



Briselē, 6.11.2015.
COM(2015) 566 final

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

**par personas datu pārsūtīšanu no ES uz Amerikas Savienotajām Valstīm saskaņā ar
Direktīvu 95/46/EK, izpildot Tiesas spriedumu lietā C-362/14 (Schrems)**

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

par personas datu pārsūtīšanu no ES uz Amerikas Savienotajām Valstīm
saskaņā ar Direktīvu 95/46/EK, izpildot Tiesas spriedumu lietā C-362/14
(*Schrems*)

1. IEVADS. LĒMUMA PAR DROŠĪBAS ZONU ANULĒŠANA

Eiropas Savienības Tiesa (turpmāk tekstā — “Tiesa”), 2015. gada 6. oktobrī pasludinot spriedumu lietā C-362/14 (*Schrems*)¹, atkārtoti uzsver ES Pamattiesību hartā iedibināto pamattiesību uz personas datu aizsardzību nozīmi arī tajos gadījumos, kad šādi dati tiek nosūtīti ārpus ES.

Personas datu pārsūtīšana ir būtisks transatlantisko attiecību elements. ES un Amerikas Savienotās Valstis ir savstarpēji svarīgi tirdzniecības partneri, un aizvien biežāk datu pārsūtīšana ir neatņemama savstarpējās tirdzniecības daļa.

Lai atvieglinātu šīs datu plūsmas, vienlaikus nodrošinot augstu personas datu aizsardzības līmeni, Komisija atzina drošības zonas sistēmas piemērotību, 2000. gada 20. jūlijā pieņemot Komisijas lēmumu 2000/520/EK (turpmāk tekstā — “Lēmums par drošības zonu”). Šajā lēmumā, pamatojoties uz Direktīvas 95/46/EK² 25. panta 6. punktu, Komisija atzina, ka privātuma drošības zonas principi un attiecīgie visbiežāk uzdotie jautājumi, kurus izdevusi Amerikas Savienoto Valstu Tirdzniecības ministrija, nodrošina pienācīgu aizsardzību personas datu nosūtīšanai no ES³. Tāpēc, lai gan Amerikas Savienotajās Valstīs nav vispārēja datu aizsardzības likuma, personas datus var brīvi pārsūtīt no ES dalībvalstīm uz ASV uzņēmumiem, kas apņēmušies ievērot minētos principus. Drošības zonas noteikumu darbības pamatā ir iesaistīto uzņēmumu apņemšanās tos ievērot un pašsertifikācija. Lai gan apņemšanās ievērot privātuma drošības zonas principus un visbiežāk uzdotos jautājumus ir brīvprātīga, saskaņā ar ASV tiesību aktiem šie noteikumi ir saistoši tām struktūrām, kuras ir apņēmušās tos ievērot, un tos īsteno ASV Federālā tirdzniecības komisija⁴.

Tiesa savā 2015. gada 6. oktobra spriedumā paziņoja, ka Lēmums par drošības zonu nav spēkā. Tādēļ šā paziņojuma mērķis ir sniegt pārskatu par alternatīviem risinājumiem transatlantiskai datu pārsūtīšanai saskaņā ar Direktīvu 95/46/EK gadījumos, kad nav lēmuma par atbilstību. Tajā ir arī īsumā aprakstīta sprieduma ietekme uz citiem Komisijas lēmumiem

¹ Tiesas 2015. gada 6. oktobra spriedums lietā C-362/14 *Maximilian Schrems* pret *Data Protection Commissioner*, ES:C:2015:650 (turpmāk tekstā arī – “spriedums” vai “spriedums *Schrems* lietā”).

² Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti, OV L 281, 23.11.1995., 31. lpp. (turpmāk tekstā — “Direktīva 95/46/EK” vai “Direktīva”).

³ Šajā paziņojumā termins “ES” ietver arī EEZ. Tāpēc jāuzskata, ka atsauces uz dalībvalstīm attiecas arī uz EEZ dalībvalstīm.

⁴ Lai gūtu padziļinātu pārskatu par drošības zonas noteikumiem, skatiet Komisijas Paziņojumu Eiropas Parlamentam un Padomei par “drošības zonas” darbību no ES pilsoņu un uzņēmumu, kas veic uzņēmējdarbību ES, viedokļa, COM/2013/0847 final.

par atbilstību. Minētajā spriedumā Tiesa paskaidroja, ka attiecībā uz Direktīvas 95/46/EK 25. panta 6. punktā paredzēto lēmumu jāievēro prasība, ka Komisija ir konstatējusi — attiecīgajā trešā valstī personas datu aizsardzības līmenis “būtībā ir līdzvērtīgs” līmenim, kāds ES ir nodrošināts ar Direktīvu, skatot to kopsakarā ar Pamattiesību hartu. Attiecībā uz Lēmumu par drošības zonu Tiesa sprieda, ka Komisija tajā nav izdarījusi pietiekamus slēdzienus par ierobežojumiem ASV valsts iestāžu piekļuvei datiem, kas pārsūtīti saskaņā ar šo lēmumu, un par efektīvu tiesisko aizsardzību pret šāda veida iejaukšanos. Proti, Tiesa paskaidroja, ka tiesiskais regulējums, saskaņā ar kuru valsts iestādēm vispārīgi tiek ļauts piekļūt elektronisko komunikāciju saturam, jāuzskata par tādu, kas apdraud pašu pamattiesību uz privātās dzīves neaizskaramību būtību. Turklāt Tiesa apstiprināja — lai gan saskaņā ar Direktīvas 95/46/EK 25. panta 6. punktu ir pieņemts Lēmums par atbilstību, dalībvalstu datu aizsardzības iestādes (DAI) joprojām ir pilnvarotas pārbaudīt un tām ir pilnīgi neatkarīgi jāpārbauda, vai datu pārsūtīšana uz trešo valsti atbilst prasībām, kas noteiktas Direktīvā 95/46/EK, skatot to kopsakarā ar Pamattiesību hartas 7., 8. un 47. pantu. Tomēr Tiesa arī apstiprināja, ka tikai Tiesa var konstatēt ES tiesību akta, kāds ir Komisijas lēmums par atbilstību, spēkā neesību.

Tiesas spriedumā ir izmantots Komisijas 2013. gada paziņojums par “drošības zonas” darbību no ES pilsoņu un uzņēmumu, kas veic uzņēmējdarbību ES, viedokļa⁵, kur Komisija norādīja vairākas nepilnības un izstrādāja 13 ieteikumus. Ņemot vērā šos ieteikumus, Komisija no 2014. gada janvāra rīkoja pārrunas ar ASV iestādēm, lai ieviestu atjauninātu un stingrāku transatlantiskās datu apmaiņas kārtību.

Pēc sprieduma pasludināšanas Komisija joprojām ir apņēmusies izstrādāt atjauninātu un pienācīgu personas datu transatlantiskās pārsūtīšanas sistēmu. Šajā ziņā tā nekavējoties atjaunoja un pasteidzināja pārrunas ar ASV valdību, lai nodrošinātu, ka jebkāda jauna personas datu transatlantiskās pārsūtīšanas kārtība pilnībā atbilst Tiesas noteiktajam standartam. Tādēļ šādai sistēmai vajadzīgi pietiekami ierobežojumi, garantijas un tiesiskās uzraudzības mehānismi, lai nodrošinātu ES iedzīvotāju personas datu pastāvīgu aizsardzību, tostarp attiecībā uz valsts iestāžu iespējamu piekļuvi tiesībaizsardzības un valsts drošības nolūkā. Tikmēr nozare ir paudusi bažas par nepārtrauktas datu pārsūtīšanas iespējām⁶. Tādēļ jāprecizē, saskaņā ar kādiem nosacījumiem šādu pārsūtīšanu var turpināt. Minētā iemesla dēļ 29. panta darba grupa — neatkarīga padomdevēja struktūra, kur apvienoti visu dalībvalstu DAI pārstāvji, kā arī Eiropas Datu aizsardzības uzraudzītājs — 16. oktobrī izdeva

⁵ Komisijas Paziņojums Eiropas Parlamentam un Padomei par “drošības zonas” darbību no ES pilsoņu un uzņēmumu, kas veic uzņēmējdarbību ES, viedokļa, COM(2013) 847 final, 27.11.2013. Sk. arī Komisijas Paziņojumu Eiropas Parlamentam un Padomei “Uzticēšanās atjaunošana datu plūsmām starp ES un ASV”, COM(2013) 846 final, 27.11.2013., un attiecīgo memorandu “Uzticēšanās atjaunošana datu plūsmām starp ES un ASV — visbiežāk uzdotie jautājumi”, MEMO/13/1059, 27.11.2013.

⁶ Nozares pārstāvju apvienības puda šīs bažas cita starpā sanāksmē, ko priekšsēdētāja vietnieks A. Ansips un komisāri V. Jourova un G. Etingers rīkoja 14. oktobrī tūlīt pēc sprieduma pasludināšanas *Schrems* lietā. Sk. *Daily News*, 14.10.2015., (MEX/15/5840). Skatiet arī: “*Open letter on the implementation of the CJEU Judgement on Case C-362/14 Maximilian Schrems v Data Protection Commissioner*” (Atklāta vēstule par Tiesas sprieduma lietā C-362/14 *Maximilian Schrems* pret *Data Protection Commissioner*), datēta ar 2015. gada 13. oktobri, kas adresēta Komisijas priekšsēdētājam Žanam Klodam Junkeram un ko parakstījušas vairākas ES un ASV nozares apvienības un uzņēmumi: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1045&PortalId=0&TabId=353.

paziņojumu⁷ par pirmajiem secinājumiem saistībā ar spriedumu. Citu punktu starpā šajā paziņojumā bija šādi norādījumi par datu pārsūtīšanu:

- datu pārsūtīšanai vairs nevar izmantot spēkā neesošo Komisijas Lēmumu par drošības zonu;
- pagaidām datu pārsūtīšanas pamatā var būt līguma standartklauzulas (turpmāk tekstā arī — “LSK”) un saistošie uzņēmumu noteikumi (turpmāk tekstā arī — “SUN”), lai gan 29. panta darba grupa arī ir paziņojusi, ka turpinās analizēt sprieduma ietekmi uz šiem alternatīvajiem risinājumiem.

Paziņojumā tika pausts arī aicinājums dalībvalstīm un ES iestādēm sākt diskusijas ar ASV iestādēm, lai rastu juridiskus un tehniskus datu pārsūtīšanas risinājumus; 29. panta darba grupa uzskata, ka šā risinājuma daļa varētu būt sarunas par jaunu drošības zonu.

29. panta darba grupa paziņoja — ja līdz 2016. gada janvāra beigām kopā ar ASV iestādēm nebūs rasts piemērots risinājums un atkarībā no datu pārsūtīšanai izmantotajiem alternatīvajiem risinājumiem, DAI veiks visus vajadzīgos un piemērotos pasākumus, tostarp saskaņotu izpildes pasākumu.

Visbeidzot, 29. panta darba grupa uzsvēra, ka DAI, ES iestādēm, dalībvalstīm un uzņēmumiem ir kopīgs pienākums rast ilgtspējīgus risinājumus, lai īstenotu Tiesas spriedumu. Jo īpaši darba grupa mudināja uzņēmumus apsvērt iespēju ieviest juridiskus un tehniskus risinājumus, lai mazinātu iespējamus riskus, kas viņiem varētu rasties, pārsūtot datus.

Šis paziņojums neskar DAI pilnvaras un pienākumu pilnīgi neatkarīgi pārbaudīt šādas pārsūtīšanas likumību⁸. Tajā nav paredzēti saistoši noteikumi un ir pilnībā ievērotas valstu tiesu pilnvaras interpretēt piemērojamos tiesību aktus un vajadzības gadījumā lūgt Tiesu sniegt prejudiciālu nolēmumu. Šo paziņojumu nevar izmantot par pamatojumu individuālām vai kolektīvām juridiskām tiesībām vai prasībām.

2. ALTERNATĪVS PAMATOJUMS PERSONAS DATU PĀRSŪTĪŠANAI UZ ASV

Direktīvā 95/46/EK paredzēto Starptautiskās datu pārsūtīšanas noteikumu pamatā ir skaidri nošķirta, no vienas puses, datu pārsūtīšana uz trešām valstīm, kuras nodrošina pietiekamu aizsardzības līmeni (Direktīvas 25. pants), un, no otras puses, datu pārsūtīšana uz trešām valstīm, kuras nenodrošina pietiekamu aizsardzības līmeni (Direktīvas 26. pants).

⁷ 29. panta darba grupas paziņojums pieejams internetā: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

⁸ Sk. Pamattiesību hartas 8. panta 3. punktu un LESD 16. panta 2. punktu. Šo neatkarību uzsvērusi arī Tiesa savā spriedumā *Schrems* lietā.

Spriedumā *Schrems* lietā aplūkoti nosacījumi, kurus piemērojot, saskaņā ar Direktīvas 95/46/EK 25. panta 6. punktu Komisija var noteikt, vai trešā valsts nodrošina pietiekamu aizsardzības līmeni.

Gadījumos, kad tiek konstatēts, ka trešā valsts, uz kuru no ES jāpārsūta personas dati, nenodrošina šādu pietiekamu aizsardzības līmeni, Direktīvas 95/46/EK 26. pantā ir noteikti vairāki alternatīvi pamatojumi, balstoties uz kuriem datu pārsūtīšanu tomēr varētu veikt. Proti, datu pārsūtīšanu var veikt, ja struktūra, kas atbild par personas datu apstrādes nolūkiem un līdzekļiem (“datu apstrādātājs”):

- sniedz atbilstošas garantijas Direktīvas 95/46/EK 26. panta 2. punkta nozīmē attiecībā uz personu privātās dzīves un pamattiesību un brīvību aizsardzību un attiecībā uz atbilstošo tiesību izmantošanu. Šādas garantijas jo īpaši var sniegt, izmantojot datu nosūtītājam un saņēmējam saistošus līguma punktus (sk. 2.1. un 2.2. sadaļu turpmāk). Tie ietver līguma standartklauzulas, ko izdevusi Komisija, un — attiecībā uz datu pārsūtīšanu starp dažādām starptautisku uzņēmumu grupas struktūrām — saistošos uzņēmuma noteikumus, ko apstiprinājušas DAI; vai
- izmanto kādu no atkāpēm, kas precīzi uzskaitītas Direktīvas 95/46/EK 26. panta 1. punkta a) līdz f) apakšpunktā (sk. 2.3. sadaļu turpmāk).

Salīdzinot ar lēmumiem par atbilstību, kurus pieņem pēc attiecīgās trešās valsts sistēmas vispārēja novērtējuma un kuri faktiski var aptvert visus datu pārsūtīšanas gadījumus uz šo sistēmu, šiem abiem alternatīvajiem datu pārsūtīšanas pamatojumiem var būt ierobežota piemērošanas joma (jo tos piemēro tikai konkrētām datu plūsmām) un plašāks aptvērums (jo tie ne vienmēr ir piesaistīti konkrētai valstij). Šos risinājumus piemēro datu plūsmām, ko veic konkrētas struktūras, kuras nolēmušas izmantot vienu no Direktīvas 95/46/EK 26. pantā piedāvātajām iespējām. Turklāt datu nosūtītājiem un saņēmējiem, kas savu datu pārsūtīšanu pamato ar minētajiem pamatojumiem un tāpēc nevar paļauties uz trešās valsts atbilstību, kas noteikta Komisijas lēmumā, jānodrošina datu pārsūtīšanas atbilstība Direktīvas prasībām.

2.1. Līgumiski risinājumi

Kā uzsvērusi 29. panta darba grupa, lai nodrošinātu pietiekamas garantijas atbilstīgi Direktīvas 95/46/EK 26. panta 2. punktam, līguma punktiem “pietiekamā mērā jākompensē neesošas pietiekamās aizsardzības vispārējais līmenis, iekļaujot būtiskos aizsardzības elementus, kuru trūkst katrā konkrētajā situācijā”⁹. Lai atvieglotu šādu instrumentu izmantošanu attiecībā uz datu starptautisku pārsūtīšanu, Komisija saskaņā ar Direktīvas 26. panta 4. punktu ir apstiprinājusi četrus līguma standartklauzulu kopumus, kas atzīti par atbilstīgiem Direktīvas 26. panta 2. punkta prasībām. Divi līguma standartklauzulu kopumi

⁹ Sk. 29. panta darba grupas dokumentu “*Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*” (Personas datu nosūtīšana uz trešām valstīm: ES Datu aizsardzības direktīvas 25. un 26. panta piemērošana) (WP 12), 1998. gada 24. jūlijs, 16. lpp.

attiecas uz datu pārsūtīšanu starp personas datu apstrādātājiem¹⁰, savukārt otri divi līguma standartklauzulu kopumi attiecas uz datu pārsūtīšanu starp datu apstrādātāju un apstrādātāju, kas darbojas saskaņā ar personas datu apstrādātāja norādījumiem¹¹. Abos šo līguma standartklauzulu kopumos ir noteikti datu nosūtītāja un datu saņēmēja attiecīgie pienākumi. Šie pienākumi cita starpā ietver drošības pasākumus, datu subjekta informēšanu slepenu datu pārsūtīšanas gadījumā, paziņošanu datu nosūtītājam par trešās valsts tiesībaizsardzības iestāžu iesniegtu piekļuves pieprasījumu vai par nejaūšu vai neatļautu piekļuvi, datu subjektu tiesības piekļūt saviem personas datiem, tos labot un dzēst, kā arī noteikumus par kompensāciju datu subjektam gadījumos, kad radīti zaudējumi, vienai no pusēm pārkāpjot līguma standartklauzulas. Līguma standartklauzulās paredzēta arī prasība nodrošināt ES datu subjektiem iespēju vērsties DAI un/vai datu nosūtītāja reģistrācijas dalībvalsts tiesā, lai īstenotu savas ieinteresētās trešās personas tiesības, kas izriet no līguma punktiem¹². Šīs tiesības un pienākumi jāiekļauj līguma punktos, jo atšķirībā no situācijas, kad Komisija ir konstatējusi atbilstību, šajā gadījumā nav iespējams uzskatīt, ka datu saņēmējam trešā valstī piemēro atbilstošu sistēmu datu aizsardzības noteikumu uzraudzībai un izpildei.

Tā kā Komisijas lēmumi dalībvalstīm pilnībā ir saistoši, līguma standartklauzulu iekļaušana līgumā nozīmē, ka valsts iestādēm faktiski jāatzīst šīs klauzulas. Tādējādi tās nevar atteikties pārsūtīt datus uz trešo valsti tikai tāpēc, ka šīs līguma standartklauzulas nenodrošina pietiekamas garantijas. Tas neskar šo iestāžu tiesības pārbaudīt šīs klauzulas, ņemot vērā prasības, ko Tiesa noteikusi spriedumā *Schrems* lietā. Šaubu gadījumā tās var ierosināt tiesvedību valsts tiesā, kas savukārt var lūgt Tiesu sniegt prejudiciālu nolēmumu. Lai gan vairākuma dalībvalstu tiesību aktos, kuros transponēta Direktīva 95/45/EK, nav prasības par iepriekšēju valsts atļauju datu pārsūtīšanai, dažas dalībvalstis ir saglabājušas sistēmu līguma standartklauzulu paziņošanai un/vai to izmantošanas iepriekšējai apstiprināšanai. Valstīs, kurās ir šāda prasība, valstu DAI jāsalīdzina konkrētā līguma faktiskie punkti ar līguma standartklauzulām un jāpārbauda, vai nav veiktas izmaiņas¹³. Ja punkti nav grozīti¹⁴, atļauja

¹⁰ Komisijas 2001. gada 15. jūnija Lēmums 2001/497/EK par līguma standartklauzulām attiecībā uz personas datu nosūtīšanu trešām valstīm saskaņā ar Direktīvu 95/46/EK, OV L 181, 4.7.2001., 19. lpp., un Komisijas 2004. gada 27. decembra Lēmums 2004/915/EK, ar ko groza Lēmumu 2001/497/EK attiecībā uz alternatīvu līguma standartklauzulu ieviešanu personas datu nosūtīšanai trešām valstīm, OV L 385, 29.12.2004., 74. lpp.

¹¹ Komisijas 2001. gada 27. decembra Lēmums 2002/16/EK par līguma standartklauzulām attiecībā uz personas datu nosūtīšanu trešās valstīs reģistrētiem apstrādātājiem saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK, OV L 6, 10.1.2002., 52. lpp., Komisijas 2010. gada 5. februāra Lēmums 2010/87/ES attiecībā uz personas datu pārsūtīšanu trešās valstīs reģistrētiem apstrādātājiem saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK, OV L 39, 12.2.2010., 5. lpp. Iepriekšējais lēmums, kas tika atcelts ar pēdējo minēto lēmumu, attiecas tikai uz līgumiem, kas noslēgti līdz 2010. gada 15. maijam.

¹² Sk., piemēram, Komisijas Lēmuma 2004/915/EK 6. apsvērumu un šā lēmuma pielikuma V punktu; Komisijas Lēmuma 2010/87/ES pielikuma 7. punktu.

¹³ Būtu jāatzīmē, ka Vispārīgās datu aizsardzības regulas priekšlikumā (COM(2012) 11 final) paredzēts, ka datu pārsūtīšanai, kas pamatota ar līguma standartklauzulām vai saistošiem uzņēmuma noteikumiem tādā apmērā, kādā tos pieņēmusi Komisija, vai saskaņā ar paredzēto konsekvences mehānismu, nav nepieciešama nekāda cita atļauja.

¹⁴ Tomēr līguma standartklauzulu izmantošana neliedz pusēm vienoties par citiem punktiem, ja tie nedz tieši, nedz netieši nav pretrunā Komisijas apstiprinātajiem punktiem vai neskar datu subjektu pamattiesības vai brīvības. Sk. Eiropas Komisija, "*Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries*" (Visbiežāk uzdotie jautājumi par personas datu pārsūtīšanu no ES/EEZ)

parasti¹⁵ tiek piešķirta automātiski¹⁶. Kā paskaidrots turpmāk (sk. 2.4. sadaļu), šāda prasība neskar papildu pasākumus, kas datu nosūtītājam būtu jāveic, jo īpaši attiecībā uz informāciju, kas saņemta no datu saņēmēja par trešās valsts tiesību sistēmas izmaiņām, kas varētu liegt datu saņēmējam pildīt savus līgumā noteiktos pienākumus. Piemērojot līguma standartklausulas, gan datu nosūtītājus, gan datu saņēmējus uzrauga datu aizsardzības iestādes.

Līguma standartklausulu pieņemšana neliedz uzņēmumiem izmantot citus instrumentus, piemēram, konkrētajam gadījumam izstrādātas līgumsaistības, lai pierādītu, ka to veiktajai datu pārsūtīšanai ir pietiekamas garantijas Direktīvas 95/46/EK 26. panta 2. punkta nozīmē. Saskaņā ar Direktīvas 26. panta 2. punktu šīs garantijas apstiprina valsts iestādes, izskatot katru konkrēto gadījumu. Dažas datu aizsardzības iestādes šajā jomā ir izstrādājušas norādījumus, tostarp kā standartizētus līgumus vai sīki izstrādātus noteikumus, kas jāievēro, sagatavojot līguma punktus par datu pārsūtīšanu. Tomēr vairākums līgumu, kurus šobrīd uzņēmumi izmanto, lai veiktu savu datu pārsūtīšanu starptautiskajā mērogā, ir pamatoti ar Komisijas apstiprinātajām līguma standartklausulām¹⁷.

2.2. Datu pārsūtīšana uzņēmumu grupā

Lai saskaņā ar prasībām Direktīvas 95/46/EK 26. panta 2. punktā pārsūtītu datus no ES uz filiālēm ārpus ES starptautisks uzņēmums var pieņemt saistošus uzņēmuma noteikumus. Šādu rīcības kodeksu var izmantot tikai datu pārsūtīšanai uzņēmumu grupā.

Tādējādi, piemērojot SUN, personas datus var brīvi pārsūtīt starp dažādām uzņēmuma grupas struktūrām visā pasaulē — neveidojot savstarpējas līgumsaistības starp katru uzņēmuma struktūru —, vienlaikus nodrošinot, ka, piemērojot saistošus un izpildāmus noteikumus, visā grupā tiek nodrošināts vienādi augsts personas datu aizsardzības līmenis. Vienādi noteikumi veido vienkāršāku un efektīvāku sistēmu, kuru ērtāk var īstenot darbinieki un izprast datu subjekti. Lai palīdzētu uzņēmumiem izstrādāt saistošos uzņēmuma noteikumus, 29. panta darba grupa, pamatojoties uz ES datu aizsardzības standartiem, attiecībā uz SUN ir izstrādājusi materiālas (piemēram, datu apstrādes mērķa ierobežojums, apstrādes drošība, pārredzama informācija datu subjektiem, ierobežojumi datu tālākai pārsūtīšanai ārpus grupas, individuālas piekļuves tiesības, labošana un apstrīdēšana) un procesuālas (piemēram, auditi,

(FAQ B.I.9), 28. lpp. (pieejams internetā: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf).

¹⁵ Ja DAI ir šaubas par līguma standartklausulu atbilstību Direktīvas prasībām, tai ar attiecīgo jautājumu jāvēršas valsts tiesā, kas var lūgt Tiesu sniegt prejudiciālu nolēmumu (sal. sprieduma *Schrems* lietā 51., 52., 64. un 65. punktu).

¹⁶ 29. panta darba grupa ir izstrādājusi īpašu datu aizsardzības iestāžu sadarbības procedūru, ko piemēro to līguma punktu apstiprināšanai, kurus uzņēmums vēlas izmantot dažādās dalībvalstīs. Sk. 29. panta darba grupas dokumentu "*Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on 'Contractual clauses' Considered as compliant with the EC Model Clause*" (Darba dokuments, ar ko nosaka sadarbības procedūru par kopējas nostājas izdošanu attiecībā uz līguma noteikumiem, kas uzskatāmi par atbilstīgiem ES standartklausulai) (WP 226), 2014. gada 26. novembris. Sk. arī Komisijas Lēmuma 2004/915/EK pielikuma VII punktu un Komisijas Lēmuma 2010/87/ES pielikuma 10. punktu.

¹⁷ Sk. 29. panta darba grupas dokumentu "*Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on 'Contractual clauses' Considered as compliant with the EC Model Clause*" (WP 226), 2014. gada 26. novembris, 2. lpp.

atbildības kontrole, sūdzību izskatīšana, sadarbība ar datu aizsardzības iestādēm, atbildība un jurisdikcija) prasības¹⁸. Šie noteikumi ir saistoši ne vien uzņēmumu grupas locekļiem, bet — līdzīgi līguma standartklauzulām — arī izpildāmi ES: personām, kuru datus apstrādā grupas struktūra, nodrošina tiesības kā ieinteresētām trešām personām iesniegt sūdzību datu aizsardzības iestādē un vērsties dalībvalsts tiesā un pieprasīt, lai tiktu ievēroti saistošie uzņēmuma noteikumi. Turklāt saistošajos uzņēmuma noteikumos jānorīko struktūra ES, kas uzņemas atbildību gadījumos, kad noteikumus ir pārkāpis jebkurš grupas loceklis ārpus ES, kuram šie noteikumi ir saistoši.

Vairākumā dalībvalstu tiesību aktos, kur transponēta Direktīva, noteikts, ka datu pārsūtīšana saskaņā ar saistošajiem uzņēmuma pamatnoteikumiem jāapstiprina datu aizsardzības iestādei katrā dalībvalstī, no kuras starptautiskais uzņēmums vēlas pārsūtīt datus. Lai atvieglotu un paātrinātu šo procesu, kā arī mazinātu pieteikumu iesniedzēju slogu, 29. panta darba grupa ir izveidojusi standartizētu pieteikuma veidlapu¹⁹ un attiecīgo DAI īpašas sadarbības procedūru²⁰, kur paredzēts arī norīkot vienu “vadošo iestādi”, kas atbild par apstiprināšanas procedūras izpildi.

2.3. Atkāpes

Ja nav lēmuma par atbilstību saskaņā ar Direktīvas 95/46/EK 25. panta 6. punktu un neatkarīgi no līguma standartklauzulu vai saistošo uzņēmuma noteikumu piemērošanas, personas datus trešā valstī reģistrētiem uzņēmumiem joprojām var pārsūtīt tādā apmērā, kādā uz tiem attiecas kāda no alternatīvajām atkāpēm, kas minētas Direktīvas 95/46/EK 26. panta 1. punktā:²¹

- datu subjekts viennozīmīgi ir devis savu piekrišanu ierosinātajai datu pārsūtīšanai;

¹⁸ Sk. 29. panta darba grupas dokumentus: “*Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*” (Darba dokuments, ar ko izveido saistošo uzņēmuma noteikumu elementu un principu tabulu) (WP 153), 2008. gada 24. jūnijs; “*Working Document setting up a framework for the structure of Binding Corporate Rules*” (Darba dokuments, ar ko izveido saistošo uzņēmuma noteikumu struktūras sistēmu) (WP 154), 2008. gada 24. jūnijs; un “*Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules*” (Darba dokuments par visbiežāk uzdotajiem jautājumiem attiecībā uz saistošajiem uzņēmuma noteikumiem) (WP 155), 2008. gada 24. jūnijs.

¹⁹ 29. panta darba grupa, “*Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data*” (Standarta pieteikuma veidlapa personas datu pārsūtīšanai piemērojamo saistošo uzņēmuma noteikumu apstiprināšanai) (WP 133), 2007. gada 10. janvāris.

²⁰ 29. panta darba grupa “*Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From 'Binding Corporate Rules'*” (Darba dokuments, ar ko nosaka sadarbības procedūru par kopējas nostājas izdošanu attiecībā uz pietiekamām garantijām, kas izriet no saistošajiem uzņēmuma noteikumiem) (WP 107), 2005. gada 14. aprīlis.

²¹ Kā uzsvērusi 29. panta darba grupa, attiecībā uz šo atkāpju piemērošanu jāievēro pārējie Direktīvas 95/46/EK noteikumi, ciktāl tie ietver papildu prasības attiecībā uz šīm atkāpēm (piemēram, 8. pantā noteiktie ierobežojumi attiecībā uz slepenu datu apstrādi). Sk. 29. panta darba grupa, “Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta piemērošanu” (WP 114), 2005. gada 25. novembris, 8. lpp. Sk. arī Eiropas Komisija, “*Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries*” (FAQ D.2), 50. lpp.

- pārsūtīšana vajadzīga, lai izpildītu līgumu starp datu subjektu un datu apstrādātāju vai lai īstenotu pēc datu subjekta pieprasījuma veiktos pasākumus, kuriem seko līguma noslēgšana;
- datu pārsūtīšana vajadzīga līguma noslēgšanai starp datu apstrādātāju un trešajām personām datu subjekta interesēs vai šāda līguma izpildei;
- datu pārsūtīšana vajadzīga vai ir likumīgi prasīta, pamatojoties uz svarīgām sabiedrības interesēm²², vai juridisku prasību pamatojumam, realizācijai vai aizstāvībai;
- datu pārsūtīšana vajadzīga, lai aizsargātu datu subjekta būtiskas intereses;
- pārsūtīšanu izdara no reģistra, kas saskaņā ar likumiem vai regulējumiem ir paredzēts, lai sniegtu informāciju sabiedrībai, un kas ir pieejams, lai gūtu informāciju, gan plaša sabiedrība, gan jebkura persona, kura var pierādīt likumīgu ieinteresētību, ciktāl likumā par informācijas pieejamību izvirzītie nosacījumi konkrētajā gadījumā tiek izpildīti.

Balstoties uz šiem pamatojumiem, var piemērot atkāpi no vispārējā aizlieguma pārsūtīt personas datus uz trešo valsti, kura nenodrošina pietiekamu aizsardzības līmeni. Datu nosūtītājam faktiski nav jānodrošina, ka datu saņēmējs nodrošinās pietiekamu aizsardzību, un parasti viņam nav jāsaņem attiecīgās valsts iestādes iepriekšēja atļauja datu pārsūtīšanai. Tomēr — tā kā šis atkāpes piemēro ārkārtas gadījumos — 29. panta darba grupa uzskata, ka tās jāinterpretē precīzi²³.

29. panta darba grupa ir izdevusi vairākus nesaistošus norādījumu dokumentus par Direktīvas 95/46/EK 26. panta 1. punkta piemērošanu²⁴. Tajos ir vairāki labas prakses noteikumi, kas paredzēti, lai datu aizsardzības iestādes varētu veikt izpildes pasākumus²⁵. Proti, darba grupa ierosina, ka personas datu pārsūtīšana, ko varētu klasificēt kā atkārtotu, masveida vai strukturālu pārsūtīšanu, būtu jāveic, nodrošinot pietiekamas garantijas, un, ja iespējams,

²² Tas var ietvert, piemēram, datu pārsūtīšanu starp nodokļu vai muitas iestādēm vai starp kompetentajiem dienestiem sociālā nodrošinājuma jautājumos (sk. Direktīvas 95/46/EK 58. apsvērumu). Arī pārsūtīt datus starp finanšu pakalpojumu nozares uzraudzības iestādēm, var izmantot atkāpi. Sk. 29. panta darba grupa, “*Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*” (WP 12), 1998. gada 24. jūlijs, 25. lpp.

²³ 29. panta darba grupa, “Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta piemērošanu” (WP 114), 2005. gada 25. novembris, 7. un 17. lpp.

²⁴ 29. panta darba grupa, “*Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*” (WP 12), 1998. gada 24. jūlijs; “Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta piemērošanu” (WP 114), 2005. gada 25. novembris. Sk. arī Eiropas Komisija, “*Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries*” (FAQ D.1–D.9), 48.–54. lpp.

²⁵ 29. panta darba grupa, “Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta piemērošanu” (WP 114), 2005. gada 25. novembris, 8.–10. lpp.

piemērojot konkrētu tiesisko regulējumu, piemēram, līguma standartklauzulas vai saistošos uzņēmuma noteikumus²⁶.

Šajā paziņojumā Komisija aplūkos tikai tās atkāpes, kas īpaši attiecas uz datu pārsūtīšanu komerciālos nolūkos, ņemot vērā slēdzienu, ka Lēmums par drošības zonu nav spēkā.

2.3.1. Pārsūtīšana, kas vajadzīga, lai izpildītu līgumu vai lai īstenotu pēc datu subjekta pieprasījuma veiktos pasākumus, kuriem seko līguma noslēgšana [26. panta 1. punkta b) apakšpunkts]

Šo atkāpi varētu piemērot, piemēram, saistībā ar viesnīcas rezervāciju vai, pārsūtot maksājuma informāciju uz trešo valsti, lai veiktu bankas pārskaitījumu. Tomēr 29. panta darba grupa uzskata, ka katrā no šiem gadījumiem jābūt “ciešai un būtiskai saistībai”, “tiešai un objektīvai saiknei” starp datu subjektu un līguma nolūku vai līguma noslēgšanas pasākumu (nepieciešamības pārbaude)²⁷. Atkāpi nevar piemērot, lai pārsūtītu papildu informāciju, kas nav nepieciešama pārsūtīšanas nolūkam, vai lai pārsūtīšanu veiktu citā nolūkā, kas nav saistīts ar līguma izpildi (piemēram, pēckontrole pēc laišanas tirgū)²⁸. Attiecībā uz līguma noslēgšanas pasākumiem 29. panta darba grupa uzskatīja, ka šajā gadījumā atkāpi var piemērot tikai saziņai, ko ierosinājis datu subjekts (piemēram, pieprasot informāciju par konkrēto pakalpojumu), nevis saziņai, kas izriet no datu apstrādātāja tirgus paņēmieniem²⁹.

2.3.2. Datu pārsūtīšana, kas vajadzīga līguma noslēgšanai starp datu apstrādātāju un trešajām personām datu subjekta interesēs vai šāda līguma izpildei [26. panta 1. punkta c) apakšpunkts]

Šo atkāpi varētu piemērot, piemēram, ja, veicot starptautisku bankas pārvedumu, datu subjekts ir ieinteresētā persona vai ceļojumu aģents pārsūta informāciju lidsabiedrībai par lidojuma rezervāciju. Arī šajā gadījumā veic nepieciešamības pārbaudi, un ir vajadzīga cieša un būtiska saikne starp datu subjekta interesēm un līguma nolūku.

2.3.3. Datu pārsūtīšana, kas vajadzīga vai ir likumīgi prasīta juridisku prasību pamatojumam, realizācijai vai aizstāvībai [26. panta 1. punkta d) apakšpunkts]

²⁶ 29. panta darba grupa, “Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta piemērošanu” (WP 114), 2005. gada 25. novembris, 9. lpp. Darba grupa uzskata, ka masveida vai atkārtotu datu pārsūtīšanu, izmantojot atkāpi, var veikt tikai tad, ja praktiski nav iespējams izmantot līguma standartklauzulas vai saistošos uzņēmuma noteikumus un ja datu subjektu risks ir niecīgs (piemēram, starptautiskie naudas pārvedumi). Sk. arī Eiropas Komisija, “*Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries*” (FAQ D.1), 49. lpp.

²⁷ 29. panta darba grupa, “Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta piemērošanu” (WP 114), 2005. gada 25. novembris, 13. lpp. Sk. arī “*Opinion 6/2002 on transmission of passenger manifest information and other data from airlines to the United States*” (Atzinums 6/2002 par aviosabiedrību pasažieru un ekipāžas locekļu datu un citu datu pārsūtīšanu Amerikas Savienotajām Valstīm) (WP 66), 2002. gada 24. oktobris.

²⁸ 29. panta darba grupa, “*Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*” (WP 12), 1998. gada 24. jūlijs, 24. lpp.; “Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta piemērošanu” (WP 114), 2005. gada 25. novembris, 13. lpp.

²⁹ 29. panta darba grupa, “*Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*” (WP 12), 1998. gada 24. jūlijs, 24. lpp.

Šo atkāpi varētu piemērot, piemēram, ja uzņēmumam jāpārsūta dati, lai aizstāvētos pret juridisku prasību vai iesniegtu šādu prasību tiesai vai iestādei. Tāpat kā attiecībā uz iepriekšējām divām atkāpēm jāveic nepieciešamības pārbaude:³⁰ šajā gadījumā jābūt ciešai saistībai ar tiesas procesu vai tiesvedību (arī administratīvo).

29. panta darba grupa uzskata, ka atkāpi var piemērot tikai tad, ja ievēroti visi starptautiskie noteikumi par sadarbību civillietās un krimināllietās, kas regulē attiecīgo datu pārsūtīšanas veidu, jo īpaši noteikumi, kuri izriet no 1970. gada 18. marta Hāgas Konvencijas (“Konvencija par pierādījumu iegūšanu”)³¹.

2.3.4. Datu subjekta viennozīmīga iepriekšēja piekrišana ierosinātajai datu pārsūtīšanai [26. panta 1. punkta a) apakšpunkts]

Lai gan datus var pārsūtīt, pamatojoties uz piekrišanu, būtu jāņem vērā vairāki apsvērumi. Tā kā “ierosinātajai datu” pārsūtīšanai jāsaņem piekrišana, ir vajadzīga iepriekšēja piekrišana konkrētajai datu pārsūtīšanai (vai konkrētajai datu pārsūtīšanas kategorijai). Prasot sniegt piekrišanu tiešsaistē, 29. panta darba grupa iesaka izmantot lodziņus, kas jāatzīmē (nevis jau iepriekš atzīmētus lodziņus)³². Tā kā piekrišanai jābūt viennozīmīgai, ja radīsies šaubas par to, vai piekrišana faktiski ir sniegta, atkāpi nedrīkstēs piemērot. Tāpēc, iespējams, daudzas situācijas, kurās tiek pieņemts, ka piekrišana ir sniegta (piemēram, ka personai ir paziņots par datu pārsūtīšanu un tā nav iebildusi), nevarēs izmantot. Toties atkāpi varētu izmantot gadījumos, kad struktūra, kas nosūta datus, tieši sazinās ar datu subjektu un var viegli sniegt vajadzīgo informāciju un saņemt viennozīmīgu piekrišanu³³.

Turklāt saskaņā ar Direktīvas 95/46/EK 2. panta h) apakšpunktu piekrišanai jābūt brīvprātīgi sniegtai, konkrētai un pamatotai. 29. panta darba grupa uzskata — pirmā prasība nozīmē, ka, izdarot “spiedienu”, piekrišana zaudē spēku. Jo īpaši būtiski tas ir saistībā ar nodarbinātību, kur darba ņēmēju padotības un atkarīgā stāvokļa dēļ piekrišanas pamatotība parasti būs apšaubāma³⁴. Vispārīgi runājot, piekrišanu, ko sniedzis datu subjekts, kuram nav bijusi īsta izvēles iespēja vai kurš nostādīts fakta priekšā, nevar uzskatīt par derīgu³⁵.

³⁰ 29. panta darba grupa, “Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta piemērošanu” (WP 114), 2005. gada 25. novembris, 15. lpp. Piemēram, saistībā ar nodarbinātību atkāpi nevar izmantot, lai nākotnē iespējamās tiesvedības vajadzībām pārsūtītu visas datnes par darba ņēmēju uz grupas mātesuzņēmumu, kas reģistrēts trešā valstī.

³¹ Hāgas Konvencija par pierādījumu iegūšanu ārvalstīs civillietās vai komercietās, *atvērta parakstīšanai* 1970. gada 18. martā, 23 U.S.T. 2555, 847 U.N.T.S. 241. Šajā konvencijā aplūkoti gadījumi saistībā ar pirmstiesas izmeklēšanu vai vienas valsts tiesu iestādes pieprasījums citas valsts kompetentajai iestādei iegūt pierādījumus izmantošanai tiesvedībā valstī, kas iesniegusi šādu pieprasījumu.

³² 29. panta darba grupa, “Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta piemērošanu” (WP 114), 2005. gada 25. novembris, 10. lpp., atsaucoties uz “*Opinion 5/2004 on unsolicited direct marketing communications under Article 13 of Directive 2002/58/EC*” (Atzinums 5/2004 par nepasūtītas tiešās reklāmas paziņojumiem saskaņā ar Direktīvas 2002/58/EK 13. pantu) (WP 90), 2004. gada 27. februāris, 3.2. punkts.

³³ 29. panta darba grupa, “*Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*” (WP 12), 1998. gada 24. jūlijs, 24. lpp.

³⁴ 29. panta darba grupa, “*Opinion 8/2001 on the processing of personal data in the employment context*” (Atzinums 8/2001 par personas datu apstrādi saistībā ar nodarbinātību) (WP 48), 2001. gada 13. septembris, 3., 23. un 26. lpp. Darba grupa uzskata, ka piekrišanas pamatota izmantošana būtu jāierobežo, iekļaujot tikai

Būtiski svarīga ir datu subjektu pienācīga iepriekšēja informēšana par datu iespējamu pārsūtīšanu ārpus ES, norādot trešo valsti, uz kuru dati tiks sūtīti, kā arī apstākļus, kādos notiks sūtīšana (sūtīšanas nolūks, saņēmēja(-u) identitāte un kontaktinformācija utt.). Šajā informācijā būtu jānorāda konkrētais risks, kas saistīts ar attiecīgās personas datu pārsūtīšanu uz trešo valsti, kurā nav nodrošināta pietiekama aizsardzība³⁶. Turklāt, kā norādījusi 29. panta darba grupa, datu subjektam atsaucot piekrišanu, lai gan tas nav iespējams ar atpakaļejošu spēku, faktiski būtu jāpārtrauc turpmākā personas datu apstrāde³⁷. Ņemot vērā šos ierobežojumus, 29. panta darba grupa uzskata — ir maz ticams, ka piekrišana būs piemērota ilgtermiņa sistēma, ko datu apstrādātāji varēs izmantot datu strukturālai pārsūtīšanai³⁸.

2.4. Personas datu pārsūtīšanai izmantojamo alternatīvo pamatojumu apkopojums

No minētā izriet, ka uzņēmumi var izmantot dažādus alternatīvus risinājumus, lai veiktu starptautisku datu pārsūtīšanu uz trešām valstīm, kuras nenodrošina pieņemamu aizsardzības līmeni Direktīvas 95/46/WSEK 25. panta 2. punkta nozīmē. Pēc sprieduma pasludināšanas *Schrems* lietā 29. panta darba grupa jo īpaši precizēja, ka datu pārsūtīšanai uz ASV var izmantot līguma standartklauzulas un saistošos uzņēmuma noteikumus, kamēr tā turpinās savu novērtējumu un, neskarot DAI pilnvaras izmeklēt konkrētus gadījumus³⁹. Savukārt nozare atšķirīgi reaģēja uz spriedumu, tostarp attiecībā uz alternatīvo risinājumu izmantošanu savu datu pārsūtīšanai⁴⁰.

Tomēr jāuzsver divi svarīgi nosacījumi. Pirmkārt, būtu jāatgādina, ka, neraugoties uz izmantoto konkrēto juridisko pamatu, datu pārsūtīšanu uz trešo valsti var likumīgi veikt tikai tad, ja datus sākotnēji ir apkopojis un tālāk apstrādājis ES reģistrēts datu apstrādātājs atbilstīgi piemērojamiem valsts tiesību aktiem, kuros transponēta Direktīva 95/46/EK. Direktīvā ir skaidri noteikts, ka, veicot datu apstrādi pirms pārsūtīšanas un veicot pārsūtīšanu, pilnībā jāievēro dalībvalstu noteikumi, kas pieņemti saskaņā ar pārējiem Direktīvas noteikumiem⁴¹.

gadījumus, kad darba ņēmējam patiešām bijusi izvēles iespēja un tāpēc viņš attiecīgi spēj atsaukt piekrišanu, sev nekaitējot. Sk. arī 29. panta darba grupa, "Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta piemērošanu" (WP 114), 2005. gada 25. novembris, 11. lpp.

³⁵ 29. panta darba grupa, "Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta piemērošanu" (WP 114), 2005. gada 25. novembris, 11. lpp. Sk. arī "Opinion 6/2002 on transmission of passenger manifest information and other data from airlines to the United States" (WP 66), 2002. gada 24. oktobris.

³⁶ 29. panta darba grupa, "Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" (WP 12), 1998. gada 24. jūlijs, 24. lpp.

³⁷ 29. panta darba grupa, "Opinion 15/2011 on the definition of consent" (Atzinums 15/2011 par termina "piekrišana" definīciju) (WP 187), 2011. gada 13. jūlijs, 9. lpp.

³⁸ 29. panta darba grupa, "Darba dokuments par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta piemērošanu" (WP 114), 2005. gada 25. novembris, 11. lpp.

³⁹ Sk. 29. panta darba grupas 2015. gada 16. oktobra paziņojumu (8. zemspītras piezīme iepriekš).

⁴⁰ Vairāki starptautiski uzņēmumi paziņoja, ka savu datu pārsūtīšanu uz ASV pamatos ar alternatīviem līdzekļiem. Sk., piemēram, *Microsoft* (<http://blogs.microsoft.com/on-the-issues/2015/10/06/a-message-to-our-customers-about-eu-us-safe-harbor/>) vai *Salesforce* paziņojumu

(<http://www.salesforce.com/company/privacy/data-processing-addendum-faq.jsp>). Citi ASV uzņēmumi, piemēram, *Oracle*, sacīja, ka viņi mākonpakalpojumu klientiem piedāvā iespēju glabāt savus datus Eiropā, tādējādi tie netiek nosūtīti glabāšanai citur: <http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505?mode=print&ot=example.AjaxPageLayout.ot>

⁴¹ Sk. Direktīvas 95/46/EEK 60. apsvērumu un 25. panta 1. punktu.

Otrkārt, gadījumos, kad Komisija nav konstatējusi atbilstību, datu apstrādātājiem jānodrošina, lai viņu veiktā datu pārsūtīšana notiktu ar pietiekamām garantijām atbilstīgi Direktīvas 26. panta 2. punktam. Šis novērtējums jāveic, ņemot vērā visus apstākļus, kas attiecas uz konkrēto pārsūtīšanas gadījumu. Proti, gan līguma standartklauzulās, gan saistošajos uzņēmuma noteikumos paredzēts, ja datu saņēmējam ir pamats uzskatīt, ka saņēmēja valstī piemērojamie tiesību akti var liegt viņam pildīt savus pienākumus, viņam nekavējoties jāinformē datu nosūtītājs ES. Šādā situācijā datu nosūtītājam jāapsver iespēja piemērot atbilstīgus pasākumus, kas vajadzīgi, lai nodrošinātu personas datu aizsardzību⁴². Šie pasākumi var būt tehniski, organizatoriski, saistīti ar uzņēmējdarbības modeli, juridiski vai pasākumi⁴³ nolūkā pārtraukt datu pārsūtīšanu vai izbeigt līguma darbību. Ņemot vērā visus datu pārsūtīšanas apstākļus, varētu būt gadījumi, kad datu nosūtītājiem nolūkā izpildīt Direktīvas 26. panta 2. punkta prasības, jāievieš papildu garantijas, lai papildinātu piemērojamā datu pārsūtīšanas juridiskā pamata nodrošinātās garantijas.

Datu aizsardzības iestādēm, pildot uzraudzības un izpildes pienākumus, galarezultātā šādu prasību ievērošana jānovērtē, izvērtējot katru konkrēto gadījumu, tostarp saistībā ar līgumsaistību un saistošo uzņēmuma noteikumu apstiprināšanu vai izskatot konkrētas sūdzības. Lai gan dažas datu aizsardzības iestādes apšaubīja iespēju transatlantiskajām datu plūsmām izmantot tādus datu pārsūtīšanas instrumentus kā līguma standartklauzulas un saistošie uzņēmuma noteikumi⁴⁴, savā paziņojumā, ko izdeva pēc sprieduma pasludināšanas *Schrems* lietā, 29. panta darba grupa paziņoja, ka turpinās analizēt sprieduma ietekmi uz citiem datu pārsūtīšanas instrumentiem⁴⁵. Tas neskar DAI pilnvaras izmeklēt konkrētus gadījumus un nodrošināt fizisku personu aizsardzību.

3. SPRIEDUMA *SCHREMS* LIETĀ IETEKME UZ LĒMUMIEM PAR ATBILSTĪBU

Tiesa savā spriedumā neapstrīdēja Direktīvas 95/46/EK 25. panta 6. punktā Komisijai piešķirtās pilnvaras konstatēt, ka trešā valsts nodrošina pietiekamu aizsardzības līmeni, ja vien tā ievēro Tiesas noteiktā prasības. Saskaņā ar šīm prasībām 2012. gada priekšlikumā

⁴² Sk., piemēram, Komisijas Lēmuma 2010/87/EU pielikuma 5. punktu un 29. panta darba grupas dokumentu "*Document setting up a framework for the structure of Binding Corporate Rules*" (WP 154), 2008. gada 24. jūnijs, 8. lpp.

⁴³ Sk., piemēram, Eiropas Savienības Tīklu un informācijas drošības aģentūras (ENISA) izdotos norādījumus: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf.

⁴⁴ Sk., piemēram, Vācijas federālo un federālo zemju datu aizsardzības iestāžu 2015. gada 26. oktobra Datu aizsardzības konferences nostājas dokumentu: <https://www.datenschutz.hessen.de/ft-europa.htm#entry4521>. Uzsverot, ka spriedumā *Schrems* lietā ir "stingras būtiskas prasības", kuras jāievēro gan Komisijai, gan DAI, nostājas dokumentā norādīts, ka Vācijas datu aizsardzības iestādes novērtēs, vai ir likumīga datu pārsūtīšana, kas veikta, izmantojot alternatīvus risinājumus (LSK, SUN), un vairs nepiešķirs jaunu atļauju šo līdzekļu izmantošanai. Papildus minētajam dažas Vācijas DAI skaidri brīdinājušas, ka alternatīviem pārsūtīšanas līdzekļiem tiks veikta rūpīga juridiska pārbaude. Sk., piemēram, nostājas dokumentus, ko izdevušas Šlēzviņas-Holšteinas DAI: <https://www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judgment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,-C-36214.html> un Reinzemes-Pfalcas DAI: https://www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuG_H-Urteil_Safe_Harbor.pdf.

⁴⁵ Sk. 29. panta darba grupas 2015. gada 16. oktobra paziņojumu (8. zemspējas piezīme iepriekš).

Vispārīgās datu aizsardzības regulai⁴⁶, ar ko paredzēts aizstāt Direktīvu 95/46/EK, ir precizēti un sīkāk izstrādāti nosacījumi, saskaņā ar kuriem var pieņemt lēmumus par atbilstību. Spriedumā *Schrems* lietā Tiesa arī precizēja — ja Komisija pieņem lēmumu par atbilstību, tas ir saistošs visām dalībvalstīm un to iestādēm, tostarp datu aizsardzības iestādēm, līdz brīdim, kad Tiesa, kurai ir ekskluzīva kompetence šajā ziņā, to ir atcēlusi, anulējusi vai atzinusi par spēkā neesošu. DAI joprojām ir tiesības pārbaudīt Direktīvas 95/46/EK 28. panta 4. punkta nozīmē iesniegtās prasības attiecībā uz datu pārsūtīšanas atbilstību prasībām, kas noteiktas Direktīvā (saskaņā ar Tiesas interpretāciju), taču tās nevar pieņemt galīgo slēdzienu. Dalībvalstīm drīzāk jānodrošina iespēja iesniegt lietu izskatīšanai valsts tiesā, kas savukārt var ierosināt Tiesas jurisdikciju, lūdzot Tiesu sniegt prejudiciālu nolēmumu saskaņā ar Līguma par Eiropas Savienības darbību (LESD) 267. pantu.

Turklāt Tiesa skaidri apstiprināja, ka trešās valsts izmantotais pašsertifikācijas process (kā arī privātuma drošības zonas principu gadījumā) neizslēdz lēmumu par atbilstību saskaņā ar Direktīvas 95/46/EK 25. panta 6. punktu, kamēr ir efektīvi konstatēšanas un uzraudzības mehānismi, kas nodrošina iespēju praktiski atklāt un sodīt jebkādas datu aizsardzības noteikumu pārkāpumus.

Tā kā Lēmumā par drošības zonu šajā ziņā nav pietiekamu slēdzienu, Tiesa atzina šo lēmumu par spēkā neesošu. Tāpēc ir skaidrs, ka datu pārsūtīšanu starp ES un Amerikas Savienotajām Valstīm vairs nevar veikt, izmantojot šo pamatojumu, t. i., tikai atsaucoties uz privātuma drošības zonas principu ievērošanu. Tā kā datu pārsūtīšana uz trešo valsti, kura nenodrošina pietiekamu aizsardzības līmeni (vai vismaz, ja to nav konstatējusi Komisija, pieņemot lēmumu saskaņā ar Direktīvas 95/46/EK 25. panta 6. punktu) faktiski ir aizliegta⁴⁷, tā būs likumīga tikai tad, ja datu nosūtītājs varēs pamatoti izmantot vienu no alternatīvajiem risinājumiem, kas aprakstīti 2. sadaļā iepriekš. Ja nav lēmuma par atbilstību, datu nosūtītājam, ko uzrauga DAI, jānodrošina, ka attiecībā uz konkrēto datu pārsūtīšanas gadījumu ir izpildīti minētā(-o) risinājuma(-u) izmantošanas nosacījumi.

Sprieduma piemērošanas joma attiecas tikai uz Komisijas Lēmumu par drošības zonu. Tomēr katrā no pārējiem lēmumiem par atbilstību⁴⁸ ir ierobežotas DAI pilnvaras, kas atbilst 3. pantam Lēmumā par drošības zonu, kuru Tiesa atzinusi par spēkā neesošu⁴⁹. Tagad Komisija no sprieduma izdarīs vajadzīgos secinājumus, drīzumā sagatavojot lēmumu, kas jāpieņem saskaņā ar piemērojamo komiteju procedūru, aizstājot šo noteikumu visos spēkā

⁴⁶ Eiropas Komisija, Priekšlikums Eiropas Parlamenta un Padomes Regulai par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (Vispārīgā datu aizsardzības regula). Sk. arī Eiropas Parlaments, 2014. gada 12. marta normatīvo rezolūcija par priekšlikumu Eiropas Parlamenta un Padomes regulai par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (Vispārīgā datu aizsardzības regula), COM(2012)0011 – C7-0025/2012 – 2012/0011(COD); Padome, Priekšlikums Eiropas Parlamenta un Padomes Regulai par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (Vispārīgā datu aizsardzības regula), vispārējas pieejas sagatavošana, 9565/15. Patlaban priekšlikums ir likumdošanas procesa noslēguma posmā.

⁴⁷ Skatīt Direktīvas 95/46/EK 57. apsvērumu.

⁴⁸ Patlaban lēmumi par atbilstību ir pieņemti attiecībā uz šādām valstīm: Andora, Argentīna, Džērsija, Fēru salas, Gērsija, Izraēla, Jaunzēlande, Kanāda, Menas sala, Šveice un Urugvaja. Sk.: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

⁴⁹ Sk. sprieduma *Schrems* lietā 99.–104. punktu.

esošajos lēmumos par atbilstību. Komisija arī regulāri novērtēs esošos un nākamos lēmumus par atbilstību, tostarp regulāri izvērtējot visu šo lēmumu darbību kopā ar attiecīgās trešās valsts kompetentajām iestādēm.

4. SECINĀJUMS

Kā apstiprinājusi 29. panta darba grupa, uzņēmumi joprojām likumīgai datu pārsūtīšanai uz tādām trešām valstīm kā Amerikas Savienotās Valstis var izmantot alternatīvus risinājumus, ar kuriem atļauj nosūtīt datu plūsmas. Tomēr Komisija uzskata, ka joprojām galvenā prioritāte ir atjaunināta un stabila sistēma personas datu pārsūtīšanai uz Amerikas Savienotajām Valstīm. Šāda sistēma ir visaptverošākais risinājums, kas efektīvi turpina Eiropas iedzīvotāju personas datu aizsardzību, pārsūtot šos datus uz Amerikas Savienotajām Valstīm. Tā nodrošina arī labāko risinājumu transatlantiskai tirdzniecībai, jo piedāvā vienkāršāku mehānismu, kas nerada lieku slogu un tāpēc ir izdevīgāks izmaksu ziņā, jo īpaši MVU.

Jau 2013. gadā Komisija sāka sarunas ar ASV valdību par jaunu transatlantiskās datu pārsūtīšanas kārtību, pamatojoties uz Komisijas 13. ieteikumiem⁵⁰. Ir panākts ievērojams progress, apvienojot abu pušu uzskatus, piemēram, par to, ka attiecīgi ASV Tirdzniecības ministrijai un ASV Federālā tirdzniecības komisijai stingrāk jāuzrauga un jāīsteno privātuma drošības zonas principi, par labāku pārredzamību patērētājiem saistībā ar viņu tiesībām uz datu aizsardzību, vieglākām un lētākām tiesiskās aizsardzības iespējām sūdzību gadījumos un skaidrākiem noteikumiem par datu pārsūtīšanu no uzņēmumiem, kas ievēro drošības zonas principus, uz uzņēmumiem, kuri neievēro drošības zonas principus (piemēram, apstrādes vai tālākas apstrādes nolūkā). Tagad, kad Lēmums par drošības zonu atzīts par spēkā neesošu, Komisija ir pasteidzinājusi sarunas ar ASV valdību, lai nodrošinātu Tiesas formulēto juridisko prasību ievērošanu. Komisija vēlas pabeigt šīs diskusijas un sasniegt šo mērķi trīs mēnešos.

Līdz brīdim, kad būs izstrādāta atjauninātā transatlantiskā sistēma, uzņēmumiem ir pamatoti jāizmanto pieejamie alternatīvie datu pārsūtīšanas risinājumi. Tomēr, izmantojot šo iespēju, datu nosūtītājiem jāpilda savi pienākumi DAI uzraudzībā.

Pretēji situācijai, kad Komisija bija konstatējusi, ka trešā valsts nodrošina pietiekamu datu aizsardzības līmeni, ko datu nosūtītāji var pamatoti izmantot datu pārsūtīšanai no ES, izmantojot alternatīvos līdzekļus, datu nosūtītājiem joprojām jāpārbauda, vai personas dati tiek efektīvi aizsargāti. Šī pārbaude vajadzības gadījumā var ietvert arī atbilstīgus pasākumus.

Šajā ziņā DAI ir galvenā loma. Būdamas datu subjektu pamattiesību galvenās īstenotājas, datu aizsardzības iestādes atbild par datu, kas tiek sūtīti no ES uz trešām valstīm, pārsūtīšanas uzraudzību un ir pilnvarotas šo uzraudzību īstenot pilnīgi neatkarīgi. Komisija aicina datu apstrādātājus sadarboties ar DAI, palīdzot tām efektīvi pildīt uzraudzības uzdevumu. Komisija turpinās ciešu sadarbību ar 29. panta darba grupu, lai nodrošinātu ES datu aizsardzības tiesību aktu vienveidīgu piemērošanu.

⁵⁰ Sk. 4. zemsvītras piezīmi iepriekš.