrātiskā sabiedrībā, kā tas ir prasīts Direktīvā par privātumu un elektronisko saziņu, kas lasāma, ņemot vērā Hartu (81. punkts).

[41] *Schrems I*, 94. punkts.

[42] *La Quadrature du Net u. c.*, 133. punkts. Šajā kontekstā Tiesa apstiprināja, ka likumdošanas pasākumi, kas kā preventīvs pasākums paredz plūsmas un atrašanās vietas datu saglabāšanu visaptverošā un nediferencētā veidā, ir izslēgti no Direktīvas par privātumu un elektronisko saziņu, kas lasāma, ņemot vērā Hartu. Turpretim Tiesa sprieda, ka situācijās, kad valsts saskaras ar nopietniem draudiem valsts drošībai, kas izrādās patiesi un faktiski vai paredzami, likumdevējs var atļaut valsts drošības nodrošināšanai izmantot rīkojumu, kas pieprasa elektronisko sakaru pakalpojumu sniedzējiem saglabāt visaptverošā un nediferencētā veidā plūsmas un atrašanās vietas datus. Šādam pasākumam tomēr jāatbilst īpašiem nosacījumiem. Konkrēti, rīkojumu var dot tikai uz absolūti nepieciešamo laiku, tomēr šo termiņu var pagarināt, ja šāds apdraudējums saglabājas (168. punkts).

[43] *Privacy International,,* 78. punkts, tostarp minētā judikatūra. Lietā *Privacy International* attiecībā uz iestādes piekļuvi personas datiem, kas sniegti saskaņā ar dalībvalsts tiesību aktiem, Tiesa nosprieda, ka "vispārēja piekļuve visiem saglabātajiem datiem, kas nav atkarīga no jebkādas, kaut arī netiešas, saiknes ar sasniedzamo mērķi, nevar tikt uzskatīta par tādu, kas ir absolūti nepieciešamā robežās" (77.–78. punkts).

[44] ECT, *Klass*, 17., 51. punkts.

[45] *Schrems II*, 179., 183. punkts.

[46] ECT, *Big Brother Watch* pārsūdzētais spriedums, 319.–320. punkts.

[47] *Schrems II*, 179. punkts.

ievēroti nosacījumi un noteiktās garantijas.[48] Lai reāllaikā apkopotu datu plūsmas un atrašanās vietas datus, pārbaudei būtu jāļauj *ex ante* pārbaudīt, cita starpā, vai apkopošana ir atļauta tikai absolūti nepieciešamā robežās. Pienācīgi pamatotas neatliekamības gadījumā pasākumus var īstenot bez šādas iepriekšējas pārskatīšanas; tomēr Tiesa joprojām pieprasa, lai turpmākā pārbaude notiktu īsā laikā.[49]

42. Kas attiecas uz pārraudzības mehānismu neatkarību attiecībā uz uzraudzību, varētu ņemt vērā EST secinājumus par struktūras neatkarību tiesiskās aizsardzības ietvaros (skatīt tālāk D garantijas sadaļā). Turklāt ECT judikatūra var piedāvāt papildu elementus. Šī tiesa ir izteikusies, ka ir vēlams tiesnesim būt atbildīgam par pārraudzības uzturēšanu. Tomēr nav izslēgts, ka cita iestāde var būt atbildīga, "ja vien tā ir pietiekami neatkarīga no izpildvaras"[50] un "no iestādēm, kas veic uzraudzību, un [tai] ir piešķirtas pietiekamas pilnvaras un kompetence īstenot efektīvu un nepārtrauktu kontroli".[51] ECT piebilda, ka, novērtējot neatkarību, jāņem vērā "uzraudzības struktūras locekļu iecelšanas veids un to juridiskais statuss"[52]. Tas ietver "personas, kas kvalificētas ieņemt tiesu varas amatus un kuras ieceļ vai nu parlaments, vai premjerministrs. Turpretim iekšlietu ministrs, kurš bija ne tikai politiski ieceltais un izpildvaras dalībnieks, bet arī bija tieši iesaistīts īpašu uzraudzības līdzekļu nozīmēšanā, tika atzīts par nepietiekami neatkarīgu"[53]. ECT arī "atzīmē, ka ir svarīgi, lai uzraudzības struktūrai būtu piekļuve visiem attiecīgajiem dokumentiem, tostarp slēgtiem materiāliem".[54] Visbeidzot, ECT ņem vērā "vai uzraudzības struktūras darbība ir publiski pārbaudāma".[55]

## D garantija — indivīdam jābūt pieejamiem efektīviem līdzekļiem

43. Šī pēdējā Eiropas būtiskā garantija ir saistīta ar indivīda tiesībām uz tiesisko aizsardzību. Viņam/viņai jābūt efektīviem tiesiskās aizsardzības līdzekļiem, lai apmierinātu savas tiesības situācijā, ja viņš/viņa uzskata, ka tās netiek vai nav tikušas ievērotas. EST paskaidroja lietā *Schrems I,* ka "tiesiskajā regulējumā, kurā indivīdiem nav paredzētas nekādas iespējas likt lietā tiesību aizsardzības līdzekļus, lai piekļūtu personas datiem, kas uz tiem attiecas, vai panākt šādu datu labošanu vai dzēšanu, nav ņemta vērā Hartas 47. pantā iedibināto pamattiesību uz efektīvu aizsardzību tiesā būtība. Hartas 47. panta pirmajā daļā ir noteikts, ka ikvienai personai, kuras tiesības un brīvības, kas garantētas Savienības tiesībās, tikušas pārkāptas, ir tiesības uz efektīvu tiesību aizsardzību tiesā, ievērojot nosacījumus, kuri paredzēti šajā pantā."[56]

44. Izvērtējot dalībvalsts tiesību aktus, kas ļauj reāllaikā apkopot plūsmas un atrašanās vietas datus, Tiesa uzskatīja, ka informēšana ir nepieciešama, "lai ļautu šīm personām īstenot to tiesības, kas izriet no Hartas 7. un 8. panta, lūgt piekļuvi saviem personas datiem, kas ir šo pasākumu priekšmets, un vajadzības gadījumā panāktu to labošanu vai dzēšanu, kā arī saskaņā ar Hartas 47. panta pirmo daļu

[48] EST, *La Quadrature du Net u. c.*, 168., 189. punkts.

[49] EST, *La Quadrature du Net u. c.*, 189. punkts.

[50] ECTR, *Zakharov*, 258. punkts, *Iordachi u. c. / Moldova*, 40. un 51. punkts un *Dumitru Popescu / Rumānija,* 70.–73. punkts.

[51] ECT, *Klass,* 56. punkts, un *Big Brother Watch* pārsūdzētais spriedums 318. punkts.

[52] ECT, *Zakharov*, 278. punkts.

[53] ECT, *Zakharov*, 278. punkts.

[54] ECT, *Zakharov*, 281. punkts.

[55] ECT, *Zakharov*, 283. punkts.

[56] EST, *Schrems I*, 95. punkts.

izmantotu tiesības par efektīvu tiesību aizsardzību tiesā".[57] Tomēr tā arī atzina, ka personu, kuru dati ir savākti vai analizēti, informēšana jāveic tikai tiktāl, ciktāl šāda informēšana vairs nevar traucēt šo iestāžu uzdevumu izpildei.[58]

45. Arī ECT jautājums par efektīvu tiesiskās aizsardzības līdzekli ir nesaraujami saistīts ar indivīda informēšanu par uzraudzības pasākumu pēc uzraudzības beigām. Konkrēti, Tiesa konstatēja, ka "attiecīgajai personai principā ir maz iespēju vērsties tiesā, ja vien tā netiek informētas par pasākumiem, kas īstenoti bez viņa vai viņas ziņas, un tādējādi šī persona var apstrīdēt to likumību retrospektīvi vai arī, ja vien jebkura persona, kurai ir aizdomas, ka viņa vai viņas saziņa tiek vai ir tikusi pārtverta, var vērsties tiesā, tiesas piekritība nevar būt atkarīga no pārtveršanas subjekta informēšanas par viņa saziņas pārtveršanu".[59] Tādējādi ECT atzina, ka dažos gadījumos informēšana varētu netikt veikta, tomēr ir jānodrošina efektīvs tiesiskās aizsardzības līdzeklis. Šajā gadījumā Tiesa, piemēram, lietā *Kennedy*, ir skaidri norādījusi, ka tiesa nodrošina pietiekamas tiesiskās aizsardzības iespējas, ja tā atbilst virknei kritēriju, t. i., tā ir neatkarīga un objektīva struktūra ar saviem procesuālajiem noteikumiem; to veido dalībnieki, kuriem jābūt vai kuri bijuši augstos tiesu varas amatos vai kuriem jābūt pieredzējušiem juristiem un, ka netiek attiecināts pierādīšanas pienākums, lai tajā iesniegtu pieteikumu.[60] Izskatot privātpersonu sūdzības, tiesai vajadzētu būt pieejai visai būtiskajai informācijai,[61] tostarp slēgtiem materiāliem. Visbeidzot, tai būtu jābūt pilnvarām novērst neatbilstību.[62]

46. Hartas 47. pantā ir atsauce uz tribunālu ("*tribunal*"), kaut arī citās valodās, kas nav angļu, priekšroka tiek dota vārdam "tiesa",[63] savukārt ECT dalībvalstīm tikai uzliek pienākumu nodrošināt, ka "ikvienam, kura tiesības un brīvības tiek pārkāptas, būtu efektīvs tiesiskās aizsardzības līdzeklis valsts iestādē",[64] kurai nav vienmēr jābūt tiesu iestādei.[65]

47. EST saistībā ar spriedumu lietā *Schrems II*, novērtējot trešās valsts aizsardzības līmeņa atbilstību, ir atkārtoti uzsvērusi, ka "datu subjektiem ir jābūt iespējai izmantot tiesību aizsardzības līdzekļus neatkarīgā un objektīvā tiesā attiecībā uz piekļuvi to personas datiem, vai panākt šo datu labošanu vai dzēšanu".[66] Šajā pašā kontekstā EST uzskata, ka efektīvu tiesisko aizsardzību pret šādiem iejaukšanās gadījumiem var nodrošināt ne tikai tiesa, bet arī iestāde,[67] kas piedāvā garantijas, kuras būtībā ir līdzvērtīgas tām, kas prasītas Hartas 47. pantā. EST savā nolēmumā lietā *Schrems II* gan uzsvēra, ka ir jānodrošina tiesas vai struktūras neatkarība, jo īpaši no izpildvaras, ar visām nepieciešamajām

[57] Skatīt 190. punktu *La Quadrature du Net u. c.* un EST Atzinumu 1/15, 220. punkts
[58] Skatīt 191. punktu *La Quadrature du Net u. c*.
[59] ECT, *Zakharov*, 234. punkts.
[60] ECT, *Kennedy*, 190. punkts.
[61] EDAK atzīmē, ka Eiropas Padomes cilvēktiesību komisārs uzskata, ka tā dēvēto "trešo personu" noteikumu, saskaņā ar kuru vienas valsts izlūkdienestam, kas sniedz datus citas valsts izlūkdienestam, var uzlikt pienākumu saņēmējiem dienestiem atklāt nodotos datus trešai personai, nevajadzētu piemērot pārraudzības struktūrām, lai neapdraudētu efektīvu tiesiskās aizsardzības iespēju (*"Issue Paper on Democratic and effective oversight of national security services"*).
[62] ECT, *Kennedy*, 167. punkts.
[63] Vārds "tribunāls", piemēram, tiek tulkots kā "*Gericht*" vācu valodā un "*gerecht*" holandiešu valodā.
[64] ECTK 13. pants.
[65] ECT, *Klass*, 67. punkts.
[66] Skatīt 194. punktu *Schrems II.*
[67] Skatīt 197. punktu *Schrems II,* kur tiesa nepārprotami izmanto šo vārdu.

garantijām, tostarp attiecībā uz tās atsaukšanu vai tās iecelšanas atcelšanu,[68] un ka pilnvarām, kas jāpiešķir tiesai, jāatbilst Hartas 47. panta prasībām. Šajā sakarā iestādei[69] piešķir pilnvaras pieņemt lēmumus, kas ir saistoši izlūkdienestiem, saskaņā ar juridiskām garantijām, uz kurām datu subjekti var paļauties.[70]

# 4. NOBEIGUMA PIEZĪMES

48. Četras Eiropas būtiskās garantijas jāuzskata par galvenajiem elementiem, kuri jākonstatē, novērtējot iejaukšanās līmeni pamattiesībās uz privātumu un datu aizsardzību. Tās nav jānovērtē atsevišķi, jo tās ir cieši saistītas, bet kopumā jāpārskata attiecīgie tiesību akti attiecībā uz uzraudzības pasākumiem, minimālais drošības līmenis datu subjektu tiesību aizsardzībai un tiesiskās aizsardzības līdzekļi, kas paredzēti saskaņā ar trešās valsts tiesību aktiem.

49. Šīs garantijas prasa izmantot zināmu interpretāciju, jo īpaši tāpēc, ka trešo valstu tiesību aktiem nav jābūt identiskiem ar ES tiesisko regulējumu.

50. Kā ECT norādīja spriedumā lietā *Kennedy*, "novērtējums ir atkarīgs no visiem lietas apstākļiem, piemēram, no iespējamo pasākumu rakstura, tvēruma un ilguma, obligāti norādāmajiem iemesliem, lai tos pieprasītu, iestādēm, kas ir kompetentas tos atļaut, īstenot un uzraudzīt un valsts tiesību aktos paredzēto aizsardzības līdzekļu veida".[71]

51. Līdz ar to, izvērtējot trešo valstu uzraudzības pasākumus *EEG* kontekstā, var izdarīt divus secinājumus:

- attiecīgie trešo valstu tiesību akti nenodrošina *EEG* prasības: šajā gadījumā trešo valstu tiesību akti nepiedāvā tādu aizsardzības līmeni, kas būtībā ir līdzvērtīgs ES garantētajam;

- attiecīgie trešo valstu tiesību akti atbilst *EEG*.

52. Vērtējot aizsardzības līmeņa atbilstību, saskaņā ar VDAR 45. pantu Komisijai būs jānovērtē, vai *EEG* ir izpildītas to elementu ietvaros, kuri jāņem vērā, lai garantētu, ka trešās valsts tiesību akti kopumā nodrošina aizsardzības līmeni, kas būtībā ir līdzvērtīgs ES garantētajam.

53. Kad datu nosūtītāji kopā ar datu saņēmējiem atsaucas uz atbilstošiem aizsardzības pasākumiem saskaņā ar VDAR 46. pantu, ņemot vērā trešo valstu tiesību aktu prasības, kas īpaši piemērojamas nosūtītajiem datiem, tiem būtu jāpārliecinās, ka efektīvi tiek panākts būtībā līdzvērtīgs aizsardzības līmenis. Jo īpaši, ja trešās valsts tiesību akti neatbilst *EEG* prasībām, tas nozīmētu pārliecināties, ka attiecīgie tiesību akti neietekmēs ar nosūtīšanu saistītās garantijas un aizsardzības mehānismus, lai panāktu, ka joprojām tiek nodrošināts aizsardzības līmenis, kas būtībā ir līdzvērtīgs tam, kas garantēts ES.

---

[68] Skatīt 195. punktu *Schrems II.*

[69] Skatīt 197. punktu *Schrems II,* kur tiesa nepārprotami izmanto šo vārdu.

[70] Skatīt 196. punktu *Schrems II.*

[71] ECT, *Kennedy*, 153. punkts.

54. EDAK ir izdevusi papildu pamatnostādnes un ieteikumus, kas jāņem vērā, veicot novērtējumu, atkarībā no izmantojamā nosūtīšanas rīka un nepieciešamības nodrošināt atbilstošus drošības pasākumus, tostarp atkarībā no gadījuma, papildu pasākumus.[72]

55. Turklāt jāatzīmē, ka Eiropas būtiskās garantijas ir balstītas tiesību aktos noteiktajās prasībās. EDAK uzsver, ka Eiropas būtisko garantiju pamatā ir pamattiesības, kas attiecas uz visiem indivīdiem, neatkarīgi no viņu valstspiederības.

56. EDAK atkārtoti uzsver, ka Eiropas būtiskās garantijas ir atsauces standarts, novērtējot trešo valstu uzraudzības pasākumu radīto iejaukšanos starptautiskās datu nosūtīšanas kontekstā. Šie standarti izriet no ES tiesību aktiem un EST un ECT judikatūras, kas dalībvalstīm ir saistoša.

[72] *Adequacy Referential WP 254 rev.01*, pārskatīts un pieņemts 2018. gada 6. februārī; EDAK Ieteikumi 01/2020 pasākumiem, ar ko papildina nosūtīšanas rīkus, lai nodrošinātu atbilstību ES personas datu aizsardzības līmenim, 2020. gada 10. novembris.