



18/LV

WP 254 rev.01

### 29. panta darba grupa

#### **Pietiekamības atsauces**

Pieņemtas 2017. gada 28. novembrī

Pēdējo reizi pārskatītas un pieņemtas 2018. gada 6. februārī

Šī darba grupa izveidota saskaņā ar Direktīvas 95/46/EK 29. pantu. Tā ir neatkarīga Eiropas padomdevēja struktūra datu aizsardzības un privātuma jautājumos. Tās uzdevumi aprakstīti Direktīvas 95/46/EK 30. pantā un Direktīvas 2002/58/EK 15. pantā.

Sekretariāta pakalpojumus nodrošina Eiropas Komisijas Tiesiskuma un patērētāju ģenerāldirektorāta C direktorāts (Pamattiesības un Savienības pilsonība), B-1049, Brisele, Beļģija, birojs nr. MO-59 02/013.

Tīmekļa vietne: [http://ec.europa.eu/newsroom/article29/news.cfm?item\\_type=1358&tpa\\_id=6936](http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936)

## **Ievads**

ES datu aizsardzības iestāžu darba grupa<sup>1</sup> (DG29) ir iepriekš publicējusi Darba dokumentu par personas datu nosūtīšanu uz trešām valstīm (WP12)<sup>2</sup>. Aizstājot direktīvu ar ES Vispārīgo datu aizsardzības regulu (VDAR)<sup>3</sup> DG29 pārskata savas agrāk izdotās vadlīnijas WP12, lai tās atjauninātu saistībā ar jaunajiem tiesību aktiem un jaunāko Eiropas Savienības Tiesas (EST) judikatūru<sup>4</sup>.

Šā darba dokumenta mērķis ir atjaunināt WP12 pirmo nodaļu, kas attiecas uz svarīgo jautājumu par pietiekamu datu aizsardzības līmeni trešā valstī, kādā minētās trešās valsts teritorijā vai vienā vai vairākos konkrētos sektoros, vai starptautiskā organizācijā (turpmāk "trešās valstis vai starptautiskas organizācijas"). Turpmākajos gados šis dokuments tiks pastāvīgi pārskatīts un vajadzības gadījumā atjaunināts, pamatojoties uz praktisko pieredzi, kas gūta, piemērojot VDAR. WP12 dokumenta 2. nodaļa ("*Pieejas piemērošana valstīm, kuras ir ratificējušas Konvenciju Nr. 108*") un 3. nodaļa ("*Pieejas piemērošana nozares pašregulēšanai*") būtu jāatjaunina vēlākā posmā.

Šajā darba dokumentā uzmanība ir pievērsta tikai lēmumiem par aizsardzības līmeņa pietiekamību, kas ir Eiropas Komisijas īstenošanas akti<sup>5</sup> saskaņā ar VDAR 45. pantu. Citi aspekti par personas datu nosūtīšanu uz trešām valstīm un starptautiskām organizācijām tiks izskatīti turpmākajos darba dokumentos, kas tiks publicēti atsevišķi (saistoši uzņēmuma noteikumi, atkāpes).

Šā dokumenta mērķis ir sniegt norādījumus Eiropas Komisijai un DG29 saskaņā ar VDAR, lai izvērtētu datu aizsardzības līmeni trešās valstīs un starptautiskās organizācijās, nosakot galvenos datu aizsardzības principus, kam jābūt trešās valsts tiesiskajā regulējumā vai starptautiskā organizācijā, lai nodrošinātu aizsardzības līmeni, kas pēc būtības ir līdzvērtīgs ES regulējumam. Turklāt tas var kalpot kā norāde trešām valstīm un starptautiskām organizācijām, kuras vēlas nodrošināt pietiekamību. Tomēr šajā darba dokumentā izklāstītie principi nav vērsti tieši uz datu pārziņiem vai datu apstrādātājiem.

Šis dokuments sastāv no četrām nodaļām:

**1. nodaļa.** Vispārīga informācija par pietiekamības jēdzienu

**2. nodaļa.** Pietiekamības konstatējumu procesuālie aspekti saskaņā ar VDAR

**3. nodaļa.** Vispārīgie datu aizsardzības principi. Šajā nodaļā ir iekļauti galvenie vispārīgie datu aizsardzības principi, kas jāievēro, lai trešā valstī vai starptautiskā organizācijā nodrošinātu datu aizsardzības līmeni, kas pēc būtības ir līdzvērtīgs ES tiesību aktos noteiktajam.

**4. nodaļa.** Būtiskas garantijas piekļuvei tiesībaizsardzības un valsts drošības nolūkos, lai ierobežotu iejaukšanos pamattiesībās. Šajā nodaļā ir iekļautas būtiskas garantijas piekļuvei tiesībaizsardzības un valsts drošības nolūkos, ievērojot EST 2015. gada spriedumu lietā *Schrems* un pamatojoties uz 2016. gadā pieņemto DG29 darba dokumentu par būtiskajām garantijām.

---

<sup>1</sup> Izveidota saskaņā ar ES Datu aizsardzības direktīvas 95/46/EK 29. pantu.

<sup>2</sup> WP12, "Darba dokuments par personas datu nosūtīšanu uz trešām valstīm: ES datu aizsardzības direktīvas 25. un 26. panta piemērošana", kuru darba grupa pieņēma 1998. gada 24. jūlijā.

<sup>3</sup> Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (Dokuments attiecas uz EEZ).

<sup>4</sup> Tostarp spriedumu lietā C-362/14 *Maximilian Schrems* pret *Data Protection Commissioner*, 2015. gada 6. oktobris.

<sup>5</sup> Vairāk informācijas par īstenošanas aktiem skatīt VDAR 45. panta 3. punktā un 93. panta 2. punktā.

## 1. nodaļa. Vispārīga informācija par pietiekamības jēdzienu

VDAR 45. panta 1. punktā noteikts princips, ka datu nosūtīšanu uz trešo valsti vai starptautisku organizāciju var veikt tikai tad, ja trešā valsts, kāda minētās trešās valsts teritorija vai viens vai vairāki konkrēti sektori, vai attiecīgā starptautiskā organizācija nodrošina pietiekamu aizsardzības līmeni.

Šo “pietiekama aizsardzības līmeņa” jēdzienu, kas bija ietverts jau Direktīvā 95/46, turpināja attīstīt EST. Šajā brīdī ir svarīgi atgādināt standartu, kādu EST ir noteikusi lietā *Schrems*, proti — lai gan “aizsardzības līmenim” trešā valstī jābūt “būtībā ekvivalentam” ES garantētajam līmenim, “līdzekļi, pie kuriem šī trešā valsts ķeras šādas aizsardzības nodrošināšanai, var atšķirties no tiem, kas tikuši likti lietā [ES]”<sup>6</sup>. Tāpēc mērķis nav Eiropas tiesību aktu precīzs atspoguļojums, bet gan šo tiesību aktu būtisku pamatprasību noteikšana.

Eiropas Komisijas lēmumu par aizsardzības līmeņa pietiekamību nolūks ir oficiāli apstiprināt, radot dalībvalstīm saistošas sekas<sup>7</sup>, ka datu aizsardzības līmenis trešā valstī vai starptautiskā organizācijā būtībā ir līdzvērtīgs datu aizsardzības līmenim Eiropas Savienībā<sup>8</sup>. Pietiekamību var panākt, apvienojot datu subjektu tiesības un to personu, kuras datus apstrādā vai arī kuras īsteno kontroli pār neatkarīgu struktūru veikto apstrādi un uzraudzību, pienākumus. Tomēr datu aizsardzības noteikumi ir efektīvi tikai tad, ja tie ir izpildāmi un ievēroti praksē. Tāpēc ir nepieciešams ņemt vērā ne tikai to noteikumu saturu, kas attiecas uz personas datiem, kuri nosūtīti uz trešo valsti vai starptautisku organizāciju, bet arī sistēmu, kas nodrošina šādu noteikumu efektivitāti. Efektīvi izpildes mehānismi ir ārkārtīgi svarīgi datu aizsardzības noteikumu efektivitātei.

VDAR 45. panta 2. punktā ir noteikti elementi, kurus Eiropas Komisija ņem vērā, izvērtējot aizsardzības līmeņa pietiekamību trešā valstī vai starptautiskā organizācijā.

Piemēram, Komisija ņem vērā tiesiskumu, cilvēktiesību un pamatbrīvību ievērošanu, attiecīgos tiesību aktus, vienas vai vairāku neatkarīgu uzraudzības iestāžu pastāvēšanu un efektīvu darbību un starptautiskās saistības, ko ir uzņēmusies trešā valsts vai starptautiskā organizācija.

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

Datu aizsardzības “saturisko” principu un “procesuālo/izpildes” prasību “būtība”, ko varētu uzskatīt par minimālajām prasībām pietiekamam datu aizsardzības līmenim, izriet no ES Pamattiesību hartas un VDAR. Papildus būtu jāņem vērā arī citi starptautiskie nolīgumi datu aizsardzības jomā, piemēram, Konvencija Nr. 108<sup>9</sup>.

Tāpat ir jāpievērš uzmanība tiesiskajam regulējumam attiecībā uz valsts iestāžu piekļuvi personas datiem. Papildu norādes šajā sakarā ir izklāstītas darba dokumentā 237 (t. i., Būtisko garantiju dokuments)<sup>10</sup> par aizsardzības pasākumiem uzraudzības jomā.

Vispārīgi noteikumi par datu aizsardzību un privātumu trešā valstī nav pietiekami. Tieši pretēji, trešās valsts vai starptautiskās organizācijas tiesiskajā regulējumā jāiekļauj īpaši noteikumi, kas attiecas uz konkrētām vajadzībām attiecībā uz praktiskā ziņā būtiskiem tiesību uz datu aizsardzību aspektiem. Šiem noteikumiem jābūt izpildāmiem.

## 2. nodaļa. Pietiekamības konstatējumu procesuālie aspekti saskaņā ar VDAR

<sup>6</sup> Spriedums lietā C-362/14 *Maximillian Schrems* pret *Data Protection Commissioner*, 2015. gada 6. oktobris (73.-74. punkts);

<sup>7</sup> LESD 288. panta 2. punkts.

<sup>8</sup> Spriedums lietā C-362/14 *Maximillian Schrems* pret *Data Protection Commissioner*, 2015. gada 6. oktobris (52. punkts);

<sup>9</sup> VDAR 105. apsvērums.

<sup>10</sup> Darba dokuments 01/2016 par pamatojumu attiecībā uz pamattiesību uz privātumu un datu aizsardzību pārkāpumu uzraudzības pasākumu rezultātā, pārsūtot personas datus (Eiropas būtiskās garantijas), 16/LV WP 237, 2016. gada 13. aprīlis.

Lai EDAK varētu pildīt savu uzdevumu, sniedzot konsultācijas Eiropas Komisijai saskaņā ar VDAR 70. panta 1. punkta s) apakšpunktu, EDAK būtu jāsaņem attiecīga dokumentācija, tostarp attiecīga korespondence un Eiropas Komisijas konstatējumi. 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 izsmelšai un EDAK jāspēj veikt savu novērtējumu attiecībā uz datu aizsardzības līmeni trešā valstī. EDAK savlaicīgi sniegs atzinumu par Eiropas Komisijas konstatējumiem un noteiks pietiekamības sistēmas nepilnības, ja tādas būs. EDAK arī centīsies ierosināt izmaiņas vai grozījumus, lai novērstu iespējamās nepilnības.

Saskaņā ar VDAR 45. panta 4. punktu Eiropas Komisijai pastāvīgi jāuzrauga norises, kas varētu ietekmēt lēmuma par aizsardzības līmeņa pietiekamību darbību.

VDAR 45. panta 3. punktā noteikts, ka vismaz reizi četros gados ir jāveic periodiska pārskatīšana. Tomēr tas ir vispārīgs laika posms, kas 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.

Ņemot vērā pilnvaras 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 jāsaņem jēgpilna informācija par to, kā ES Komisija uzrauga attiecīgās norises šajā trešajā valstī vai starptautiskajā organizācijā. Tādējādi EDAK būtu jāsaņem informācija par jebkuru pārskatīšanas procesu un pārskatīšanas vizīti trešā valstī vai starptautiskajā organizācijā. EDAK labprāt tiktu uzaicināts piedalīties šajos pārskatīšanas procesos un vizītēs.

Tāpat būtu jāatzīmē, ka saskaņā ar VDAR 45. panta 5. punktu Eiropas Komisijai ir tiesības atcelt, grozīt vai apturēt esošos lēmumus par aizsardzības līmeņa pietiekamību. Līdz ar to atcelšanas, grozīšanas vai apturēšanas procedūrā būtu jāiesaista EDAK, lūdzot tās atzinumu saskaņā ar 70. panta 1. punkta s) apakšpunktu.

Turklāt, kā jau atzīts VDAR 58. panta 5. punktā un saskaņā ar EST spriedumu lietā *Schrems*, datu aizsardzības iestādēm jāspēj iesaistīties tiesvedībā, ja tās uzskata, ka personas prasība pret lēmumu par aizsardzības līmeņa pietiekamību ir pamatota: *“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.”*<sup>11</sup>.

---

<sup>11</sup> Spriedums lietā C-362/14 *Maximilian Schrems* pret *Data Protection Commissioner*, 2015. gada 6. oktobris (65. punkts)

**3. nodaļa. Vispārīgie datu aizsardzības principi, lai nodrošinātu, ka aizsardzības līmenis trešā valstī, kādā minētās trešās valsts teritorijā vai vienā vai vairākos konkrētos sektoros, vai starptautiskā organizācijā būtībā ir līdzvērtīgs tam, kas garantēts ES tiesību aktos**

**Trešās valsts vai starptautiskas organizācijas sistēmā jāietver šādi pamata saturiskie un procesuālie/izpildes datu aizsardzības principi un mehānismi:**

**A. Saturiskie principi**

**1) Jēdzieni**

Jāpastāv datu aizsardzības pamatjēdzieniem un/vai pamatprincipiem. Tiem nav jāatspoguļo VDAR terminoloģija, bet tiem būtu jāatspoguļo un jāaskaidro Eiropas datu aizsardzības tiesību aktos ietvertajiem jēdzieniem. Piemēram, VDAR iekļauti šādi svarīgi jēdzieni: “personas dati”, “personas datu apstrāde”, “datu pārzinis”, “datu apstrādātājs”, “saņēmējs” un “sensitīvi dati”.

**2) Iemesli likumīgai un godprātīgai apstrādei leģitīmos nolūkos**

Dati ir jāapstrādā likumīgi, godprātīgi un leģitīmi.

Juridiskais pamats, saskaņā ar kuru personas datus var likumīgi, godprātīgi un leģitīmi apstrādāt, būtu jānosaka pietiekami skaidri. Eiropas sistēmā tiek atzīti vairāki šādi leģitīmi iemesli, tostarp, piemēram, valsts tiesību aktu normas, datu subjekta piekrišana, datu pārziņa vai trešās personas līgumsaistību izpilde vai leģitīmas intereses, kas nav svarīgākas par indivīda interesēm.

**3) Nolūka ierobežošanas princips**

Dati būtu jāapstrādā noteiktā nolūkā, un pēc tam tos var izmantot, ciktāl tas nav pretrunā apstrādes nolūkam.

**4) Datu kvalitātes un proporcionālītātes princips**

Datiem vajadzētu būt precīziem un nepieciešamības gadījumā atjauninātiem. Datiem vajadzētu būt adekvātiem, atbilstīgiem un ne pārmērīgiem, ņemot vērā nolūkus, kādos tos apstrādā.

**5) Datu saglabāšanas princips**

Parasti datus būtu jāglabā ne ilgāk, kā tas ir nepieciešams nolūkiem, kādos personas datus apstrādā.

**6) Drošības un konfidencialitātes princips**

Jebkurai vienībai, kura apstrādā personas datus, būtu, izmantojot atbilstīgus tehniskus vai organizatoriskus pasākumus, jānodrošina, ka dati tiek apstrādāti tādā veidā, kas nodrošina personas datu drošību, tostarp aizsardzību pret neatļautu vai nelikumīgu apstrādi, kā arī pret nejaušu nozauģēšanu, iznīcināšanu vai sabojāšanu. Drošības pakāpē būtu jāņem vērā tehnikas līmenis un ar to saistītās izmaksas.

**7) Pārredzamības princips**

Jebkura persona būtu jāinformē par visiem galvenajiem tās personas datu apstrādes elementiem skaidrā, viegli pieejamā, kodolīgā, pārredzamā un saprotamā veidā. Šādā informācijā būtu jāiekļauj apstrādes nolūks, personas datu pārziņa identitāte, personai pieejamās tiesības un cita informācija, ciktāl tas ir nepieciešams godprātības nodrošināšanai. Noteiktos apstākļos var pastāvēt daži izņēmumi no šīm tiesībām uz informāciju, piemēram, lai garantētu kriminālizmeklēšanu, valsts drošību, tiesu iestāžu neatkarību un tiesvedību vai citus svarīgus vispārējo sabiedrības interešu mērķus, kas minēti VDAR 23. pantā.

## **8) Tiesības piekļūt datiem, labot un dzēst tos un celt iebildumus**

Datu subjektam vajadzētu būt tiesībām saņemt apstiprinājumu par to, vai tiek veikta viņa/viņas datu apstrāde, kā arī piekļūt saviem datiem, tostarp iegūt visu ar datu subjektu saistīto apstrādāto datu kopiju.

Datu subjektam vajadzētu būt tiesībām, pamatojoties uz konkrētiem iemesliem, veikt savu datu labojumus, piemēram, ja tie izrādās neprecīzi vai nepilnīgi, kā arī panākt savu personas datu dzēšanu, ja, piemēram, to apstrāde vairs nav nepieciešama vai ir nelikumīga.

Datu subjektam vajadzētu arī būt tiesībām jebkurā laikā, balstoties uz būtisku, ar viņa/viņas konkrēto situāciju saistītu leģitīmu iemeslu, iebilst pret viņa/viņas datu apstrādi īpašos apstākļos, kas noteikti trešās valsts tiesiskajā regulējumā. VDAR šādi apstākļi ir, piemēram, gadījumā, ja apstrāde ir nepieciešama, lai izpildītu uzdevumu, ko veic sabiedrības interesēs, vai lai īstenotu datu pārzinim likumīgi piešķirtās oficiālās pilnvaras, vai ja apstrāde ir nepieciešama personas datu pārziņa vai trešās personas leģitīmo interešu ievērošanai.

Šo tiesību īstenošana datu subjektam nedrīkst būt pārmērīgi apgrūtināša. Iespējamie ierobežojumi šādām tiesībām var rasties, piemēram, lai garantētu kriminālizmeklēšanu, valsts drošību, tiesu iestāžu neatkarību un tiesvedību vai citus svarīgus vispārējo sabiedrības interešu mērķus, kas minēti VDAR 23. pantā.

## **9) Tālākas nosūtīšanas ierobežojumi**

Sākotnējais datu saņēmējs drīkst nosūtīt oriģinālos personas datus tālāk tikai tad, ja turpmākajam saņēmējam (t. i., pārsūtīto datu saņēmējam) arī piemēro noteikumus (tostarp līguma noteikumus), kas nodrošina pietiekamu aizsardzības līmeni, un tas ievēro attiecīgus norādījumus, veicot datu apstrādi datu pārziņa uzdevumā. Tālāk nosūtot datus, nedrīkst mazināt to fizisko personu aizsardzības līmeni, kuru dati tiek nosūtīti. No ES nosūtīto datu sākotnējais saņēmējs ir atbildīgs par to, lai tiktu nodrošināti atbilstīgi aizsardzības pasākumi datu tālākai nosūtīšanai, ja nav pieņemts lēmums par aizsardzības līmeņa pietiekamību. Šāda datu tālāka nosūtīšana būtu jāveic tikai ierobežotiem un konkrētiem nolūkiem un tikai tad, ja pastāv šādas apstrādes juridiskais pamats.

## **B. Piemēri papildu saturiskajiem principiem, kurus piemēro konkrētiem apstrādes veidiem**

### **1) Īpašās datu kategorijas**

Ja tiek skartas īpašas datu kategorijas, būtu jāparedz konkrēti aizsardzības pasākumi<sup>12</sup>. Šīm kategorijām būtu jāatspoguļo VDAR 9. un 10. pantā noteiktās. Šāda aizsardzība būtu jāievieš, piemērojot stingrākas datu apstrādes prasības, piemēram, datu subjekts sniedz savu nepārprotamu piekrišanu apstrādei vai, izmantojot papildu drošības pasākumus.

### **2) Tiešā tirgvedība**

---

<sup>12</sup> Šādas īpašās kategorijas VDAR 10. apsvērumā tiek sauktas arī par "sensitīviem datiem".

Ja dati tiek apstrādāti tiešās tirgvedības nolūkā, datu subjektam jebkurā brīdī būtu jāspēj bez maksas iebilst pret savu datu apstrādi šādā nolūkā.

### **3) Automatizēta lēmumu pieņemšana un profilēšana**

Lēmumi, kuru pamatā ir tikai automatizēta apstrāde (automatizēta individuālu lēmumu pieņemšana), tostarp profilēšana, kā rezultātā datu subjektam iestājas juridiskas sekas vai būtiska ietekme, var tikt veikta tikai ar konkrētiem nosacījumiem, kas noteikti trešās valsts tiesiskajā regulējumā. Eiropas sistēmā šādi nosacījumi ietver, piemēram, vajadzību iegūt datu subjekta nepārprotamu piekrišanu vai šāda lēmuma nepieciešamību līguma noslēgšanai. Ja lēmums neatbilst tādiem nosacījumiem, kādi noteikti trešās valsts tiesiskajā regulējumā, datu subjektam vajadzētu būt tiesībām netikt pakļautam šādi lēmumu pieņemšanai. Trešās valsts tiesību aktos jebkurā gadījumā būtu jānodrošina nepieciešamie aizsardzības pasākumi, tostarp tiesības tikt informētam par lēmuma pamatā esošajiem konkrētiem iemesliem un izmantoto loģiku, labot neprecīzu vai nepilnīgu informāciju un apstrīdēt lēmumu, ja tas ir pieņemts, pamatojoties uz nepareiziem faktiem.

## **C. Procesuālie un izpildes mehānismi**

**Kaut arī līdzekļi, kādus trešā valsts izmanto, lai nodrošinātu pietiekamu aizsardzības līmeni, var atšķirties no tiem, kas tiek izmantoti Eiropas Savienībā<sup>13</sup>, Eiropas sistēmai atbilstošu sistēmu raksturo šādi elementi:**

### **1) Kompetenta neatkarīga uzraudzības iestāde**

Vajadzētu būt vienai vai vairākām neatkarīgām uzraudzības iestādēm, kurām ir pienākums uzraudzīt, 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 visām nepieciešamajām un pieejamām pilnvarām un misijām, lai 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.

### **2) Datu aizsardzības sistēmai ir jānodrošina labs atbilstības līmenis**

Trešās valsts sistēmai būtu jānodrošina augsts pārskatatbildības un 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 iedarbīgiem un preventīviem sodiem, gan arī iestāžu, reidentu vai neatkarīgu datu aizsardzības amatpersonu veiktu tiešo pārbaužu sistēmām.

### **3) Pārskatatbildība**

Trešās valsts datu aizsardzības sistēmā būtu jāuzliek par pienākumu datu pārziņiem un/vai personām, kuras apstrādā personas datus viņu vārdā, to ievērot un spēt uzskatāmi parādīt šādu atbilstību jo īpaši kompetentajai uzraudzības iestādei. Šādi pasākumi var būt, piemēram, datu aizsardzības ietekmes novērtējumi, datu apstrādes darbību ierakstu vai žurnālu saglabāšana uz atbilstošu laika periodu, datu aizsardzības speciālista norīkošana vai integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma.

---

<sup>13</sup> Spriedums lietā C-362/14 *Maximilian Schrems* pret *Data Protection Commissioner*, 2015. gada 6. oktobris (74. punkts).

**4) Datu aizsardzības sistēmai jānodrošina atbalsts un palīdzība atsevišķiem datu subjektiem, īstenojot viņu tiesības, kā arī atbilstošus tiesiskās aizsardzības mehānismus**

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

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



#### **4. nodaļa. Būtiskas garantijas piekļuvei trešās valstīs tiesībaizsardzības un valsts drošības nolūkos, lai ierobežotu iejaukšanos pamattiesībās**

Izvērtējot aizsardzības līmeņa pietiekamību, saskaņā ar 45. panta 2. punkta a) apakšpunktu Komisijai ir jāņem vērā “attiecināmie tiesību akti, gan vispārējie, gan nozaru, tostarp attiecībā uz sabiedrisko drošību, aizsardzību, valsts drošību un krimināltiesībām un publisko iestāžu piekļuvi personas datiem, kā arī šādu tiesību aktu (...) īstenošana (...)”.

EST lietā *Schrems* atzīmēja, ka “*“pienācīgs aizsardzības līmenis” būtu jāsaprot kā tāds, kur šī trešā valsts tik tiešām, pamatojoties uz savu iekšējo tiesisko kārtību vai starptautiskajām saistībām, ko tā uzņēmusies, nodrošina būtībā ekvivalentu pamatbrīvību un pamattiesību aizsardzības līmeni, kāds saskaņā ar Direktīvu 95/46, to lasot Hartas gaismā, ir garantēts Savienībā*”. Kaut arī līdzekļi, kurus šī trešā valsts izmanto, šajā sakarā var atšķirties no tiem, kurus izmanto Eiropas Savienībā, tomēr šiem līdzekļiem praksē ir jābūt efektīviem<sup>14</sup>.

Šajā kontekstā Tiesa arī kritiski atzīmēja, ka iepriekšējā drošības zonas lēmumā nebija “*ietverts neviens secinājums par to, ka ASV ir spēkā valsts tiesību akti, kuru mērķis ir ierobežot iespējamo iejaukšanos to personu pamattiesībās, kuru dati no Eiropas Savienības ir pārsūtīti uz ASV, — iejaukšanos, ko šīs valsts struktūras ir tiesīgas praktizēt, ja tā kalpo leģitīmam mērķim — kā valsts drošība*”.

2016. gada 13. aprīlī pieņemtajā atzinumā WP237 DG29 noteica būtiskas garantijas, kas atspoguļo EST un ECTK judikatūru uzraudzības jomā. Lai gan WP237 sīki izklāstītie ieteikumi joprojām paliek spēkā un tie būtu jāņem vērā, izvērtējot trešās valsts atbilstību uzraudzības jomā, šo garantiju piemērošana var atšķirties attiecībā uz piekļuvi datiem tiesībaizsardzības un valsts drošības nolūkos. Joprojām ir nepieciešams ievērot šīs četras garantijas attiecībā uz piekļuvi datiem gan valsts drošības, gan tiesībaizsardzības nolūkos visās trešās valstīs, lai tās varētu uzskatīt par atbilstošām:

- 1) apstrādei vajadzētu būt balstītai uz skaidriem, precīziem un pieejamiem noteikumiem (juridiskais pamats);**
- 2) attiecībā uz īstenotiem leģitīmajiem mērķiem ir uzskatāmi jāparāda nepieciešamība un proporcionalitāte;**
- 3) apstrādei ir jābūt pakļautai neatkarīgai pārraudzībai;**
- 4) personām ir jābūt pieejamiem efektīviem tiesiskās aizsardzības līdzekļiem.**

---

<sup>14</sup> Spriedums lietā C-362/14 *Maximilian Schrems* pret *Data Protection Commissioner*, 2015. gada 6. oktobris (74. punkts).