Judikatūras krājums

TIESAS SPRIEDUMS (virspalāta)

2020. gada 16. jūlijā *

Lūgums sniegt prejudiciālu nolēmumu – Fizisko personu aizsardzība attiecībā uz personas datu apstrādi – Eiropas Savienības Pamattiesību harta – 7., 8. un 47. pants – Regula (ES) 2016/679 – 2. panta 2. punkts – Piemērojamība – Personas datu pārsūtīšana trešajām valstīm komerciāliem mērķiem – 45. pants – Komisijas lēmums par aizsardzības līmeņa pietiekamību – 46. pants – Pārsūtīšana, kurai piemērojamas atbilstošas garantijas – 58. pants – Uzraudzības iestāžu pilnvaras – Datu, kurus trešās valsts publiskās iestādes pārsūta valsts drošības nolūkos, apstrāde – Trešajā valstī nodrošinātā aizsardzības līmeņa pietiekamības vērtējums – Lēmums 2010/87/ES – Standartklauzulas attiecībā uz personas datu pārsūtīšanu uz trešajām valstīm – Pārziņa sniegtās atbilstošās garantijas – Spēkā esamība – Īstenošanas lēmums (ES) 2016/1250 – Eiropas Savienības un Amerikas Savienoto Valstu privātuma vairoga nodrošinātās aizsardzības pietiekamība – Spēkā esamība – Fiziskas personas sūdzība, kuras dati ir tikuši pārsūtīti no Eiropas Savienības uz ASV

Lietā C-311/18

par lūgumu sniegt prejudiciālu nolēmumu atbilstoši LESD 267. pantam, ko *High Court* (Augstā tiesa, Īrija) iesniedza ar lēmumu, kurš pieņemts 2018. gada 4. maijā un kurš Tiesā reģistrēts 2018. gada 9. maijā, tiesvedībā

Data Protection Commissioner

pret

Facebook Ireland Ltd,

Maximilian Schrems,

piedaloties:

The United States of America,

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

* Tiesvedības valoda – angļu.

TIESA (virspalāta)

šādā sastāvā: priekšsēdētājs K. Lēnartss [*K. Lenaerts*], priekšsēdētāja vietniece R. Silva de Lapuerta [*R. Silva de Lapuerta*], palātu priekšsēdētāji A. Arabadžijevs [*A. Arabadjiev*], A. Prehala [*A. Prechal*], M. Vilars [*M. Vilaras*], M. Safjans [*M. Safjan*], S. Rodins [*S. Rodin*], P. Dž. Švīrebs [*P. G. Xuereb*], L. S. Rosi [*L. S. Rossi*] un I. Jarukaitis [*I. Jarukaitis*], tiesneši M. Ilešičs [*M. Ilešič*], T. fon Danvics [*T. von Danwitz*] (referents) un D. Švābi [*D. Šváby*],

ģenerāladvokāts: H. Saugmandsgors Ē [*H. Saugmandsgaard Øe*],

sekretāre: S. Stremholma [*C. Strömholm*], administratore,

ņemot vērā rakstveida procesu un 2019. gada 9. jūlija tiesas sēdi,

ņemot vērā apsvērumus, ko sniedza:

– *Data Protection Commissioner* vārdā – *D. Young, solicitor, B. Murray* un *M. Collins, SC,* kā arī *C. Donnelly, BL,*

– *Facebook Ireland Ltd* vārdā – *P. Gallagher* un *N. Hyland, SC, A. Mulligan* un *F. Kieran, BL,* kā arī *P. Nolan, C. Monaghan, C. O'Neill* un *R. Woulfe, solicitors,*

– *M. Schrems* vārdā – *H. Hofmann, Rechtsanwalt, E. McCullough, J. Doherty* un *S. O'Sullivan, SC,* kā arī *G. Rudden, solicitor,*

– *The United States of America* vārdā – *E. Barrington, SC, S. Kingston, BL,* kā arī *S. Barton* un *B. Walsh, solicitors,*

– *Electronic Privacy Information Centre* vārdā – *S. Lucey, solicitor, G. Gilmore* un *A. Butler, BL,* kā arī *C. O'Dwyer, SC,*

– *BSA Business Software Alliance Inc.* vārdā – *B. Van Vooren* un *K. Van Quathem, advocaten,*

– *Digitaleurope* vārdā – *N. Cahill, barrister, J. Cahir, solicitor,* un *M. Cush, SC,*

– Īrijas vārdā – *A. Joyce* un *M. Browne,* pārstāvji, kuriem palīdz *D. Fennelly, BL,*

– Beļģijas valdības vārdā – *J.-C. Halleux* un *P. Cottin,* pārstāvji,

– Čehijas valdības vārdā – *M. Smolek, J. Vláčil* un *O. Serdula,* kā arī *A. Kasalická,* pārstāvji,

– Vācijas valdības vārdā – *J. Möller, D. Klebs* un *T. Henze,* pārstāvji,

– Francijas valdības vārdā – *A.-L. Desjonquères,* pārstāve,

– Nīderlandes valdības vārdā – *C. S. Schillemans, K. Bulterman* un *M. Noort,* pārstāves,

– Austrijas valdības vārdā – *J. Schmoll* un *G. Kunnert,* pārstāvji,

– Polijas valdības vārdā – *B. Majczyna,* pārstāvis,

– Portugāles valdības vārdā – *L. Inez Fernandes,* kā arī *A. Pimenta* un *C. Vieira Guerra,* pārstāvji,

– Apvienotās Karalistes valdības vārdā – *S. Brandon*, pārstāvis, kuram palīdz *J. Holmes*, *QC*, un *C. Knight*, *barrister*,

– Eiropas Parlamenta vārdā – *M. J. Martínez Iglesias* un *A. Caiola*, pārstāvji,

– Eiropas Komisijas vārdā – *D. Nardi*, *H. Krämer* un *H. Kranenborg*, pārstāvji,

– Eiropas Datu aizsardzības kolēģijas (EDAK) vārdā – *A. Jelinek* un *K. Behn*, pārstāvji,

noklausījusies ģenerāladvokāta secinājumus 2019. gada 19. decembra tiesas sēdē,

pasludina šo spriedumu.

Spriedums

1 Lūgums sniegt prejudiciālu nolēmumu būtībā ir par

– Eiropas Parlamenta un Padomes Direktīvas 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV 1995, L 281, 31. lpp.) 3. panta 2. punkta pirmā ievilkuma, 25. un 26. panta, kā arī 28. panta 3. punkta, skatot kopā ar LES 4. panta 2. punktu un Eiropas Savienības Pamattiesību hartas (turpmāk tekstā – "Harta") 7., 8. un 47. pantu, interpretāciju,

– Komisijas Lēmuma 2010/87/ES (2010. gada 5. februāris) par līguma standartklauzulām attiecībā uz personas datu pārsūtīšanu trešās valstīs reģistrētiem apstrādātājiem saskaņā ar [Direktīvu 95/46] (OV 2010, L 39, 5. lpp.), kurā grozījumi izdarīti ar Komisijas Īstenošanas lēmumu (ES) 2016/2297 (2016. gada 16. decembris) (OV 2016, L 344, 100. lpp.) (turpmāk tekstā – "LSK lēmums"), interpretāciju un spēkā esamību, kā arī

– Komisijas Īstenošanas lēmuma (ES) 2016/1250 (2016. gada 12. jūlijs) saskaņā ar [Direktīvu 95/46] par pienācīgu aizsardzību, ko nodrošina ES un ASV privātuma vairogs (OV 2016, L 207, 1. lpp.; turpmāk tekstā – "PV lēmums"), interpretāciju un spēkā esamību.

2 Šis lūgums ir iesniegts tiesvedībā starp *Data Protection Commissioner* (Datu aizsardzības komisārs, Īrija) (turpmāk tekstā – "komisārs"), no vienas puses, un *Facebook Ireland Ltd* un *Maximillian Schrems*, no otras puses, par viņa iesniegto sūdzību par *Facebook Ireland* īstenoto personas datu pārsūtīšanu *Facebook Inc.* uz Amerikas Savienotajām Valstīm.

Atbilstošās tiesību normas

Direktīva 95/46

3 Direktīvas 95/46 3. panta "Darbības joma" 2. punktā bija paredzēts:

"Šī direktīva neattiecas uz personas datu apstrādi:

– tādu pasākumu gaitā, uz kuru neattiecas Kopienas tiesību akti, kā Līguma par Eiropas Savienību V un VI sadaļā paredzētie pasākumi un, jebkurā gadījumā, uz apstrādes operācijām attiecībā uz sabiedrības drošību, aizsardzību, valsts drošību (ieskaitot valsts ekonomisko labklājību, ja apstrādes operācija attiecas uz valsts drošības jautājumiem) un uz valsts pasākumiem krimināltiesību jomā;

[..]."

4 Šīs direktīvas 25. pantā bija noteikts:

"1. Dalībvalstis paredz to, ka personas datu [..] pārsūtīšana var notikt tikai tad, ja, neierobežojot atbilstību attiecīgās valsts noteikumiem, kuri pieņemti saskaņā ar šīs direktīvas pārējiem noteikumiem, attiecīgā trešā valsts nodrošina pietiekamu aizsardzības līmeni.

2. Trešās valsts sniegtās aizsardzības līmeņa pietiekamība jānovērtē, paturot prātā visus ar datu pārsūtīšanas darbību vai datu pārsūtīšanas darbību kopumu cieši saistītos apstākļus; [..].

[..]

6. Saskaņā ar 31. panta 2. punktā minēto procedūru Komisija var konstatēt, ka trešā valsts nodrošina pietiekamu aizsardzības līmeni šā panta 2. punkta nozīmē, pamatojoties uz savas valsts tiesībām vai uz starptautiskajām saistībām, kuras tā noslēgusi [tā uzņēmusies], jo īpaši uz 5. punktā minēto sarunu par personu privātās dzīves un pamatbrīvību un tiesību aizsardzību atzinumu.

Dalībvalstis veic nepieciešamos pasākumus, lai izpildītu Komisijas lēmumu."

5 Minētās direktīvas 26. panta 2. un 4. punktā bija paredzēts:

"2. Neierobežojot 1. punktu, dalībvalsts var atļaut personas datu pārsūtīšanu vai pārsūtījumu kopumu uz trešo valsti, kura nenodrošina pietiekamu aizsardzības līmeni 25. panta 2. punkta nozīmē, ja personas datu apstrādātājs sniedz atbilstošas garantijas attiecībā uz personu privātās dzīves un pamattiesību un brīvību aizsardzību un attiecībā uz atbilstošo tiesību izmantošanu; šādas garantijas jo īpaši var izrietēt no attiecīgajiem līguma punktiem.

[..]

4. Ja Komisija saskaņā ar 31. panta 2. punktā noteikto procedūru nolemj, ka daži līguma pamatpunkti sniedz pietiekamas garantijas, kā paredzēts 2. punktā, dalībvalstis veic nepieciešamos pasākumus, lai izpildītu Komisijas lēmumu."

6 Saskaņā ar šīs pašas direktīvas 28. panta 3. punktu:

"Katrai iestādei ir piešķirtas:

– izmeklēšanas pilnvaras, tādas kā datu, kuri veido apstrādes darbību priekšmetu, piekļuves pilnvaras un pilnvaras ievākt tās uzraudzības pienākumu izpildei visu vajadzīgo informāciju;

– efektīvas iejaukšanās pilnvaras, tādas kā, piemēram, saskaņā ar 20. pantu atzinumu sniegšana pirms datu apstrādes darbību veikšanas un pilnvaras nodrošināt šādu atzinumu atbilstīgu nodošanu atklātībai, likt noslēgt piekļuvi, dzēst vai iznīcināt datus, noteikt pagaidu vai galīgu aizliegumu datu apstrādei, brīdināt vai izteikt aizrādījumu personas datu apstrādātājam vai nodot jautājumu izskatīšanai valstu parlamentiem vai citām politiskām institūcijām,

– pilnvaras uzsākt procesuālas darbības, ja pārkāpti saskaņā ar šo direktīvu pieņemtie attiecīgās valsts noteikumi[,] vai darīt zināmus šos pārkāpumus tiesu iestādēm.

[..]"

VDAR

7 Direktīva 95/46 tika atcelta un aizstāta ar Eiropas Parlamenta un Padomes Regulu (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] (Vispārīgā datu aizsardzības regula) (OV 2016, L 119, 1. lpp.; turpmāk tekstā – "VDAR").

8 VDAR 6., 10., 101., 103., 104., 107.–109., 114., 116. un 141. apsvērumā ir noteikts:

"(6) Straujā tehnoloģiju attīstība un globalizācija ir radījusi jaunas problēmas personas datu aizsardzības jomā. Personas datu vākšanas un apmaiņas apjoms ir būtiski pieaudzis. Tehnoloģija ļauj gan privātām uzņēmējsabiedrībām, gan publiskām iestādēm vēl nepieredzētā apjomā savas darbības mērķiem izmantot personas datus. Fiziskas personas aizvien biežāk personiska rakstura informāciju dara publiski un globāli pieejamu. Tehnoloģija ir pārveidojusi gan ekonomiku, gan sociālo dzīvi, un tai arī turpmāk būtu jāuzlabo personas datu brīva aprite Savienībā un nosūtīšana uz trešām valstīm un starptautiskām organizācijām, vienlaikus nodrošinot personas datu augsta līmeņa aizsardzību.

[..]

(10) Lai nodrošinātu konsekventu un augsta līmeņa aizsardzību fiziskām personām un novērstu šķēršļus personu datu apritei Savienībā, fiziskas personas tiesību un brīvību aizsardzības līmenim attiecībā uz šādu datu apstrādi visās dalībvalstīs vajadzētu būt vienādam. Visā Savienībā būtu jānodrošina noteikumu par fiziskas personas pamattiesību un brīvību aizsardzību attiecībā uz personas datu apstrādi vienveidīga piemērošana. Attiecībā uz personas datu apstrādi, kuru veic, lai izpildītu juridisku pienākumu, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtas oficiālas pilnvaras, būtu jāļauj dalībvalstīm saglabāt vai ieviest valsts noteikumus, ar ko vēl vairāk precizē šīs regulas noteikumu piemērošanu. Saistībā ar vispārējiem un horizontāliem tiesību aktiem par datu aizsardzību, ar kuriem īsteno Direktīvu 95/46/EK, dalībvalstīm ir vairāki uz konkrētām nozarēm attiecināmi tiesību akti jomās, kurās ir vajadzīgi precīzāki noteikumi. Šajā regulā dalībvalstīm ir arī paredzēta rīcības brīvība precizēt tās noteikumus, tostarp attiecībā uz īpašu kategoriju personas datu ("sensitīvu datu") apstrādi. Šajā ziņā ar šo regulu neizslēdz dalībvalstu tiesību aktus, kuros nosaka konkrētu apstrādes situāciju apstākļus, tostarp precīzāk nosakot apstākļus, kādos personas datu apstrāde ir likumīga.

[..]

(101) Personas datu plūsmas uz valstīm ārpus Savienības un starptautiskām organizācijām un no tām ir vajadzīgas starptautiskās tirdzniecības un starptautiskās sadarbības paplašināšanai. Šīs aprites palielināšanās ir radījusi jaunas problēmas un bažas par personas datu aizsardzību. Taču gadījumos, kad personas dati no Savienības tiek nosūtīti pārziņiem, apstrādātājiem vai citiem saņēmējiem trešās valstīs vai starptautiskām organizācijām, aizsardzības līmenim, ko šī regula nodrošina fiziskām personām Savienībā, nebūtu jāsamazinās, tostarp gadījumos, kad personas dati no trešās valsts vai starptautiskās organizācijas tiek nosūtīti tālāk pārziņiem, apstrādātājiem tajā pašā vai citā trešā valstī vai starptautiskā organizācijā. Jebkurā gadījumā nosūtīt datus uz trešām valstīm un starptautiskām organizācijām var tikai tad, ja tiek pilnībā ievēroti šīs regulas noteikumi. Nosūtīšana varētu notikt tikai tad, ja, ņemot vērā pārējos šīs regulas noteikumus, pārzinis vai apstrādātājs ievēro šīs regulas noteikumus attiecībā uz personas datu nosūtīšanu trešām valstīm vai starptautiskām organizācijām.

[..]

(103) Komisija attiecībā uz visu Savienību var nolemt, ka trešā valsts, teritorija vai konkrēts sektors trešā valstī, vai starptautiska organizācija nodrošina datu aizsardzību pietiekamā līmenī, tādējādi nodrošinot juridisko noteiktību un vienotību visā Savienībā attiecībā uz trešo valsti vai starptautisko organizāciju, par kuru uzskata, ka tā nodrošina šādu aizsardzības līmeni. Šādos gadījumos personas datus uz minēto trešo valsti vai starptautisko organizāciju var nosūtīt bez nepieciešamības saņemt jebkādu turpmāku atļauju. Komisija pēc paziņojuma sniegšanas un pilnvērtīga paziņojuma, kurā izklāstīti iemesli nosūtīšanas trešai valstij vai starptautiskai organizācijai var arī nolemt atsaukt šādu lēmumu.

(104) Saskaņā ar pamatvērtībām, uz kurām balstās Savienība, un jo īpaši cilvēktiesību aizsardzību, Komisijai, novērtējot trešo valsti vai kādu teritoriju vai konkrētu sektoru trešā valstī, būtu jāņem vērā tas, kā konkrēta trešā valsts ievēro tiesiskumu, tiesu pieejamību, kā arī starptautiskās cilvēktiesību normas un standartus, un tās vispārējie un nozaru tiesību akti, tostarp tiesību akti attiecībā uz sabiedrisko drošību, aizsardzību un valsts drošību, kā arī sabiedrisko kārtību un krimināltiesībām. Pieņemot lēmumu par aizsardzības līmeņa pietiekamību kādā teritorijā vai konkrētā nozarē trešā valstī, būtu jāņem vērā skaidri un objektīvi kritēriji, piemēram, konkrētas apstrādes darbības un piemērojamo juridisko standartu un attiecīgajā trešā valstī spēkā esošo tiesību aktu darbības joma. Trešai valstij būtu jāpiedāvā garantijas, kas nodrošina pietiekamu aizsardzības līmeni, kurš pēc būtības ir līdzvērtīgs Savienībā nodrošinātajam, jo īpaši, ja personas datus apstrādā vienā vai vairākos konkrētos sektoros. Trešai valstij jo īpaši būtu jānodrošina efektīva neatkarīga datu aizsardzības uzraudzība un būtu jāparedz sadarbības mehānismi ar dalībvalstu datu aizsardzības iestādēm, un priekš datu subjektiem būtu jāparedz efektīvas un īstenojamas tiesības un efektīva aizsardzība administratīvā kārtā vai tiesā.

[..]

(107) Komisija var atzīt, ka trešā valsts, kāda teritorija vai konkrēts sektors trešā valstī, vai starptautiska organizācija vairs nenodrošina pietiekamu datu aizsardzības līmeni. Līdz ar to personas datu nosūtīšana uz šo trešo valsti vai starptautisko organizāciju būtu jāaizliedz, ja vien nav izpildītas šīs regulas prasības attiecībā uz nosūtīšanu, kam piemēro atbilstošas garantijas, tostarp saistošus uzņēmuma noteikumus, un atkāpēm īpašās situācijās. Šādā gadījumā būtu jāparedz noteikumi par apspriešanās procesu starp Komisiju un šādu trešo valsti vai starptautisko organizāciju. Komisijai būtu laikus jāinformē attiecīgā trešā valsts vai starptautiskā organizācija par iemesliem un jāapspriežas ar to, lai šo situāciju atrisinātu.

(108) Kamēr lēmums par aizsardzības līmeņa pietiekamību nav pieņemts, pārzinim vai apstrādātājam būtu jāveic pasākumi, kas kompensētu datu aizsardzības trūkumus trešā valstī, paredzot atbilstošas garantijas datu subjektam. Šādas atbilstošas garantijas varētu nozīmēt, ka tiek izmantoti saistošie uzņēmuma noteikumi, Komisijas pieņemtās standarta datu aizsardzības klauzulas, uzraudzības iestādes pieņemtās standarta datu aizsardzības klauzulas vai uzraudzības iestādes apstiprinātās līguma klauzulas. Minētajām garantijām būtu jānodrošina, lai tiktu ievērotas datu aizsardzības prasības un datu subjektu tiesības atbilstīgi Savienībā veiktai apstrādei, tostarp īstenojamu datu subjekta tiesību un efektīvu tiesiskās aizsardzības līdzekļu pieejamība, ieskaitot iespēju saņemt efektīvu aizsardzību administratīvā kārtā vai tiesā un pieprasīt kompensāciju Savienībā un trešā valstī. Tiem jo īpaši būtu jāattiecas uz atbilstību vispārīgiem principiem, kuri saistīti ar personas datu apstrādi, un "integrētas datu aizsardzības" un "datu aizsardzības pēc noklusējuma" principiem. [..]

(109) Iespējai, ka pārzinis vai apstrādātājs var izmantot Komisijas vai uzraudzības iestādes pieņemtās standarta datu aizsardzības klauzulas, nebūtu jāizslēdz ne tas, ka pārzinis vai apstrādātājs var iekļaut standarta datu aizsardzības klauzulas plašākā līgumā, piemēram, līgumā starp apstrādātāju un citu apstrādātāju, ne arī tas, ka pārzinis vai apstrādātājs var pievienot citas klauzulas vai papildu garantijas, ar noteikumu, ka tās tieši vai netieši nav pretrunā Komisijas vai

uzraudzības iestādes pieņemtajām līguma standartklauzulām vai neierobežo datu subjekta pamattiesības vai brīvības. Pārziņi un apstrādātāji būtu jāmudina nodrošināt papildu garantijas, izmantojot līgumsaistības, ar kurām papildina standarta aizsardzības klauzulas.

[..]

(114) Jebkurā gadījumā, ja Komisija nav pieņēmusi lēmumu par datu aizsardzības līmeņa pietiekamību trešā valstī, pārzinim vai apstrādātājam būtu jāizmanto risinājumi, kas datu subjektiem sniedz īstenojamas un efektīvas tiesības attiecībā uz viņu datu apstrādi Savienībā arī pēc tam, kad minētie dati ir nosūtīti, lai tādējādi viņi joprojām varētu baudīt savas pamattiesības un garantijas.

[..]

(116) Personas datu pārvietošanās pāri robežām ārpus Savienības var ievērojami apdraudēt fizisko personu spējas īstenot tiesības uz datu aizsardzību, jo īpaši, lai aizsargātos pret nelikumīgu izmantošanu vai šādas informācijas atklāšanu. Vienlaikus uzraudzības iestādes var saskarties ar situāciju, ka tās nevar reaģēt uz sūdzībām vai veikt izmeklēšanu saistībā ar darbībām, kas norisinās robežu otrā pusē. To pūles kopīgi strādāt pārrobežu kontekstā var sarežģīt arī nepietiekamās preventīvās vai korektīvās pilnvaras, tiesisko regulējumu atšķirības un tādi praktiski šķēršļi kā, piemēram, ierobežoti līdzekļi. [..]

[..]

(141) Katram datu subjektam vajadzētu būt tiesībām iesniegt sūdzību vienai uzraudzības iestādei, jo īpaši viņa pastāvīgās dzīvesvietas dalībvalstī, un tiesībām uz efektīvu tiesību aizsardzību tiesā saskaņā ar hartas 47. pantu, ja datu subjekts uzskata, ka viņa tiesības saskaņā ar šo regulu ir pārkāptas, vai ja uzraudzības iestāde nereaģē uz sūdzību, daļēji vai pilnībā noraida sūdzību vai nerīkojas, kad šāda rīcība ir nepieciešama, lai aizsargātu datu subjekta tiesības. [..]"

9 Šīs regulas 2. panta 1. un 2. punktā ir paredzēts:

"1. Šo regulu piemēro personas datu apstrādei, kas pilnībā vai daļēji veikta ar automatizētiem līdzekļiem, un tādu personas datu apstrādei, kuri veido daļu no kartotēkas vai ir paredzēti, lai veidotu daļu no kartotēkas, ja apstrādi neveic ar automatizētiem līdzekļiem.

2. Šo regulu nepiemēro personas datu apstrādei:

a) tādas darbības gaitā, kas neietilpst Savienības tiesību aktu darbības jomā;

b) ko īsteno dalībvalstis, veicot darbības, kas ir LES V sadaļas 2. nodaļas darbības jomā;

c) ko veic fiziska persona tikai personiska vai mājsaimnieciska pasākuma gaitā;

d) ko veic kompetentas iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināLsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu."

10 Minētās regulas 4. pantā ir noteikts:

"Šajā regulā:

[..]

2) “apstrāde” ir jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana;

[..]

7) “pārzinis” ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kas viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus; ja šādas apstrādes nolūkus un līdzekļus nosaka ar Savienības vai dalībvalsts tiesību aktiem, pārzini vai tā iecelšanas konkrētos kritērijus var paredzēt Savienības vai dalībvalsts tiesību aktos;

8) “apstrādātājs” ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura pārziņa vārdā apstrādā personas datus;

9) “saņēmējs” ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kurai izpauž personas datus – neatkarīgi no tā, vai tā ir trešā persona vai nav. Tomēr publiskas iestādes, kas var saņemt personas datus saistībā ar konkrētu izmeklēšanu saskaņā ar Savienības vai dalībvalsts tiesību aktiem, netiek uzskatītas par saņēmējiem; minēto datu apstrāde, ko veic minētās publiskās iestādes, atbilst piemērojamiem datu aizsardzības noteikumiem saskaņā ar apstrādes nolūkiem;

[..]”

11 Šīs pašas regulas 23. pantā ir noteikts:

“1. Saskaņā ar Savienības vai dalībvalsts tiesību aktiem, kas piemērojami datu pārzinim vai apstrādātājam, ar leģislatīvu pasākumu var ierobežot to pienākumu un tiesību darbības jomu, kas paredzēti 12.–22. pantā un 34. pantā, kā arī 5. pantā, ciktāl tā noteikumi atbilst 12.–22. pantā paredzētajām tiesībām un pienākumiem, – ja ar šādu ierobežojumu tiek ievērota pamattiesību un pamatbrīvību būtība un tas demokrātiskā sabiedrībā ir nepieciešams un samērīgs, lai garantētu:

a) valsts drošību;

b) aizsardzību;

c) sabiedrisko drošību;

d) noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu vai saukšanu pie atbildības par tiem vai kriminālsodu izpildi, tostarp aizsardzību pret sabiedriskās drošības apdraudējumiem un to novēršanu;

[..]

2. Jo īpaši – jebkurā leģislatīvā pasākumā, kas minēts 1. punktā, ietver konkrētus noteikumus attiecīgā gadījumā vismaz par:

a) nolūkiem, kādos veic apstrādi, vai apstrādes kategorijām;

b) personas datu kategorijām;

c) ieviesto ierobežojumu darbības jomu;

d) garantijām, lai novērstu ļaunprātīgu izmantošanu vai nelikumīgu piekļuvi vai nosūtīšanu;

e) pārziņa vai pārziņu kategoriju noteikšanu;

f) glabāšanas laikposmiem un piemērojamām garantijām, ņemot vērā apstrādes vai apstrādes kategoriju raksturu, darbības jomu un nolūkus;

g) riskiem attiecībā uz datu subjektu tiesībām un brīvībām; un

h) datu subjektu tiesībām saņemt informāciju par ierobežojumu, izņemot tad, ja tas var kaitēt ierobežojuma mērķim."

12 VDAR V nodaļā "Personas datu nosūtīšana uz trešām valstīm vai starptautiskām organizācijām" ir ietverts šīs regulas 44.–50. pants. Šīs regulas 44. pantā "Nosūtīšanas vispārīgie principi" ir noteikts:

"Personas datus, kuri tiek apstrādāti vai kurus ir paredzēts apstrādāt pēc nosūtīšanas uz trešo valsti vai starptautisku organizāciju, nosūta tikai tad, ja, ņemot vērā pārējos šīs regulas noteikumus, pārzinis un apstrādātājs ir ievērojuši šajā nodaļā paredzētos nosacījumus, ietverot arī personas datu tālāku nosūtīšanu no trešās valsts vai starptautiskās organizācijas uz citu trešo valsti vai citu starptautisku organizāciju. Piemēro visus šīs nodaļas noteikumus, lai nodrošinātu, ka nemazinās ar šo regulu garantētais fizisku personu aizsardzības līmenis."

13 Šīs regulas 45. panta "Nosūtīšana, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību" 1.–3. punktā ir paredzēts:

"1. Personas datu nosūtīšanu uz trešo valsti vai starptautisku organizāciju var veikt, ja Komisija ir nolēmusi, ka trešā valsts, kāda minētās trešās valsts teritorija vai viens vai vairāki konkrēti sektori, vai attiecīgā starptautiskā organizācija nodrošina pietiekamu aizsardzības līmeni. Šādai nosūtīšanai nav nepieciešama nekāda īpaša atļauja.

2. Izvērtējot aizsardzības līmeņa pietiekamību, Komisija jo īpaši ņem vērā šādus elementus:

a) tiesiskums, cilvēktiesību un pamatbrīvību ievērošana, attiecīgie 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, datu aizsardzības noteikumu, dienesta noteikumu un drošības pasākumu īstenošana, tostarp noteikumi par personas datu tālāku nosūtīšanu uz citu trešo valsti vai starptautisko organizāciju, kurus ievēro minētajā valstī vai minētajā starptautiskajā organizācijā, judikatūra, kā arī tas, vai pastāv efektīvas un tiesiski īstenojamas datu subjektu tiesības un efektīva aizsardzība administratīvā kārtā vai tiesā tiem datu subjektiem, kuru personas datus nosūta;

b) tas, vai attiecīgajā trešā valstī vai attiecībā uz starptautisko organizāciju pastāv un efektīvi darbojas viena vai vairākas neatkarīgas uzraudzības iestādes, kuras ir atbildīgas par datu aizsardzības noteikumu ievērošanas nodrošināšanu un īstenošanu, tostarp ar adekvātām izpildes pilnvarām, par palīdzību un konsultāciju sniegšanu datu subjektiem saistībā ar viņu tiesību īstenošanu un par sadarbību ar dalībvalstu uzraudzības iestādēm; un

c) starptautiskās saistības, ko ir uzņēmusies attiecīgā trešā valsts vai starptautiskā organizācija, vai citi pienākumi, kas izriet no juridiski saistošām konvencijām vai instrumentiem, kā arī no tās dalības daudzpusējās vai reģionālās sistēmās, jo īpaši saistībā ar personas datu aizsardzību.

3. Komisija pēc aizsardzības līmeņa pietiekamības izvērtēšanas ar īstenošanas aktu var nolemt, ka trešā valsts, trešās valsts teritorija vai viens vai vairāki konkrēti sektori, vai starptautiska organizācija nodrošina pietiekamu aizsardzības līmeni šā panta 2. punkta nozīmē. Īstenošanas aktā paredz periodiskas, vismaz reizi četros gados notiekošas pārskatīšanas mehānismu, kurā ņem vērā visas attiecīgās norises trešajā valstī vai starptautiskajā organizācijā. Īstenošanas aktā precizē tā teritoriālo un

sektoriālo piemērošanu un attiecīgā gadījumā norāda šā panta 2. punkta b) apakšpunktā minēto uzraudzības iestādi vai iestādes. Īstenošanas aktu pieņem saskaņā ar pārbaudes procedūru, kas minēta 93. panta 2. punktā."

14 Šīs pašas regulas 46. panta "Nosūtīšana, pamatojoties uz atbilstošām garantijām" 1.–3. punktā ir noteikts:

"1. Ja nav pieņemts lēmums saskaņā ar 45. panta 3. punktu, pārzinis vai apstrādātājs var nosūtīt personas datus uz trešo valsti vai uz starptautisku organizāciju tikai tad, ja pārzinis vai apstrādātājs ir sniedzis atbilstošas garantijas, un ar nosacījumu, ka datu subjektiem ir pieejamas īstenojamas datu subjekta tiesības un efektīvi tiesiskās aizsardzības līdzekļi.

2. Šā panta 1. punktā minētās atbilstošās garantijas, uzraudzības iestādei neprasot īpašu atļauju, var tikt nodrošinātas ar:

a) starp publiskām iestādēm vai struktūrām juridiski saistošu un tiesiski īstenojamu instrumentu;

b) saistošiem uzņēmuma noteikumiem saskaņā ar 47. pantu;

c) standarta datu aizsardzības klauzulām, ko Komisija pieņem saskaņā ar 93. panta 2. punktā minēto pārbaudes procedūru;

d) standarta datu aizsardzības klauzulām, ko pieņem uzraudzības iestāde un apstiprina Komisija saskaņā ar 93. panta 2. punktā minēto pārbaudes procedūru;

e) saskaņā ar 40. pantu apstiprinātu rīcības kodeksu kopā ar trešās valsts datu pārziņa vai apstrādātāja saistošām un tiesiski īstenojamām saistībām piemērot atbilstošās garantijas, tostarp attiecībā uz datu subjekta tiesībām; vai

f) saskaņā ar 42. pantu apstiprinātu sertifikācijas mehānismu kopā ar trešās valsts datu pārziņa vai apstrādātāja saistošām un tiesiski īstenojamām saistībām piemērot atbilstošas garantijas, tostarp attiecībā uz datu subjektu tiesībām.

3. Ja kompetentā uzraudzības iestāde dod tādu atļauju, tad 1. punktā minētās atbilstošās garantijas var arī nodrošināt jo īpaši ar:

a) starp pārzini vai apstrādātāju un trešā valstī vai starptautiskā organizācijā esošu pārzini, apstrādātāju vai personas datu saņēmēju noslēgtu līgumu klauzulām; vai

b) noteikumiem, kuri iekļaujami administratīvajās vienošanās starp publiskām iestādēm vai struktūrām un kuri ietver īstenojamas un efektīvas datu subjektu tiesības."

15 Minētās regulas 49. pantā "Atkāpes īpašās situācijās" ir noteikts:

"1. Ja nav pieņemts lēmums par aizsardzības līmeņa pietiekamību saskaņā ar 45. panta 3. punktu vai nav nodrošinātas atbilstošas garantijas saskaņā ar 46. pantu, tostarp saistoši uzņēmuma noteikumi, personas datu nosūtīšana vai vairākkārtēja nosūtīšana uz trešo valsti vai starptautisku organizāciju notiek tikai tad, ja izpildīts viens no turpmāk minētajiem nosacījumiem:

a) datu subjekts ir skaidri piekritis ierosinātajai nosūtīšanai pēc tam, kad ir ticis informēts par iespējamiem riskiem, ko šāda nosūtīšana var radīt datu subjektam lēmuma par aizsardzības līmeņa pietiekamību un atbilstošu garantiju trūkuma dēļ;

b) nosūtīšana ir vajadzīga, lai izpildītu līgumu starp datu subjektu un pārzini vai īstenotu pasākumus pirms līguma noslēgšanas, kas pieņemti pēc datu subjekta pieprasījuma;

c) nosūtīšana ir vajadzīga līguma noslēgšanai starp pārzini un citu fizisku vai juridisku personu datu subjekta interesēs vai šāda līguma izpildei;

d) nosūtīšana ir vajadzīga, ja ir svarīgi iemesli sabiedrības interesēs;

e) nosūtīšana ir vajadzīga, lai celtu, īstenotu vai aizstāvētu likumīgas prasības;

f) nosūtīšana ir vajadzīga, lai aizsargātu datu subjekta vai citu personu vitālas intereses, ja datu subjekts ir fiziski vai tiesiski nespējīgs dot savu piekrišanu;

g) nosūtīšanu izdara no reģistra, kurš saskaņā ar Savienības vai dalībvalsts tiesību aktiem ir paredzēts, lai sniegtu informāciju sabiedrībai, un kuru var izmantot vai nu plaša sabiedrība, vai jebkura persona, kas var pierādīt savas leģitīmās intereses, taču vienīgi tiktāl, ciktāl konkrētajā gadījumā tiek pildīti Savienības vai dalībvalsts tiesību aktos paredzētie izmantošanas nosacījumi.

Ja nosūtīšanu nevar balstīt uz 45. vai 46. pantā ietvertu noteikumu, tostarp noteikumu par saistošiem uzņēmuma noteikumiem, un nav piemērojama neviena no atkāpēm īpašās situācijās saskaņā ar šā punkta pirmo daļu, nosūtīšana uz trešo valsti vai starptautisku organizāciju var notikt tikai tad, ja nosūtīšana neatkārtojas, attiecas vienīgi uz ierobežotu skaitu datu subjektu, ir vajadzīga pārziņa pārliecinošām leģitīmām interesēm, attiecībā uz kurām datu subjekta intereses vai tiesības un brīvības nav svarīgākas, un pārzinis ir novērtējis visus apstākļus saistībā ar datu nosūtīšanu un, pamatojoties uz minēto novērtējumu, ir sniedzis atbilstošas garantijas attiecībā uz personas datu aizsardzību. Pārzinis par nosūtīšanu informē uzraudzības iestādi. Papildus 13. un 14. pantā minētās informācijas sniegšanai pārzinis informē datu subjektu par nosūtīšanu un par pārliecinošām leģitīmām interesēm.

2. Nosūtot datus saskaņā ar 1. punkta pirmās daļas g) apakšpunktu, nenosūta pilnīgi visus reģistrā ietvertos personas datus vai veselas personas datu kategorijas. Ja reģistrs ir paredzēts, lai to varētu izmantot personas, kurām ir leģitīmas intereses, datus nosūta tikai pēc minēto personu pieprasījuma vai ja šīs personas ir datu saņēmēji.

3. Šā panta 1. punkta pirmās daļas a), b) un c) apakšpunktu un otro daļu nepiemēro publisko iestāžu darbībai, kad tās īsteno savas publiskās pilnvaras.

4. Sabiedrības intereses, kas minētas 1. punkta pirmās daļas d) apakšpunktā, ir atzītas Savienības tiesībās vai tās dalībvalsts tiesībās, kas ir piemērojamas pārzinim.

5. Ja nav lēmuma par aizsardzības līmeņa pietiekamību, Savienības vai dalībvalsts tiesību aktos, ja ir svarīgi iemesli sabiedrības interesēs, skaidri nosaka ierobežojumus attiecībā uz konkrētu kategoriju personas datu nosūtīšanu uz trešo valsti vai starptautisku organizāciju. Dalībvalstis par jebkādiem šādiem noteikumiem paziņo Komisijai.

6. Pārzinis vai apstrādātājs 30. pantā minētajos datu reģistros dokumentē novērtējumu, kā arī šā panta 1. punkta otrajā daļā izklāstītās atbilstošās garantijas."

16 Saskaņā ar VDAR 51. panta 1. punktu:

"Katra dalībvalsts paredz, ka viena vai vairākas neatkarīgas publiskas iestādes ir atbildīgas par šīs regulas piemērošanas uzraudzību, lai aizsargātu fizisku personu pamattiesības un pamatbrīvības saistībā ar apstrādi un veicinātu personas datu brīvu apriti Savienībā ("uzraudzības iestāde")."

17 Saskaņā ar šīs regulas 55. panta 1. punktu "katra uzraudzības iestāde savas dalībvalsts teritorijā ir kompetenta pildīt uzticētos uzdevumus un īstenot pilnvaras, ko tai piešķir saskaņā ar šo regulu".

18 Minētās regulas 57. panta 1. punktā ir paredzēts:

"Neskarot citus uzdevumus, kas noteikti ar šo regulu, ikviena uzraudzības iestāde savā teritorijā:

a) uzrauga un īsteno šīs regulas piemērošanu;

[..]

f) izskata kāda datu subjekta [..] iesniegtās sūdzības [..], atbilstošā apjomā izmeklē jautājumu un saprātīgā termiņā informē sūdzības iesniedzēju par lietas virzību un izmeklēšanas rezultātiem, jo īpaši, ja ir nepieciešama papildus izmeklēšana vai koordinācija ar citu uzraudzības iestādi;

[..]."

19 Saskaņā ar šīs pašas regulas 58. panta 2. un 4. punktu:

"2. Katrai uzraudzības iestādei ir visas šādas korektīvās pilnvaras:

[..]

f) uzlikt pagaidu vai galīgu apstrādes ierobežojumu, tostarp aizliegumu;

[..]

j) izdot rīkojumu apturēt datu plūsmu pie saņēmēja trešā valstī vai pie starptautiskas organizācijas.

[..]

4. Uzraudzības iestāde saskaņā ar šo pantu piešķirto pilnvaru īstenošanā ievēro atbilstošas garantijas, tostarp efektīvu tiesību aizsardzību tiesā un pienācīgas procedūras, kas noteiktas Savienības un dalībvalstu tiesību aktos saskaņā ar Hartu."

20 VDAR 64. panta 2. punkts ir formulēts šādi:

"Jebkura uzraudzības iestāde, [Eiropas Datu aizsardzības kolēģijas (EDAK)] priekšsēdētājs vai Komisija var pieprasīt, lai kolēģija izskata jebkuru jautājumu par vispārējo piemērošanu vai kas rada sekas vairāk nekā vienā dalībvalstī nolūkā saņemt atzinumu, jo īpaši, ja kompetentā uzraudzības iestāde neievēro savstarpējas palīdzības pienākumu saskaņā ar 61. pantu vai kopīgu operāciju pienākumu saskaņā ar 62. pantu."

21 Saskaņā ar šīs regulas 65. panta 1. punktu:

"Lai nodrošinātu šīs regulas pareizu un konsekventu piemērošanu katrā atsevišķā gadījumā, kolēģija pieņem saistošu lēmumu šādos gadījumos:

[..]

c) ja kompetentā uzraudzības iestāde 64. panta 1. punktā minētajos gadījumos nepieprasa kolēģijas atzinumu vai neievēro kolēģijas atzinumu, kas izsniegts saskaņā ar 64. pantu. Šādā gadījumā jebkura attiecīgā uzraudzības iestāde vai Komisija var par to informēt kolēģiju."

22 Minētās regulas 77. pantā "Tiesības iesniegt sūdzību uzraudzības iestādē" ir noteikts:

"1. Neskarot jebkādus citus administratīvos tiesību aizsardzības līdzekļus vai tiesību aizsardzību tiesā, katram datu subjektam ir tiesības iesniegt sūdzību uzraudzības iestādē, jo īpaši tajā dalībvalstī, kurā ir viņa pastāvīgā dzīvesvieta, darbavieta vai iespējamā pārkāpuma izdarīšanas vieta, ja datu subjekts uzskata, ka viņa personas datu apstrāde pārkāpj šo regulu.

2. Uzraudzības iestāde, kurā ir iesniegta sūdzība, informē sūdzības iesniedzēju par sūdzības izskatīšanas virzību un iznākumu, tostarp par tiesību aizsardzības tiesā iespēju saskaņā ar 78. pantu."

23 Šīs pašas regulas 78. panta "Tiesības uz efektīvu tiesību aizsardzību tiesā pret uzraudzības iestādi" 1. un 2. punktā ir paredzēts:

"1. Neskarot jebkādus citus administratīvos vai ārpustiesas tiesību aizsardzības līdzekļus, katrai fiziskai vai juridiskai personai ir tiesības uz efektīvu tiesību aizsardzību tiesā pret uzraudzības iestādes pieņemtu juridiski saistošu lēmumu, kas skar minētās personas.

2. Neskarot jebkādus citus administratīvos vai ārpustiesas tiesību aizsardzības līdzekļus, katram datu subjektam ir tiesības uz efektīvu tiesību aizsardzību tiesā, ja uzraudzības iestāde, kas ir kompetenta, ievērojot 55. un 56. pantu, trīs mēnešu laikā neizskata sūdzību vai neinformē datu subjektu par sūdzības, kas iesniegta, ievērojot 77. pantu, izskatīšanas virzību vai rezultātiem."

24 VDAR 94. pantā ir noteikts:

"1. Direktīvu [95/46] atceļ no 2018. gada 25. maija.

2. Atsauces uz atcelto direktīvu uzskata par atsaucēm uz šo regulu. Atsauces uz Darba grupu personu aizsardzībai attiecībā uz personas datu apstrādi, kas izveidota ar Direktīvas [95/46] 29. pantu, uzskata par atsaucēm uz Eiropas Datu aizsardzības kolēģiju, kas izveidota ar šo regulu."

25 Saskaņā ar šīs regulas 99. pantu:

"1. Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

2. To piemēro no 2018. gada 25. maija."

LSK lēmums

26 LSK lēmuma 11. apsvērums ir formulēts šādi:

"Dalībvalstu uzraudzības iestādēm ir izšķiroša nozīme šajā līguma mehānismā, nodrošinot personas datu pienācīgu aizsardzību pēc pārsūtīšanas. Izņēmuma gadījumos, kad datu nosūtītāji atsakās dot datu saņēmējam pietiekamus norādījumus vai arī nespēj šādus norādījumus dot, tādējādi radot būtiska kaitējuma draudus datu subjektiem, līguma standartklauzulās uzraudzības iestādēm jāļauj veikt pārbaudes attiecībā uz datu saņēmējiem un apakšapstrādātājiem un attiecīgā gadījumā pieņemt lēmumus, kas datu saņēmējiem apakšapstrādātājiem ir saistoši. Uzraudzības iestādēm jābūt pilnvarotām aizliegt vai pārtraukt vienu vai vairākas datu pārsūtīšanas, balstoties uz līguma standartklauzulām tajos izņēmuma gadījumos, kad ir noteikts, ka pārsūtīšana, pamatojoties uz līgumu, iespējams, var ļoti negatīvi ietekmēt garantijas un pienākumus, kas datu subjektam sniedz pienācīgu aizsardzību."

27 Šī lēmuma 1. pantā ir noteikts:

"Uzskata, ka šā lēmuma pielikumā paredzētās līguma standartklauzulas sniedz pienācīgu nodrošinājumu attiecībā uz indivīdu privātās dzīves, pamattiesību un pamatbrīvību aizsardzību un attiecībā uz attiecīgo tiesību izmantošanu, kā noteikts Direktīvas [95/46] 26. panta 2. punktā."

28 Atbilstoši minētā lēmuma 2. panta otrajai daļai tas "attiecas uz personas datiem, ko Eiropas Savienībā reģistrēti atbildīgie par datu apstrādi pārsūta saņēmējiem, kuri ir reģistrēti ārpus Eiropas Savienības teritorijas un kuri darbojas tikai kā apstrādātāji".

29 Šī paša lēmuma 3. pantā ir noteikts:

"Šajā lēmumā piemēro šādas definīcijas:

[..]

c) "datu nosūtītājs" ir atbildīgais par datu apstrādi, kas pārsūta personas datus;

d) "datu saņēmējs" ir trešā valstī reģistrēts atbildīgais par datu apstrādi, kas piekrīt personas datus saņemt no datu nosūtītāja, lai tos pēc pārsūtīšanas apstrādātu nosūtītāja uzdevumā saskaņā ar tā norādījumiem un šā lēmuma noteikumiem, un uz ko neattiecas trešās valsts sistēma, ar kuru nodrošina pienācīgu aizsardzību Direktīvas [95/46] 25. panta 1. punkta nozīmē;

[..]

f) "piemērojamie tiesību akti datu aizsardzības jomā" ir tiesību akti, kas aizsargā personu pamattiesības un pamatbrīvības, un jo īpaši viņu tiesības uz privāto dzīvi attiecībā uz personas datu apstrādi, un kas attiecas uz atbildīgo par datu apstrādi dalībvalstī, kurā datu nosūtītājs ir reģistrēts;

[..]."

30 Lēmuma 2010/87 4. pantā, tā sākotnējā redakcijā, kas bija spēkā pirms Īstenošanas lēmuma 2016/2297 stāšanās spēkā, bija paredzēts:

"1. Neskarot dalībvalstu kompetento iestāžu pilnvaras rīkoties, lai nodrošinātu to valsts tiesību aktu ievērošanu, kas ir pieņemti atbilstīgi Direktīvas [95/46] II, III, V un VI nodaļai, tās var īstenot savas pašreizējās pilnvaras, lai aizliegtu vai apturētu datu plūsmu uz trešām valstīm, lai aizsargātu personas attiecībā uz viņu personas datu apstrādi, ja:

a) konstatē, ka tiesību akti, kuri datu saņēmējam vai apakšapstrādātājam jāievēro, uzliek tam pienākumu atkāpties no piemērojamiem tiesību aktiem datu aizsardzības jomā, kas pārsniedz ierobežojumus, kuri ir vajadzīgi demokrātiskā sabiedrībā, kā paredzēts Direktīvas [95/46] 13. pantā, ja ir iespējamība, ka šis pienākums var ļoti negatīvi ietekmēt garantijas, kas ir paredzētas piemērojamos tiesību aktos datu aizsardzības jomā un līguma standartklauzulās;

b) kompetentā iestāde ir konstatējusi, ka datu saņēmējs vai apakšapstrādātājs nav ievērojis pielikumā minētās līguma standartklauzulas; vai

c) ir liela iespējamība, ka nav ievērotas vai netiks ievērotas pielikumā minētās līguma standartklauzulas, un pārsūtīšanas turpināšana datu subjektiem radītu būtiska kaitējuma draudus.

2. Aizliegumu vai pārtraukšanu atbilstīgi 1. punktam atceļ, tiklīdz tam vairs nav iemesla.

3. Ja dalībvalstis nosaka pasākumus atbilstīgi 1. un 2. punktam, tās nekavējoties informē Komisiju, kas nosūta informāciju pārējām dalībvalstīm."

31 Īstenošanas lēmuma 2016/2297, kas pieņemts pēc 2015. gada 6. oktobra sprieduma *Schrems* (C-362/14, EU:C:2015:650) pasludināšanas, 5. apsvērums ir formulēts šādi:

"*Mutatis mutandis* Komisijas lēmums, kas pieņemts saskaņā ar Direktīvas [95/46] 26. panta 4. punktu, ir saistošs visām dalībvalstu iestādēm, kurām tas ir adresēts, tostarp to neatkarīgajām uzraudzības iestādēm, uz ko šis lēmums attiecas, ciktāl tā rezultātā tiek atzīts, ka pārsūtīšana, kas notiek, pamatojoties uz šajā direktīvā ietvertajām līguma standartklauzulām, sniedz pietiekamu aizsardzības līmeni, kāds pieprasīts minētās direktīvas 26. panta 2. punktā. Tas neliedz valsts uzraudzības iestādei īstenot tās pilnvaras pārraudzīt datu plūsmas, tostarp pilnvaras apturēt vai aizliegt personas datu pārsūtīšanu, ja tā konstatē, ka pārsūtīšana notiek, pārkāpjot ES vai valsts datu aizsardzības tiesību aktus, piemēram, ja datu saņēmējs neievēro līguma standartklauzulas."

32 LSK lēmuma 4. pantā, tā pašreizējā redakcijā, kas izriet no Īstenošanas lēmuma 2016/2297, ir noteikts:

"Kad kompetentās iestādes dalībvalstī, lai pasargātu personas attiecībā uz viņu personas datu apstrādi, izmanto savas pilnvaras atbilstīgi Direktīvas [95/46] 28. panta 3. punktam, kā rezultātā tiek apturētas vai pilnībā aizliegtas datu plūsmas uz trešām valstīm, attiecīgā dalībvalsts nekavējoties informē Komisiju, kas nosūta informāciju pārējām dalībvalstīm."

33 LSK lēmuma pielikumā "Līguma standartklauzulas (apstrādātāji)" ir ietvertas divpadsmit standartklauzulas. Tā 3. klauzulā "Ieinteresētās trešās personas klauzula" ir paredzēts:

"1. Datu subjekts kā ieinteresētā trešā persona var piemērot pret datu nosūtītāju šo klauzulu, 4. klauzulas b)–i) punktu, 5. klauzulas a)–e) un g)–j) punktu, 6. klauzulas 1. un 2. punktu, 7. klauzulu, 8. klauzulas 2. punktu un 9.–12. klauzulu.

2. Datu subjekts var piemērot pret datu saņēmēju šo klauzulu, 5. klauzulas a)–e) un g) punktu, 6. klauzulu, 7. klauzulu, 8. klauzulas 2. punktu un 9.–12. klauzulu gadījumos, kad datu nosūtītājs ir faktiski zudis vai juridiski beidzis pastāvēt, ja vien kāds tiesību pārņēmējs ar līgumu vai likumiskā kārtā nav uzņēmies visas datu nosūtītāja juridiskās saistības, kā rezultātā tas uzņemas datu nosūtītāja tiesības un pienākumus, un šādā gadījumā datu subjekts tos var piemērot pret minēto personu.

[..]"

34 Saskaņā ar šī pielikuma 4. klauzulu "Datu nosūtītāja pienākumi":

"Datu nosūtītājs piekrīt un garantē, ka:

a) personas datu apstrāde, tostarp pati pārsūtīšana, tiek un arī turpmāk tiks veikta saskaņā ar datu aizsardzības jomā piemērojamiem tiesību aktiem (un attiecīgos gadījumos par to tiek ziņots attiecīgajām iestādēm dalībvalstī, kurā reģistrēts datu nosūtītājs) un netiek pārkāpti minētās valsts attiecīgie noteikumi;

b) tas ir devis norādījumus un visā personas datu apstrādes pakalpojumu sniegšanas laikā turpinās dot norādījumus datu saņēmējam apstrādāt pārsūtītos personas datus vienīgi datu nosūtītāja uzdevumā un saskaņā ar datu aizsardzības jomā piemērojamiem tiesību aktiem un šīm klauzulām;

[..]

f) tad, ja pārsūtīšana ietver īpašas datu kategorijas, datu subjekts tiek vai tiks informēts iepriekš, ka tā dati varētu tikt pārraidīti uz trešo valsti, kas nesniedz pietiekamu aizsardzības līmeni Direktīvas [95/46] nozīmē, vai iespējami drīz pēc tam;

g) saskaņā ar 5. klauzulas b) punktu un 8. klauzulas 3. punktu datu aizsardzības uzraudzības iestādei tiek pārsūtīti visi paziņojumi, kas saņemti no datu saņēmēja vai kāda apakšapstrādātāja, ja datu nosūtītājs nolemj turpināt pārsūtīšanu vai atcelt aizliegumu;

[..]."

35 Minētā pielikuma 5. klauzulā "Datu saņēmēja pienākumi [..]" ir noteikts:

"Datu saņēmējs piekrīt un garantē, ka:

a) tas apstrādās personas datus vienīgi datu nosūtītāja vārdā un saskaņā ar tā norādījumiem un klauzulām; gadījumā, ja datu saņēmējs kāda iemesla dēļ nevar nodrošināt norādījumu un klauzulu ievērošanu, tas piekrīt nekavējoties informēt par to datu nosūtītāju, un šādā gadījumā datu nosūtītājam ir tiesības apturēt datu pārsūtīšanu un/vai izbeigt līgumu;

b) tam nav iemesla uzskatīt, ka datu saņēmējam piemērojamie tiesību akti neļauj tam izpildīt datu nosūtītāja norādījumus un līgumā paredzētos pienākumus, un ka gadījumā, ja tiek izdarītas tādas izmaiņas datu saņēmēja tiesību aktos, kas var negatīvi ietekmēt klauzulās noteiktās garantijas un pienākumus, tas nekavējoties paziņos par šīm izmaiņām datu nosūtītājam, tiklīdz tās kļūs zināmas, un šādā gadījumā datu nosūtītājam ir tiesības apturēt datu pārsūtīšanu un/vai izbeigt līgumu;

[..]

d) tas nekavējoties paziņos datu nosūtītājam par:
   i) tiesībaizsardzības iestāžu jebkuru juridiski saistošu pieprasījumu atklāt personas datus, ja vien tas citādi nav aizliegts, piemēram, krimināltiesībās paredzētais aizliegums nolūkā saglabāt tiesībaizsardzības iestāžu veiktās izmeklēšanas konfidencialitāti;
   ii) jebkuru nejaušu vai neatļautu piekļuvi; kā arī
   iii) jebkuru pieprasījumu, kas tiešā veidā saņemts no datu subjektiem, neatbildot uz minēto pieprasījumu, ja vien tas nav citādi pilnvarots to darīt;

[..]."

36 Zemsvītras piezīmē, uz kuru ir atsauce šīs 5. klauzulas virsrakstā, ir noteikts:

"Valsts tiesību aktu obligātās prasības, ko piemēro datu saņēmējam un kas nepārsniedz prasības, kuras ir vajadzīgas demokrātiskā sabiedrībā, pamatojoties uz vienu no Direktīvas [95/46] 13. panta 1. punktā minētajām interesēm, proti, ja tās ir nepieciešams aizsargpasākums valsts drošībai, aizsardzībai, sabiedrības drošībai, kriminālsodāmu noziedzīgu nodarījumu vai reglamentētu profesiju ētikas pārkāpumu novēršanai, izmeklēšanai, atklāšanai un kriminālvajāšanai, valsts svarīgās ekonomiskās vai finansiālās interesēs vai datu subjekta aizsardzībai vai citu personu tiesību un brīvību aizsardzībai, nav pretrunā līguma standartklauzulām. [..]"

37 LSK lēmuma pielikuma 6. klauzulā "Atbildība" ir paredzēts:

"1. Puses vienojas, ka datu subjektam, kam nodarīts kaitējums 3. vai 11. klauzulā minēto noteikumu pārkāpumu rezultātā, kurus izdarījusi kāda no pusēm vai apakšapstrādātājs, ir tiesības saņemt no datu nosūtītāja kompensāciju par nodarīto kaitējumu.

2. Ja datu subjekts pret datu nosūtītāju nevar vērsties ar 1. punktā minēto prasību par kompensāciju, kas izriet no tā, ka datu nosūtītājs vai tā apakšapstrādātājs nav izpildījis kādu no 3. vai 11. klauzulā minētajiem pienākumiem, sakarā ar to, ka datu nosūtītājs ir faktiski zudis vai juridiski beidzis pastāvēt, vai arī ir kļuvis maksātnespējīgs, datu saņēmējs piekrīt, ka datu subjekts var izvirzīt prasību pret datu saņēmēju tā, it kā tas būtu datu nosūtītājs [..].

[..]"

38 Šī pielikuma 8. klauzulas "Sadarbība ar uzraudzības iestādēm" 2. punktā ir paredzēts:

"Puses piekrīt, ka uzraudzības iestādei ir tiesības veikt datu saņēmēja vai jebkura apakšapstrādātāja revīziju, kurai ir tāds pats apjoms un uz kuru attiecas tādi paši nosacījumi, kādi būtu piemērojami datu nosūtītāja revīzijai saskaņā ar piemērojamiem tiesību aktiem datu aizsardzības jomā."

39 Minētā pielikuma 9. klauzula "Piemērojamie tiesību akti" paredz, ka līguma standartklauzulas reglamentē tās dalībvalsts tiesību akti, kurā datu nosūtītājs ir reģistrēts.

40 Saskaņā ar tā paša pielikuma 11. klauzulu "Apakšapstrāde":

"1. Datu saņēmējs bez datu nosūtītāja iepriekšējas rakstiskas piekrišanas neslēdz apakšuzņēmuma līgumus par savām apstrādes darbībām, ko saskaņā ar šo klauzulu noteikumiem tas veic datu nosūtītāja uzdevumā. Ja datu saņēmējs ar datu nosūtītāja piekrišanu noslēdz apakšuzņēmuma līgumu par savu pienākumu izpildi saskaņā ar šo klauzulu noteikumiem, to var darīt vienīgi, noslēdzot ar apakšapstrādātāju rakstisku līgumu, ar kuru apakšapstrādātājam tiek uzlikti tādi paši pienākumi kā datu saņēmējam saskaņā ar šīm klauzulām. [..]

2. Iepriekšējā rakstiskajā līgumā starp datu saņēmēju un apakšapstrādātāju tiek iekļauta arī ieinteresētās trešās personas klauzula, kā noteikts 3. klauzulā, attiecībā uz gadījumiem, kad datu subjekts nevar vērsties pret datu nosūtītāju vai datu saņēmēju ar 6. klauzulas 1. punktā minēto prasību par kompensāciju sakarā ar to, ka tie ir faktiski zuduši vai juridiski beiguši pastāvēt, vai arī ir kļuvuši maksātnespējīgi, un neviens tiesību pārņēmējs ar līgumu vai likumiskā kārtā nav uzņēmies visas datu nosūtītāja vai datu saņēmēja juridiskās saistības. Minētā apakšapstrādātāja civiltiesiskā atbildība attiecas vienīgi uz tā paša apstrādes darbībām saskaņā ar šo klauzulu noteikumiem.

[..]"

41 LSK lēmuma pielikuma 12. klauzulas "Pienākumi pēc personas datu apstrādes pakalpojumu izbeigšanas" 1. punktā ir paredzēts šādi:

"Puses vienojas, ka, izbeidzot personas datu apstrādes pakalpojumu sniegšanu, datu saņēmējs un apakšapstrādātājs pēc datu nosūtītāja izvēles nodod atpakaļ datu nosūtītājam visus pārsūtītos personas datus un to kopijas vai iznīcina visus personas datus un apliecina datu nosūtītājam, ka tas ir izdarīts, ja vien datu saņēmējam piemērojamie tiesību akti neliedz tam nodot atpakaļ vai iznīcināt visus vai daļu no pārsūtītajiem personas datiem. [..]"

PV lēmums

42 Ar 2015. gada 6. oktobra spriedumu *Schrems* (C-362/14, EU:C:2015:650) Tiesa atzina par spēkā neesošu Komisijas Lēmumu 2000/520/EK (2000. gada 26. jūlijs) atbilstīgi [Direktīvai 95/46] par pienācīgu aizsardzību, kas noteikta ar privātuma drošības zonas principiem un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija (OV 2000, L 215, 7. lpp.), kurā Komisija bija konstatējusi, ka šī trešā valsts nodrošina pienācīgu aizsardzības līmeni.

43 Pēc šī sprieduma pasludināšanas Komisija pieņēma PV lēmumu, kad tā šai nolūkā bija izvērtējusi Amerikas Savienoto Valstu tiesisko regulējumu, kā tas ir precizēts minētā lēmuma 65. apsvērumā:

"Komisija ir izvērtējusi ierobežojumus un aizsardzības pasākumus, kas pieejami ASV tiesībās attiecībā uz piekļuvi datiem, kuri tiek nosūtīti ES un ASV privātuma vairoga ietvaros, un to izmantošanu ASV valsts iestādēs valsts drošības, tiesībaizsardzības un citu valsts interešu nolūkos. Papildus ASV valdība ar Nacionālās izlūkošanas direktora biroja (NIDB) starpniecību [..] ir sniegusi Komisijai detalizētus apgalvojumus un uzņēmusies saistības, kas iekļautas šā lēmuma VI pielikumā. Ar valsts sekretāra parakstītu un šā lēmuma III pielikumā pievienotu vēstuli ASV valdība ir uzņēmusies saistības arī nodrošināt jaunu pārraudzības mehānismu valsts drošības interferencei – privātuma vairoga ombudu, kurš darbojas neatkarīgi no izlūkdienestiem. Visbeidzot, ASV Tieslietu ministrijas apgalvojumos, kas iekļauti šā lēmuma VII pielikumā, ir aprakstīti ierobežojumi un aizsardzības pasākumi, kas piemērojami valsts iestādēm datu piekļuvei un izmantošanai tiesībaizsardzības un citu valsts interešu nolūkos. Lai uzlabotu pārredzamību un atspoguļotu šo saistību tiesisko raksturu, katrs šajā lēmuma uzskaitītais un tam pievienotais dokuments tiks publicēts ASV Federālajā reģistrā."

44 Komisijas veiktā šo ierobežojumu un garantiju analīze ir apkopota PV lēmuma 67.–135. apsvērumā, savukārt šīs iestādes secinājumi par pietiekamu aizsardzības līmeni saistībā ar Eiropas Savienības un ASV privātuma vairogu ir ietverti tā 136.–141. apsvērumā.

45 Konkrētāk, šī lēmuma 68., 69., 76., 77., 109., 112.–116., 120., 136. un 140. apsvērumā ir teikts:

"(68) Atbilstīgi ASV Konstitūcijai rūpes par valsts drošību ir prezidenta kompetencē, kurš ir kā virspavēlnieks, galvenā izpildvara un, attiecībā uz ārvalstu izlūkošanu, ASV ārlietu vadītājs. Lai arī Kongresam ir tiesības piemērot ierobežojumus, un tas ir darīts dažādos aspektos, prezidents šajā kontekstā var pārvaldīt ASV izlūkdienestu darbības, jo īpaši ar izpildrīkojumiem vai prezidenta direktīvām. [..] Šobrīd divi galvenie tiesību akti šajā jomā ir Izpildrīkojums Nr. 12333 (*Executive Order, E.O. 12333*) un Prezidenta politikas direktīva Nr. 28 (*PPD-28*).

(69) Ar 2014. gada 17. janvārī izdoto Prezidenta politikas direktīvu Nr. 28 ("PPD-28") ir noteikti vairāki ierobežojumi "sakaru izlūkošanas" darbībām [..]. Prezidenta direktīva ir saistoša ASV izlūkošanas iestādēm [..] un saglabā spēku līdz ASV valdības maiņai [..]. PPD-28 ir īpaši svarīga citu valstu personām, tostarp ES datu subjektiem. [..]

[..]

(76) Lai arī tas nav noformulēts šajos [PPD-28] juridiskajos noteikumos, šie principi iemieso nepieciešamības un proporcionalitātes principu būtību. [..]

(77) Tā kā prasības ir iekļautas direktīvā, ko izdevis prezidents kā galvenā izpildvara, tās ir saistošas visiem izlūkdienestiem un ir tālāk īstenotas ar aģentūru noteikumiem un procedūrām, ar kurām vispārējos principus transponē konkrētos virzienos ikdienas darbībām. [..]

[..]

(109) Turpretī saskaņā ar ĀIUL [*Foreign Intelligence Surveillance Act*; Ārvalstu izlūkošanas uzraudzības likums] 702. pantu ĀIUT [*United States Foreign Intelligence Surveillance Court*, ĀIUL tiesa] neapstiprina individuālus uzraudzības pasākumus, bet gan uzraudzības programmas (piemēram, *PRISM*, *UPSTREAM*), pamatojoties uz ikgadējām sertifikācijām, kuras sagatavo ģenerālprokurors [*United States Attorney General*] un nacionālās izlūkošanas direktors [*Director of National Intelligence*]. [..] Kā norādīts, sertifikācijas, kuras jāapstiprina ĀIUT, nesatur informāciju par atsevišķām personām, kuras jāizseko, bet gan identificē ārvalstu izlūkošanas informācijas kategorijas [..]. Lai arī ĀIUT nevērtē – pamatojoties uz ticamu iemeslu

vai kādu citu standartu –, vai personas ir atbilstīgi izsekotas, lai iegūtu ārvalstu izlūkošanas informāciju, tās kontrole ietver nosacījumu, ka "būtisks iegūšanas mērķis ir iegūt ārvalstu izlūkošanas informāciju". [..]

[..]

(112) Pirmkārt, Ārvalstu izlūkošanas uzraudzības likums paredz vairākus tiesiskās aizsardzības līdzekļus, pieejamus arī [..] personām[, kas nav ASV pilsoņi], ar kuriem apstrīdēt nelikumīgu elektronisko uzraudzību. To vidū ir iespēja personām celt civilprasību pret Amerikas Savienotajām Valstīm par finansiāliem zaudējumiem, ja informācija par šīm personām ir nelikumīgi un tīši izmantota vai izpausta [..]; iesūdzēt tiesā ASV valsts amatpersonas kā privātpersonas (kas nelikumīgi veic likumīgu darbību) par finansiāliem zaudējumiem [..]; un apstrīdēt uzraudzības likumību (un pieprasīt noklusēt informāciju) gadījumā, ja ASV valdība plāno izmantot vai izpaust jebkādu informāciju, kas iegūta vai atvasināta no elektroniskās uzraudzības attiecībā uz personu, tiesā vai administratīvajā kārtībā Amerikas Savienotajās Valstīs [..].

(113) Otrkārt, ASV valdība norādīja Komisijai vairākas papildu iespējas, kuras ES datu subjekti var izmantot, lai pieprasītu tiesību aizsardzību pret valdības amatpersonām attiecībā uz nelikumīgu valdības piekļuvi personas datiem vai to izmantošanu, tostarp paredzētos nacionālās drošības nolūkos [..].

(114) Visbeidzot, ASV valdība ir norādījusi uz LIB [*Freedom of Information Act*; Likums par informācijas brīvību] kā līdzekli citu valstu personām, ar kuru pieprasīt piekļuvi esošajiem federālās aģentūras ierakstiem, tostarp tad, ja tie satur attiecīgās privātpersonas personas datus [..]. Ņemot vērā tvērumu, uz ko vērsts LIB, tas neparedz individuālu tiesību aizsardzību pret iejaukšanos personas datos, lai arī principā tas ļautu personām iegūt piekļuvi būtiskai informācijai, kuru glabā nacionālās izlūkošanas aģentūras. [..]

(115) Lai arī tādējādi personām, tostarp ES datu subjektiem, ir vairākas tiesiskās aizsardzības iespējas, ja tās ir pakļautas nelikumīgai (elektroniskajai) uzraudzībai nacionālās drošības nolūkos, tikpat skaidrs ir tas, ka nav iekļauti atsevišķi juridiskie pamatojumi (piemēram, *E.O. 12333*), kurus var izmantot ASV izlūkošanas iestādes. Turklāt, ja tiesiskās aizsardzības iespējas principā ir citu valstu personām, piemēram, uzraudzībai saskaņā ar ĀIUL, pieejamie rīcības pamatojumi ir ierobežoti [..], un personu (tostarp ASV piederīgu personu) prasības tiks atzītas par nepieņemamām, ja tās nevar pierādīt "tiesībspēju" [..], un tas ierobežo piekļuvi parastajām tiesām [..].

(116) Lai paredzētu papildu tiesiskās aizsardzības iespējas, kas pieejamas visiem ES datu subjektiem, ASV valdība ir nolēmusi izveidot jaunu ombuda mehānismu, kā izklāstīts ASV valsts sekretāra vēstulē Komisijai, vēstule ir pievienota šā lēmuma III pielikumā. Šā mehānismā pamatā ir vecākā koordinatora (valsts sekretāra vietnieka līmenī) iecelšana Valsts departamentā saskaņā ar PPD-28, kurš darbosies kā kontaktpunkts ārvalstu valdībām, lai tās varētu izteikt bažas saistībā ar ASV sakaru izlūkošanas darbībām, taču tā darbības joma ir daudz plašāka par sākotnējo konceptu.

[..]

(120) ASV valdība apņemas nodrošināt, ka, veicot savas funkcijas, privātuma aizsardzību ombuds varēs paļauties uz sadarbību no citiem pārraudzības un atbilstības pārbaudes mehānismiem, kuri pieejami ASV tiesību aktos. [..] Ja viena no šīm pārraudzības iestādēm ir konstatējusi neatbilstību, attiecīgajam izlūkdienestu elementam (piemēram, izlūkošanas aģentūrai) būs jānovērš neatbilstība, jo tikai šādi ombuds varēs sniegt personai pozitīvu atbildi (t.i., ka jebkāda neatbilstība ir novērsta) – kā ASV valdība ir to apņēmusies. [..]

[..]

(136) Ņemot vērā minētos konstatējumus, Komisija uzskata, ka Amerikas Savienotās Valstis nodrošina pienācīgu aizsardzības līmeni personas datiem, kas [Eiropas Savienības] un [Amerikas Savienoto Valstu] privātuma vairoga ietvaros no Savienības tiek nosūtīti organizācijām Amerikas Savienotajās Valstīs.

[..]

(140) Visbeidzot, pamatojoties uz pieejamo informāciju par ASV tiesību sistēmu, tostarp ASV valdības apgalvojumiem un saistībām, Komisija uzskata, ka jebkāda ASV valsts iestāžu iejaukšanās to personu pamattiesībās, kuru dati privātuma vairoga ietvaros no Savienības tiek nosūtīti uz Amerikas Savienotajām Valstīm, ja tas notiek valsts drošības, tiesībaizsardzības vai citu valsts interešu nolūkos, un sekojošie ierobežojumi, kas piemēroti pašsertificētām organizācijām attiecībā uz to principialitāti, būs ierobežoti līdz tādam apmēram, kas ir absolūti nepieciešams, lai sasniegtu attiecīgo likumīgo mērķi, un tādējādi tie nodrošina efektīvu tiesisko aizsardzību pret šādu iejaukšanos."

46 Saskaņā ar PV lēmuma 1. pantu:

"1. Direktīvas [95/46] 25. panta 2. punkta izpratnē Amerikas Savienotās Valstis nodrošina pienācīgu aizsardzības līmeni personas datiem, kas [Eiropas Savienības] un [Amerikas Savienoto Valstu] privātuma vairoga ietvaros no Savienības tiek nosūtīti organizācijām Amerikas Savienotajās Valstīs.

2. [Eiropas Savienības] un [Amerikas Savienoto Valstu] privātuma vairogu veido principi, kurus ASV Tirdzniecības ministrija izdevusi 2016. gada 7. jūlijā, kas izklāstīti II pielikumā, un oficiālie apgalvojumi un saistības, kas iekļautas dokumentos I un III–VII pielikumā.

3. Šā panta 1. punkta īstenošanai personas dati tiek pārsūtīti [Eiropas Savienības] un [Amerikas Savienoto Valstu] privātuma vairoga ietvaros, ja tos no Savienības pārsūta Amerikas Savienoto Valstu organizācijām, kuras ir iekļautas "Privātuma vairoga sarakstā", ko uztur un publicē ASV Tirdzniecības ministrija saskaņā ar II pielikumā izklāstīto principu I un III sadaļu."

47 PV lēmuma II pielikuma "[Eiropas Savienības] un [Amerikas Savienoto Valstu] privātuma vairoga regulējuma principi, ko izdevusi ASV Tirdzniecības ministrija" I.5. punktā ir paredzēts, ka šo principu ievērošanu var ierobežot tostarp, lai "ievērotu valsts drošību, sabiedrības intereses vai izpildītu tiesībaizsardzības prasības".

48 Šī lēmuma III pielikumā ir ietverta Džona Kerija [*John Kerry*], toreizējā *Secretary of State* (Valsts sekretārs, Amerikas Savienotās Valstis), 2016. gada 7. jūlija vēstule tieslietu, patērētāju un dzimumu līdztiesības komisārei, šīs vēstules A pielikumā pievienojot memorandu ar nosaukumu "[Eiropas Savienības] un ASV privātuma vairoga ombuda mehānisms sakaru izlūkošanas jomā", kurā ir ietverts šāds fragments:

"Atzīstot [Eiropas Savienības] un ASV privātuma vairoga regulējuma nozīmi, šajā memorandā ir izklāstīts process, kas jāievēro, lai īstenotu jauno mehānismu – atbilstīgi Prezidenta politikas direktīvai Nr. 28 (PPD-28) – sakaru izlūkošanas jomā.

[..] Prezidents B. Obama paziņoja, ka, lai "skaidri noteiktu, kādas darbības mēs veicam un kādas neveicam saistībā ar mūsu īstenoto aizjūras izlūkošanu", tiks pieņemta jauna prezidenta direktīva – PPD-28.

Tās 4. panta d) punktā ir noteikts, ka valsts sekretārs ieceļ "vecāko koordinatoru starptautiskās informācijas tehnoloģijas diplomātijas jautājumos" ("vecākais koordinators"), "kas [..] darbosies kā kontaktpersona ārvalstu valdībām, kuras vēlas paust bažas par Amerikas Savienoto Valstu īstenotajām sakaru izlūkošanas darbībām."

[..]

1) [Vecākais koordinators] darbosies kā privātuma vairoga ombuds un [..] cieši sadarbosies ar attiecīgajiem darbiniekiem no citām ministrijām un aģentūrām, kas atbild par pieprasījumu apstrādi atbilstīgi piemērojamiem Amerikas Savienoto Valstu tiesību aktiem un politikai. Ombuds ir neatkarīgs no izlūkdienestiem. Ombuds ir tieši pakļauts valsts sekretāram, kas nodrošina, ka ombuds savus uzdevumus veic objektīvi un neatkarīgi no neatbilstīgas ietekmes, kas var ietekmēt sniedzamo atbildi.

[..]"

49 PV lēmuma VI pielikumā ir ietverta Valsts izlūkdienesta biroja (*Office of the Director of National Intelligence*) 2016. gada 21. jūnija vēstule ASV Tirdzniecības ministrijai, kā arī Starptautiskās tirdzniecības administrācijai, kurā ir precizēts, ka *PPD-28* ļauj veikt ""lielapjoma" vākšanu [jeb] sakaru izlūkošanas informācijas vai datu iegūšanu relatīvi lielā daudzumā apstākļos, kad izlūkdienesti vākšanas fokusēšanai nevar izmantot identifikatoru, kas saistīts ar konkrētu mērķi".

Pamatlieta un prejudiciālie jautājumi

50 *M. Schrems*, Austrijā dzīvojošs šīs pašas valsts pilsonis, ir sociālā tīkla *Facebook* (turpmāk tekstā – "*Facebook*") lietotājs kopš 2008. gada.

51 Visiem *Facebook* lietotājiem, kas dzīvo Savienības teritorijā, reģistrējoties tiek lūgts parakstīt līgumu ar *Facebook Ireland* – mātesuzņēmuma *Facebook Inc.*, kura mītne ir ASV, meitasuzņēmumu. Savienības teritorijā dzīvojošo *Facebook* lietotāju dati vai daļa no tiem tiek pārsūtīti uz *Facebook Inc.* serveriem, kas atrodas ASV teritorijā, kur tie tiek apstrādāti.

52 2013. gada 25. jūnijā *M. Schrems* iesniedza komisāram sūdzību, kurā viņš būtībā lūdza aizliegt *Facebook Ireland* pārsūtīt viņa personas datus uz ASV, apgalvojot, ka šajā valstī spēkā esošās tiesības un prakse nenodrošina pietiekamu tās teritorijā uzglabāto personas datu aizsardzību pret publisko iestāžu veiktajām uzraudzības darbībām. Šī sūdzība tika noraidīta, pamatojoties it īpaši uz to, ka Komisija Lēmumā 2000/520 bija konstatējusi, ka ASV nodrošina pietiekamu aizsardzības līmeni.

53 *High Court* (Augstā tiesa, Īrija), kurā *M. Schrems* cēla prasību par viņa sūdzības noraidīšanu, vērsās Tiesā ar lūgumu sniegt prejudiciālu nolēmumu par Lēmuma 2000/520 interpretāciju un spēkā esamību. Ar 2015. gada 6. oktobra spriedumu *Schrems* (C-362/14, EU:C:2015:650) Tiesa šo lēmumu atzina par spēkā neesošu.

54 Pēc šī sprieduma pasludināšanas iesniedzējtiesa atcēla lēmumu, ar kuru komisārs bija noraidījis *M. Schrems* sūdzību, un nosūtīja to komisāram. Pēdējā minētā uzsāktās izmeklēšanas ietvaros *Facebook Ireland* paskaidroja, ka liela daļa personas datu tika nodota *Facebook Inc.*, pamatojoties uz LSK lēmuma pielikumā ietvertajām datu aizsardzības standartklauzulām. Ņemot vērā šos apstākļus, komisārs aicināja *M. Schrems* savu sūdzību pārformulēt.

55 Šādi pārformulētajā sūdzībā, kas iesniegta 2015. gada 1. decembrī, *M. Schrems* tostarp apgalvoja, ka ASV tiesībās ir noteikts, ka *Facebook Inc.* ir pienākums nodot tām pārsūtītos personas datus tādām ASV iestādēm kā *National Security Agency* (*NSA*) un *Federal Bureau of Investigation* (*FBI*). Viņš

apgalvoja – tā kā šie dati tiek izmantoti dažādās uzraudzības programmās, kas nav saderīgas ar Hartas 7., 8. un 47. pantu, LSK lēmums nevar pamatot minēto datu pārsūtīšanu uz ASV. Šādos apstākļos *M. Schrems* lūdza komisāru aizliegt vai apturēt viņa personas datu pārsūtīšanu uz *Facebook Inc.*

56 2016. gada 24. maijā komisārs publicēja "lēmumprojektu", kurā bija apkopoti viņa izmeklēšanas pagaidu secinājumi. Šajā projektā viņš provizoriski uzskatīja, ka pastāv risks, ka ar Savienības pilsoņu personas datiem, kuri tikuši pārsūtīti uz ASV, var iepazīties ASV iestādes un tās tos var apstrādāt veidā, kas nav saderīgs ar Hartas 7. un 8. pantu, un ka ASV tiesībās šiem pilsoņiem nav paredzēti tiesību aizsardzības līdzekļi, kuri atbilstu Hartas 47. pantam. Komisārs uzskatīja, ka ar LSK lēmuma pielikumā esošajām datu aizsardzības standartklauzulām nevar izlabot šo trūkumu, jo ar tām datu subjektiem tiek piešķirtas tikai līgumiskas tiesības pret nosūtītāju un saņēmēju, tomēr tās nav saistošas ASV iestādēm.

57 Tā kā šajos apstākļos *M. Schrems* pārformulētajā sūdzībā tika izvirzīts jautājums par LSK lēmuma spēkā esamību, komisārs 2016. gada 31. maijā vērsās *High Court* (Augstā tiesa), pamatojoties uz judikatūru, kas izriet no 2015. gada 6. oktobra sprieduma *Schrems* (C-362/14, EU:C:2015:650, 65. punkts), lai pēdējā minētā uzdotu Tiesai šo jautājumu. Ar 2018. gada 4. maija lēmumu *High Court* (Augstā tiesa) vērsās Tiesā ar šo lūgumu sniegt prejudiciālu nolēmumu.

58 *High Court* (Augstā tiesa) šim lūgumam sniegt prejudiciālu nolēmumu pievienoja 2017. gada 3. oktobrī pasludinātu spriedumu, tajā izklāstot valsts tiesvedībā, kurā bija piedalījusies ASV valdība, iesniegto pierādījumu pārbaudes rezultātu.

59 Šajā spriedumā, uz kuru lūgumā sniegt prejudiciālu nolēmumu ir vairākas atsauces, iesniedzējtiesa ir norādījusi, ka tai principā ir ne tikai tiesības, bet arī pienākums izvērtēt visus tajā izvirzītos faktus un argumentus, lai, pamatojoties uz tiem, izlemtu, vai ir nepieciešams iesniegt lūgumu sniegt prejudiciālu nolēmumu. Katrā ziņā tai esot jāņem vērā iespējamās izmaiņas tiesiskajā regulējumā, kas ir notikušas laikā starp prasības celšanu un tajā rīkoto tiesas sēdi. Šī tiesa precizēja, ka tiesvedībā pamatlietā tās vērtējums nav ierobežots ar komisāra izvirzītajiem spēkā neesamības pamatiem, līdz ar to tā pēc savas ierosmes var izvirzīt arī citus spēkā neesamības pamatus un, balstoties uz tiem, iesniegt lūgumu sniegt prejudiciālu nolēmumu.

60 Saskaņā ar minētajā spriedumā ietvertajiem konstatējumiem ASV iestāžu informācijas vākšanas darbības attiecībā uz personas datiem, kas pārsūtīti uz ASV, it īpaši ir balstītas uz ĀIUL 702. pantu un *E.O. 12333.*

61 Attiecībā uz ĀIUL 702. pantu iesniedzējtiesa tajā pašā spriedumā precizē, ka šis pants ļauj ģenerālprokuroram un nacionālās izlūkošanas direktoram ar ĀIUT piekrišanu nolūkā iegūt "informāciju ārvalstu izlūkošanas jomā" kopīgi atļaut veikt personu, kas nav ASV pilsoņi, uzraudzību ārpus ASV teritorijas, un tas it īpaši kalpo par pamatu *PRISM* un *UPSTREAM* uzraudzības programmām. *PRISM* programmas ietvaros saskaņā ar šīs tiesas konstatēto interneta pakalpojumu sniedzējiem ir jāsniedz *NSA* visa saziņa, ko nosūtījis un saņēmis "atlasītājs", daļa no kuras arī tiek nodota *FBI* un *Central Intelligence Agency* (Centrālā izlūkošanas pārvalde; *CIA*).

62 Attiecībā uz *UPSTREAM* programmu minētā tiesa konstatēja, ka šīs programmas ietvaros telekomunikāciju uzņēmumiem, kas ekspluatē interneta "mugurkaulu", proti, kabeļu tīklu, pārslēdzējus un maršrutētājus, pa kuriem cirkulē telefoniskās un interneta komunikācijas, ir jāļauj *NSA* kopēt un filtrēt interneta datu plūsmas, lai apkopotu saziņas materiālu, ko saņēmusi vai nosūtījusi persona, vai kas attiecas uz personu, kura nav ASV valstspiederīgā un uz kuru attiecas "atlasītājs". Minētās programmas ietvaros *NSA* saskaņā ar šīs pašas tiesas konstatējumiem ir piekļuve gan metadatiem, gan attiecīgās saziņas saturam.

63 Attiecībā uz *E.O. 12333* iesniedzējtiesa konstatē, ka tas ļauj *NSA* piekļūt uz ASV "tranzītā esošiem" datiem, piekļūstot zemūdens kabeļiem, kas izvietoti Atlantijas okeāna dzīlēs, kā arī iegūt un saglabāt šos datus pirms to ierašanās ASV un tur tiem tiek piemēroti ĀIUL noteikumi. Tā precizē, ka uz *E.O. 12333* balstītas darbības nav reglamentētas likumā.

64 Attiecībā uz izlūkošanas darbībām noteiktajiem ierobežojumiem iesniedzējtiesa uzsver, ka uz personām, kas nav ASV valstspiederīgie, attiecas tikai *PPD-28* un ka tajā ir vienīgi norādīts, ka izlūkošanas darbībām ir jābūt "pēc iespējas mērķtiecīgākām" (*as tailored as feasible*). Pamatojoties uz šiem konstatējumiem, minētā tiesa uzskata, ka ASV veic datu apstrādi masveidā, nenodrošinot Hartas 7. un 8. pantā garantētajai aizsardzībai būtībā līdzvērtīgu aizsardzību.

65 Attiecībā uz tiesību aizsardzību tiesā šī pati tiesa norāda, ka Savienības pilsoņiem nav pieejami tādi paši līdzekļi, kādi pret Amerikas iestāžu veikto personas datu apstrādi ir ASV pilsoņiem, jo *Constitution of the United States* (Amerikas Savienoto Valstu Konstitūcija) ceturtais grozījums, kas ASV tiesībās ir visbūtiskākā aizsardzība pret nelikumīgu uzraudzību, nav piemērojams Savienības pilsoņiem. Šajā ziņā iesniedzējtiesa precizē, ka pēdējo minēto rīcībā esošie tiesību aizsardzības līdzekļi atduras pret būtiskiem šķēršļiem, it īpaši pienākumu – kas, pēc tās domām, ir pārmērīgi grūti izpildāms – pamatot to tiesības celt prasību. Turklāt saskaņā ar šīs tiesas konstatējumiem *NSA* darbības, kas balstītas uz *E.O. 12333*, nav pakļautas tiesas uzraudzībai un par tām nevar celt prasību tiesā. Visbeidzot minētā tiesa uzskata – tā kā, tās skatījumā, datu aizsardzības vairoga ombuds nav tiesa Hartas 47. panta izpratnē, ASV tiesības nenodrošina Savienības pilsoņiem aizsardzības līmeni, kas būtībā ir līdzvērtīgs tam, kuru garantē šajā pantā paredzētās pamattiesības.

66 Lūgumā sniegt prejudiciālu nolēmumu iesniedzējtiesa vēl precizē, ka pamatlietas dalībnieki tostarp nav vienisprātis par Savienības tiesību piemērojamību attiecībā uz tādu personas datu pārsūtīšanu uz trešo valsti, kurus šīs valsts iestādes var apstrādāt tostarp valsts drošības nolūkā, kā arī par elementiem, kas ir jāņem vērā, lai novērtētu minētās valsts nodrošinātā aizsardzības līmeņa pietiekamību. It īpaši šī tiesa norāda, ka, *Facebook Ireland* skatījumā, tādi Komisijas konstatējumi par trešajā valstī nodrošinātā aizsardzības līmeņa pietiekamību kā PV lēmumā minētie ir saistoši uzraudzības iestādēm arī saistībā ar personas datu nodošanu, pamatojoties uz LSK lēmuma pielikumā ietvertajām datu aizsardzības standartklauzulām.

67 Attiecībā uz šīm datu aizsardzības standartklauzulām minētā tiesa jautā, vai LSK lēmumu var uzskatīt par spēkā esošu, lai gan, kā uzskata šī pati tiesa, minētajām klauzulām nav saistoša rakstura attiecībā uz attiecīgās trešās valsts publiskajām iestādēm un līdz ar to ar tām nevar novērst iespējamu aizsardzības līmeņa nepietiekamību šajā valstī. Šajā ziņā tā uzskata, ka Lēmuma 2010/87 – redakcijā, kas bija spēkā pirms Īstenošanas lēmuma 2016/2297 stāšanās spēkā, – 4. panta 1. punkta a) apakšpunktā dalībvalstu kompetentajām iestādēm atzītā iespēja aizliegt personas datu pārsūtīšanu uz trešo valsti, kas nosūtītājam uzliek pienākumus, kuri nav saderīgi ar šajās pašās klauzulās ietvertajām garantijām, pierāda, ka trešās valsts tiesiskais regulējums var pamatot datu nosūtīšanas aizliegumu, pat ja tas ir veikts, pamatojoties uz LSK lēmuma pielikumā ietvertajām datu aizsardzības standartklauzulām, un tādējādi atklāj, ka ar tām var nebūt pietiekami, lai nodrošinātu pienācīgu aizsardzību. Tālab iesniedzējtiesa vēlas noskaidrot, cik plašas ir komisāra pilnvaras aizliegt datu pārsūtīšanu, pamatojoties uz šīm klauzulām, vienlaikus uzskatot, ka diskrecionārās pilnvaras nav pietiekamas, lai nodrošinātu pienācīgu aizsardzību.

68 Šādos apstākļos *High Court* (Augstā tiesa) nolēma apturēt tiesvedību un uzdot Tiesai šādus prejudiciālus jautājumus:

"1) Vai – apstākļos, kad privāts uzņēmums no [Savienības] dalībvalsts saskaņā ar [LSK lēmumu] komerciāliem mērķiem pārsūta personas datus privātam uzņēmumam trešajā valstī, kurā turpmāk šīs trešās valsts iestādes var tos apstrādāt ne vien valsts drošības vajadzībām, bet arī šīs trešās valsts tiesībaizsardzības un ārlietu vajadzībām, – attiecībā uz šo datu pārsūtīšanu ir piemērojami

Savienības tiesību akti, tostarp Harta, neraugoties uz LES 4. panta 2. punkta noteikumiem par valsts drošību un Direktīvas [95/46] 3. panta 2. punkta pirmā ievilkuma noteikumiem attiecībā uz sabiedrisko drošību, aizsardzību un valsts drošību?

2) a) Vai Direktīvas [95/46] izpratnē atbilstoša mēraukla, lai noteiktu, vai ir noticis fiziskas personas tiesību pārkāpums, saskaņā ar [LSK lēmumu] veicot datu pārsūtīšanu no [Savienības] uz trešo valsti, kur tos vēlāk varētu apstrādāt valsts drošības nolūkos, ir:
   i) Harta, LES, LESD, Direktīva [95/46], [Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencija, kas parakstīta Romā 1950. gada 4. novembrī (turpmāk tekstā – "ECPAK")] (vai jebkura cita [Savienības] tiesību norma), vai
   ii) vienas vai vairāku dalībvalstu valsts tiesību normas?

   b) Vai – gadījumā, ja atbilstošā mēraukla ir ii) iedaļā minētās tiesību normas, – šajā mērauklā ir iekļaujami arī pasākumi, kas vienā vai vairākās dalībvalstīs tiek veikti saistībā ar valsts drošību?

3) Vai, vērtējot to, vai personas datiem, kas saskaņā ar Direktīvas [95/46] 26. pantu tiek pārsūtīti uz trešo valsti, šī valsts nodrošina tādu aizsardzības līmeni, kāds tiek prasīts Savienības tiesību aktos, šajā trešajā valstī esošais aizsardzības līmenis ir jāvērtē atsaucoties uz:
   a) trešajā valstī piemērojamajiem noteikumiem, kas izriet no tās valsts tiesībām vai starptautiskajām saistībām, un praksi, ar kuru paredzēts nodrošināt šo noteikumu ievērošanu, tostarp šajā trešajā valstī ievērotajām profesionālās ētikas normām un veiktajiem drošības pasākumiem;

   vai

   b) noteikumiem, kas minēti a) daļā, kopā ar tādu administratīvo, regulēšanas un īstenošanas praksi un aizsardzības pasākumu politiku, procedūrām, protokoliem, pārraudzības mehānismiem un ārpustiesas tiesību aizsardzības līdzekļiem, kādi ir spēkā trešajā valstī?

4) Vai – ņemot vērā *High Court* (Augstā tiesa) konstatētos faktus par ASV tiesībām – ar fiziskas personas datu pārsūtīšanu no [Savienības] uz ASV saskaņā ar [LSK lēmumu] tiek pārkāptas Hartas 7. vai 8. pantā paredzētās fizisko personu tiesības?

5) Vai – ņemot vērā *High Court* (Augstā tiesa) konstatētos faktus par ASV tiesībām – personas datu pārsūtīšanā no [Savienības] uz ASV saskaņā ar [LSK lēmumu]:
   a) ar ASV nodrošināto aizsardzības līmeni tiek ievērota pati būtība, kas piemīt tiesībām – kuras Hartas 47. pantā ir garantētas fiziskajai personai – vērsties tiesā gadījumā, ja ir pārkāptas tās tiesības uz personas datu aizsardzību?

   Ja atbilde uz piektā jautājuma a) daļā esošo jautājumu ir apstiprinoša:

   b) vai ierobežojumi, ko ASV valsts drošības kontekstā fiziskas personas tiesībām vērsties tiesā paredz ASV tiesību akti, ir samērīgi Hartas 52. panta izpratnē un nepārsniedz to, kas ir vajadzīgs demokrātiskā sabiedrībā valsts drošības nolūkos?

6) a) Kāda līmeņa aizsardzība – Direktīvas [95/46] tiesību normu, it īpaši tās 25. un 26. panta kontekstā, lasot tos kopsakarā ar Hartu – ir jānodrošina personas datiem, kas uz trešo valsti pārsūtīti atbilstoši līguma standartklauzulām, kuras pieņemtas, pamatojoties uz Komisijas lēmumu saskaņā ar [Direktīvas 95/46] 26. panta 4. punktu?
   b) Kas ir jāņem vērā, vērtējot, vai aizsardzības līmenis, kas tiek nodrošināts datiem, kuri tiek pārsūtīti uz trešo valsti saskaņā ar [LSK lēmumu], atbilst Direktīvas [95/46] un Hartas prasībām?

7) Vai tas, ka aizsardzības standartklauzulas ir piemērojamas attiecībās starp datu nosūtītāju un datu saņēmēju un nav saistošas trešās valsts iestādēm, kuras savu drošības dienestu labā varētu pieprasīt no datu saņēmēja piekļuvi, lai turpmāk apstrādātu datus, kas pārsūtīti saskaņā ar [LSK lēmumā] paredzētajam klauzulām, izslēdz, ka šajās klauzulās tiek sniegtas atbilstošas garantijas, kā paredzēts Direktīvas [95/46] 26. panta 2. punktā?

8) Vai – gadījumā, ja attiecībā uz trešajā valstī esošo datu saņēmēju ir piemērojami pretizlūkošanas tiesību akti, kas, datu aizsardzības iestādes ieskatā, ir pretrunā aizsardzības standartklauzulām vai Direktīvas [95/46] 25. un 26. pantam vai Hartai – personas datu aizsardzības iestādei ir pienākums izmantot īstenošanas pilnvaras, kas tai ir paredzētas Direktīvas [95/46] 28. panta 3. punktā, lai apturētu datu plūsmu, vai tomēr šādu pilnvaru izmantošana ir ierobežota, to paredzot tikai ārkārtas gadījumiem, ņemot vērā [LSK lēmuma] 11. apsvērumu, vai arī personas datu aizsardzības iestāde var izmantot savu rīcības brīvību neapturēt datu plūsmu?

9) a) Vai – Direktīvas [95/46] 25. panta 6. punkta izpratnē – [PV] lēmums ir vispārpiemērojams un dalībvalstu datu aizsardzības iestādēm un tiesām saistošs konstatējums, ka ASV nodrošina pietiekamu aizsardzības līmeni Direktīvas [95/46] 25. panta 2. punkta izpratnē ar savu valsts tiesību vai noslēgto starptautisko saistību palīdzību?
   b) Kāda – gadījumā, ja atbildams noliedzoši, – ir [PV] lēmuma nozīme, ja tāda ir, vērtējumā par aizsardzības pasākumu līmeņa pienācīgumu, kas tiek nodrošināti personas datiem, kuri tiek pārsūtīti uz Amerikas Savienotajām Valstīm saskaņā ar [LSK lēmumu]?

10) Vai, ņemot vērā *High Court* (Augstā tiesa) atzinumus par ASV tiesībām, [PV] lēmuma III pielikuma A pielikumā rodamais noteikums par "privātuma vairoga" ombudu, aplūkojot to kopsakarā ar ASV pastāvošo kārtību, nodrošina, ka datu subjektiem, kuru personas dati tiek pārsūtīti uz ASV saskaņā ar [LSK lēmumu], ASV paredz tādus tiesību aizsardzības līdzekļus, kas ir saderīgi ar Hartas 47. pantu?

11) Vai ar [LSK lēmumu] tiek pārkāpts Hartas 7., 8. vai 47. pants?"

Par lūguma sniegt prejudiciālu nolēmumu pieņemamību

69 *Facebook Ireland*, kā arī Vācijas un Apvienotās Karalistes valdības apgalvo, ka lūgums sniegt prejudiciālu nolēmumu nav pieņemams.

70 *Facebook Ireland* par tās izvirzīto iebildi norāda, ka Direktīvas 95/46 normas, uz kurām ir balstīti prejudiciālie jautājumi, ir atceltas ar VDAR.

71 Šajā ziņā jānorāda, ka, lai gan Direktīva 95/46 saskaņā ar VDAR 94. panta 1. punktu no 2018. gada 25. maija patiešām tika atcelta, tā vēl bija spēkā brīdī, kad 2018. gada 4. maijā tika formulēts šis lūgums sniegt prejudiciālu nolēmumu, kas Tiesā saņemts 2018. gada 9. maijā. Turklāt Direktīvas 95/46 3. panta 2. punkta pirmais ievilkums, 25. un 26. pants, kā arī 28. panta 3. punkts, uz kuriem ir atsauce prejudiciālajos jautājumos, būtībā ir pārņemti attiecīgi VDAR 2. panta 2. punktā, kā arī tās 45., 46. un 58. pantā. Jāatgādina arī, ka Tiesas uzdevums ir interpretēt visas Savienības tiesību normas, kas valsts tiesām ir vajadzīgas, lai tās varētu izskatīt attiecīgās lietas, pat ja šīs normas nav tieši norādītas jautājumos, kurus tai ir iesniegušas šīs tiesas (spriedums, 2020. gada 2. aprīlis, *Ruska Federacija*, C-897/19 PPU, EU:C:2020:262, 43. punkts un tajā minētā judikatūra). Šo dažādo iemeslu dēļ apstāklis, ka iesniedzējtiesa prejudiciālos jautājumus ir formulējusi, atsaucoties vienīgi uz Direktīvas 95/46 normām, nav iemesls šo lūgumu sniegt prejudiciālu nolēmumu atzīt par nepieņemamu.

72 Savukārt Vācijas valdība savu iebildi par nepieņemamību pamato ar apstākli, pirmkārt, ka komisārs ir paudis tikai šaubas, nevis galīgo viedokli par LSK lēmuma spēkā esamību un, otrkārt, ka iesniedzējtiesa nav pārbaudījusi, vai *M. Schrems* neapšaubāmi ir devis savu piekrišanu datu nosūtīšanai pamatlietā, kas – ja tas tā būtu bijis – atbildi uz šo jautājumu padarītu nelietderīgu. Visbeidzot, pēc Apvienotās Karalistes valdības domām, prejudiciālie jautājumi ir hipotētiski, jo šī tiesa nav konstatējusi, ka šie dati patiešām ir tikuši pārsūtīti, pamatojoties uz minēto lēmumu.

73 No Tiesas pastāvīgās judikatūras izriet, ka vienīgi valsts tiesa, kas izskata strīdu un uzņemas atbildību par tālāko tiesas nolēmumu, var, izvērtējot katras konkrētās lietas apstākļus, noteikt gan prejudiciāla nolēmuma nepieciešamību sprieduma taisīšanas vajadzībām, gan Tiesai uzdoto jautājumu nozīmību. Līdz ar to, ja uzdotie jautājumi attiecas uz Savienības tiesību normas interpretāciju vai spēkā esamību, Tiesai principā ir par tiem jālemj. No tā izriet, ka uz jautājumiem par Savienības tiesībām ir attiecināms atbilstības pieņēmums. Atteikties lemt par valsts tiesas uzdotu prejudiciālo jautājumu Tiesa var tikai tad, ja lūgtajai interpretācijai nav nekāda sakara ar pamatlietas apstākļiem vai tās priekšmetu, ja problēmai ir hipotētisks raksturs vai arī ja Tiesai nav zināmi faktiskie un tiesību apstākļi, kas vajadzīgi, lai sniegtu lietderīgu atbildi uz minētajiem jautājumiem (spriedumi, 2015. gada 16. jūnijs, *Gauweiler* u.c., C-62/14, EU:C:2015:400, 24. un 25. punkts; 2018. gada 2. oktobris, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 45. punkts, kā arī 2019. gada 19. decembris, *Dobersberger*, C-16/18, EU:C:2019:1110, 18. un 19. punkts).

74 Šajā gadījumā lēmumā par prejudiciālu jautājumu uzdošanu ir ietverta pietiekama informācija par faktiskajiem un tiesību apstākļiem, lai varētu izprast prejudiciālo jautājumu tvērumu. Turklāt un galvenokārt – nekas Tiesas rīcībā esošajos lietas materiālos neļauj uzskatīt, ka lūgtajai Savienības tiesību interpretācijai nebūtu nekāda sakara ar pamatlietas faktisko situāciju vai priekšmetu vai ka tā būtu hipotētiska, it īpaši tādēļ, ka pamatlietā aplūkotā personas datu pārsūtīšana būtu balstīta uz datu subjekta skaidru piekrišanu šai pārsūtīšanai, nevis uz LSK lēmumu. Proti, saskaņā ar šajā lūgumā ietvertajām norādēm *Facebook Ireland* ir atzinusi, ka tā pārsūta *Facebook Inc.* savu Savienībā dzīvojošo lietotāju personas datus un ka liela daļa šo sūtījumu, kuru likumību *M. Schrems* apstrīd, tiek veikti, pamatojoties uz LSK lēmuma pielikumā ietvertajām datu aizsardzības standartklauzulām.

75 Turklāt šī lūguma sniegt prejudiciālu nolēmumu pieņemamību neietekmē tas, ka komisārs nav izteicis galīgo viedokli par šī lēmuma spēkā esamību, jo iesniedzējtiesa uzskata, ka atbilde uz prejudiciālajiem jautājumiem par Savienības tiesību normu interpretāciju un spēkā esamību ir nepieciešama pamatlietas atrisināšanai.

76 No tā izriet, ka lūgums sniegt prejudiciālu nolēmumu ir pieņemams.

Par prejudiciālajiem jautājumiem

77 Vispirms jāatgādina, ka šis lūgums sniegt prejudiciālu nolēmumu ir balstīts uz *M. Schrems* sūdzību nolūkā panākt, lai komisārs apturētu vai nākotnē aizliegtu *Facebook Ireland* pārsūtīt personas datus *Facebook Inc.* Lai gan prejudiciālajos jautājumos ir atsauce uz Direktīvas 95/46 noteikumiem, ir skaidrs, ka komisārs vēl nebija pieņēmis galīgo lēmumu par šo sūdzību, kad no 2018. gada 25. maija šī direktīva tika atcelta un aizstāta ar VDAR.

78 Šī valsts lēmuma neesamība nošķir pamatlietā aplūkoto situāciju no situācijām, kurās tika pasludināti 2019. gada 24. septembra spriedums *Google* (Atsauču atsaistīšanas teritoriālā piemērojamība) (C-507/17, EU:C:2019:772) un 2019. gada 1. oktobra spriedums *Planet49* (C-673/17, EU:C:2019:801), kuros tika aplūkoti lēmumi, kas bija pieņemti pirms minētās direktīvas atcelšanas.

79 Līdz ar to uz prejudiciālajiem jautājumiem ir jāatbild, ņemot vērā VDAR, nevis Direktīvas 95/46 noteikumus.

Par pirmo jautājumu

80 Ar pirmo jautājumu iesniedzējtiesa būtībā vēlas noskaidrot, vai VDAR 2. panta 1. punkts un 2. panta 2. punkta a), b) un d) apakšpunkts, lasot tos kopsakarā ar LES 4. panta 2. punktu, ir jāinterpretē tādējādi, ka šīs regulas piemērošanas jomā ietilpst personas datu pārsūtīšana, ko kādā dalībvalstī reģistrēts tirgus dalībnieks veic citam tirgus dalībniekam, kurš ir reģistrēts trešajā valstī, ja šīs pārsūtīšanas laikā vai pēc tam šie dati var tikt apstrādāti šīs trešās valsts iestādes sabiedriskās drošības, aizsardzības un valsts drošības nolūkā.

81 Šajā ziņā vispirms ir jānorāda, ka LES 4. panta 2. punktā ietvertā tiesību norma, saskaņā ar kuru Savienībā valsts drošība ir vienīgi katras dalībvalsts pašas atbildība, attiecas tikai uz Savienības dalībvalstīm. Līdz ar to šī tiesību norma šajā gadījumā nav atbilstoša, lai interpretētu VDAR 2. panta 1. punktu un 2. panta 2. punkta a), b) un d) apakšpunktu.

82 Atbilstoši VDAR 2. panta 1. punktam to piemēro personas datu apstrādei, kas pilnībā vai daļēji veikta ar automatizētiem līdzekļiem, un tādu personas datu apstrādei, kuri veido daļu no kartotēkas vai ir paredzēti, lai veidotu daļu no kartotēkas, ja apstrādi neveic ar automatizētiem līdzekļiem. Šīs regulas 4. panta 2. punktā jēdziens "apstrāde" ir definēts kā "jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem", un kā piemēri tajā ir minēti "izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus", nenošķirot, vai šīs darbības tiek veiktas Savienībā vai arī tām ir saikne ar trešo valsti. Turklāt minētajā regulā personas datu nosūtīšana uz trešajām valstīm ir pakļauta īpašiem noteikumiem, kas ietverti tās V nodaļā "Personas datu nosūtīšana uz trešām valstīm vai starptautiskām organizācijām", un turklāt uzraudzības iestādēm šajā ziņā ir piešķirtas īpašas pilnvaras, kas ietvertas šīs pašas regulas 58. panta 2. punkta j) apakšpunktā.

83 No tā izriet, ka darbība, kas ietver personas datu nosūtīšanu no dalībvalsts uz trešo valsti kā tāda ir personas datu apstrāde VDAR 4. panta 2. punkta izpratnē, kas veikta dalībvalsts teritorijā, un šai apstrādei minētā regula ir piemērojama atbilstoši tās 2. panta 1. punktam (pēc analoģijas attiecībā uz Direktīvas 95/46 2. panta b) punktu un 3. panta 1. punktu skat. spriedumu, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 45. punkts un tajā minētā judikatūra).

84 Attiecībā uz jautājumu, vai šāda darbība var tikt uzskatīta par izslēgtu no VDAR piemērošanas jomas saskaņā ar tās 2. panta 2. punktu, ir jāatgādina, ka šajā tiesību normā ir paredzēti izņēmumi no šīs regulas piemērošanas jomas, kas definēta tās 2. panta 1. punktā, un ka šie izņēmumi ir jāinterpretē šauri (pēc analoģijas attiecībā uz Direktīvas 95/46 3. panta 2. punktu skat. spriedumu, 2018. gada 10. jūlijs, *Jehovan todistajat*, C-25/17, EU:C:2018:551, 37. punkts un tajā minētā judikatūra).

85 Šajā gadījumā, tā kā pamatlietā aplūkoto personas datu nosūtīšana notika no *Facebook Ireland* uz *Facebook Inc.*, proti, starp divām juridiskām personām, tai nav piemērojams VDAR 2. panta 2. punkta c) apakšpunkts, kas attiecas uz datu apstrādi, ko veic fiziska persona tikai personiskas vai mājsaimnieciskas darbības gaitā. Uz minēto nosūtīšanu neattiecas arī šīs regulas 2. panta 2. punkta a), b) un d) apakšpunktos ietvertie izņēmumi, jo darbības, kas kā piemēri tajos ir minētas, katrā ziņā ir valsts vai valsts iestāžu darbības, kas neietilpst privātpersonu darbību jomās (pēc analoģijas attiecībā uz Direktīvas 95/46 3. panta 2. punktu skat. spriedumu, 2018. gada 10. jūlijs, *Jehovan todistajat*, C-25/17, EU:C:2018:551, 38. punkts un tajā minētā judikatūra).

86 Iespējamība, ka personas datus, kas tiek pārsūtīti starp diviem tirgus dalībniekiem komerciālos nolūkos, nosūtīšanas laikā vai pēc tam attiecīgās trešās valsts iestādes apstrādā sabiedrības drošības, aizsardzības un valsts drošības nolūkā, nevar izslēgt minēto nosūtīšanu no VDAR piemērošanas jomas.

87 Turklāt, skaidri nosakot Komisijai pienākumu, kad tā vērtē trešās valsts nodrošinātā aizsardzības līmeņa pietiekamību, ņemt vērā it īpaši "attiecīgos tiesību aktus, gan vispārējos, gan nozaru, tostarp attiecībā uz sabiedrisko drošību, aizsardzību, valsts drošību un krimināltiesībām un publisko iestāžu piekļuvi

personas datiem, kā arī šādu tiesību aktu, datu aizsardzības noteikumu, dienesta noteikumu un drošības pasākumu īstenošanu", ar pašu šīs regulas 45. panta 2. punkta a) apakšpunkta formulējumu tiek uzsvērts apstāklis, ka iespēja, ka trešajā valstī attiecīgie dati var tikt apstrādāti sabiedrības drošības, aizsardzības un valsts drošības nolūkā, nerada šaubas par minētās regulas piemērojamību attiecīgajai datu nosūtīšanai.

88 No tā izriet, ka šāda nosūtīšana nevar būt ārpus VDAR piemērošanas jomas, jo attiecīgos datus attiecīgās trešās valsts iestādes šīs nosūtīšanas laikā vai pēc tam var apstrādāt sabiedrības drošības, aizsardzības un valsts drošības nolūkā.

89 Līdz ar to uz pirmo jautājumu ir jāatbild, ka VDAR 2. panta 1. un 2. punkts ir jāinterpretē tādējādi, ka šīs regulas piemērošanas jomā ietilpst personas datu pārsūtīšana, ko kādā dalībvalstī reģistrēts tirgus dalībnieks komerciālā nolūkā veic citam tirgus dalībniekam, kurš ir reģistrēts trešajā valstī, neraugoties uz iespēju, ka šīs pārsūtīšanas laikā vai pēc tam šos datus attiecīgās trešās valsts iestādes var apstrādāt sabiedrības drošības, aizsardzības un valsts drošības nolūkā.

Par otro, trešo un sesto jautājumu

90 Ar otro, trešo un sesto jautājumu iesniedzējtiesa būtībā jautā Tiesai par aizsardzības līmeni, kāds ir prasīts VDAR 46. panta 1. punktā un 2. punkta c) apakšpunktā saistībā ar personas datu nosūtīšanu uz trešo valsti, pamatojoties uz datu aizsardzības standartklauzulām. It īpaši šī tiesa lūdz Tiesu precizēt elementus, kas būtu jāņem vērā, lai noteiktu, vai minētās nosūtīšanas kontekstā šāds aizsardzības līmenis tiek nodrošināts.

91 Attiecībā uz nepieciešamo aizsardzības līmeni no šīm tiesību normām, skatītām kopsakarā, izriet, ka tad, ja nav atbilstoši šīs regulas 45. panta 3. punktam pieņemta lēmuma par aizsardzības līmeņa pietiekamību, pārzinis vai apstrādātājs personas datus var nosūtīt uz trešo valsti tikai tad, ja tajā ir paredzētas "atbilstošas garantijas", un ar nosacījumu, ka datu subjektiem ir "īstenojamas [..] tiesības un efektīvi tiesiskās aizsardzības līdzekļi", un šīs atbilstošās garantijas tostarp var tikt sniegtas ar Komisijas pieņemtām datu aizsardzības standartklauzulām.

92 Lai gan VDAR 46. pantā nav precizēts to prasību raksturs, kas izriet no šīs atsauces uz "attiecīgajām garantijām", "īstenojamām tiesībām" un "efektīviem tiesību aizsardzības līdzekļiem", ir jānorāda, ka šis pants ir ietverts šīs regulas V nodaļā un līdz ar to minētais pants ir jāskata kopā ar šīs regulas 44. pantu "Nosūtīšanas vispārīgie principi", kurā ir noteikts, ka "[p]iemēro visus [šīs] nodaļas noteikumus, lai nodrošinātu, ka nemazinās ar šo regulu garantētais fizisku personu aizsardzības līmenis". Līdz ar to šis aizsardzības līmenis ir jānodrošina neatkarīgi no tā, kura ir tā šīs nodaļas norma, uz kā pamata tiek veikta personas datu nosūtīšana uz trešo valsti.

93 Kā secinājumu 117. punktā ir norādījis ģenerāladvokāts, VDAR V nodaļas noteikumu mērķis ir nodrošināt ar šo regulu garantētā personas datu aizsardzības augstā līmeņa nepārtrauktību, pārsūtot datus ārpus Savienības, atbilstoši šīs regulas 6. apsvērumā precizētajam mērķim.

94 VDAR 45. panta 1. punkta pirmajā teikumā ir paredzēts, ka personas datu nosūtīšanu uz trešo valsti var veikt, ja Komisija ir nolēmusi, ka trešā valsts, kāda šīs trešās valsts teritorija vai viens vai vairāki konkrēti tajā norādīti sektori nodrošina pietiekamu aizsardzības līmeni. Šajā ziņā, nepieprasot, lai attiecīgā trešā valsts garantētu tādu pašu aizsardzības līmeni kā Savienības tiesību sistēmā garantētais, jēdziens "pietiekams aizsardzības līmenis", kā to apliecina šīs regulas 104. apsvērums, ir jāsaprot tādējādi, ka 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 minēto regulu, to lasot Hartas kontekstā, ir garantēts Savienībā. Faktiski, ja

šādas prasības nebūtu, iepriekšējā punktā minētais mērķis netiktu ievērots (pēc analoģijas attiecībā uz Direktīvas 95/46 25. panta 6. punktu skat. spriedumu, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 73. punkts).

95 Šajā kontekstā VDAR 107. apsvērumā ir noteikts, ka tad, ja "trešā valsts, kāda teritorija vai konkrēts sektors trešā valstī [..] vairs nenodrošina pietiekamu datu aizsardzības līmeni [..], personas datu pārsūtīšana uz trešo valsti [..] būtu jāaizliedz, ja vien nav izpildītas šīs regulas prasības attiecībā uz nosūtīšanu, kam piemēro atbilstošas garantijas [..]". Šajā ziņā minētās regulas 108. apsvērumā ir precizēts – kamēr nav pieņemts lēmums par aizsardzības līmeņa pietiekamību, attiecīgajām garantijām, kuras saskaņā ar šīs pašas regulas 46. panta 1. punktu ir jāsniedz personas datu pārzinim vai apstrādātājam, ir "jākompensē datu aizsardzības trūkumi trešajā valstī", lai "tiktu ievērotas datu aizsardzības prasības un datu subjektu tiesības atbilstīgi Savienībā veiktai apstrādei".

96 No tā izriet, kā ģenerāladvokāts ir norādījis secinājumu 115. punktā, ka šīm atbilstošām garantijām ir jābūt tādām, lai nodrošinātu, ka personām, kuru personas dati, pamatojoties uz datu aizsardzības standartklauzulām, tiek pārsūtīti uz trešo valsti, tiek nodrošināts tāds aizsardzības līmenis, kas būtībā ir līdzvērtīgs Savienībā garantētajam līmenim, gluži kā gadījumā, kad nosūtīšana notiek, pamatojoties uz lēmumu par aizsardzības līmeņa pietiekamību.

97 Iesniedzējtiesa šaubās arī par to, vai šis, Savienībā garantētajam būtībā līdzvērtīgais, aizsardzības līmenis ir jānosaka, ņemot vērā Savienības tiesības, it īpaši Hartā garantētās tiesības, un/vai Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijā (turpmāk tekstā – "ECPAK") noteiktās pamattiesības, vai arī dalībvalstu tiesības.

98 Šajā ziņā ir jāatgādina, ka, lai gan – kā to apliecina LES 6. panta 3. punkts – pamattiesības, kas atzītas ECPAK, kā vispārējie principi ir daļa no Savienības tiesībām un lai gan Hartas 52. panta 3. punktā ir paredzēts, ka tajā ietvertajām tiesībām, kas atbilst ECPAK garantētajām tiesībām, ir tāda pati nozīme un apjoms, kāds tām ir noteikts minētajā konvencijā, šī pēdējā minētā konvencija, kamēr Savienība nav tai pievienojusies, nav Savienības tiesību sistēmā formāli integrēts juridisks instruments (spriedumi, 2013. gada 26. februāris, *Åkerberg Fransson*, C-617/10, EU:C:2013:105, 44. punkts un tajā minētā judikatūra, kā arī 2018. gada 20. marts, *Menci*, C-524/15, EU:C:2018:197, 22. punkts).

99 Šādos apstākļos Tiesa ir nospriedusi, ka Savienības tiesību interpretācija, kā arī Savienības tiesību aktu spēkā esamības pārbaude ir jāveic, ņemot vērā Hartā garantētās pamattiesības (pēc analoģijas skat. spriedumu, 2018. gada 20. marts, *Menci*, C-524/15, EU:C:2018:197, 24. punkts).

100 Turklāt saskaņā ar pastāvīgo judikatūru Savienības tiesību normu spēkā esamība un, ja nav tiešas norādes uz dalībvalstu tiesībām, to interpretācija nevar tikt izvērtēta, ņemot vērā šīs valsts tiesības, pat konstitucionāla līmeņa tiesības, it īpaši pamattiesības, kādas tās ir formulētas valsts konstitūcijā (šajā nozīmē skat. spriedumus, 1970. gada 17. decembris, *Internationale Handelsgesellschaft*, 11/70, EU:C:1970:114, 3. punkts; 1979. gada 13. decembris, *Hauer*, 44/79, EU:C:1979:290, 14. punkts, kā arī 2016. gada 18. oktobris, *Nikiforidis*, C-135/15, EU:C:2016:774, 28. punkts un tajā minētā judikatūra).

101 No tā izriet – tā kā, pirmkārt, tāda personas datu nosūtīšana kā pamatlietā, ko komerciālos nolūkos veic vienā dalībvalstī reģistrēts tirgus dalībnieks citam tirgus dalībniekam, kurš ir reģistrēts trešajā valstī, kā tas izriet no atbildes uz pirmo jautājumu, ietilpst VDAR piemērošanas jomā un, otrkārt, šīs regulas mērķis, kā minēts tās 10. apsvērumā, ir nodrošināt konsekventu un augsta līmeņa aizsardzību fiziskām personām Savienībā un šai nolūkā noteikumu par šo personu pamattiesību un pamatbrīvību aizsardzību attiecībā uz personas datu apstrādi vienveidīgu piemērošanu visā Savienībā, minētās regulas 46. panta 1. punktā prasītais pamattiesību aizsardzības līmenis ir jānosaka, balstoties uz šīs pašas regulas normām, skatot tos kopā ar Hartā garantētajām pamattiesībām.

102 Iesniedzējtiesa vēl vēlas arī noskaidrot, kādi apstākļi ir jāņem vērā, lai noteiktu aizsardzības līmeņa pietiekamību saistībā ar personas datu pārsūtīšanu uz trešo valsti, pamatojoties uz datu aizsardzības standartklauzulām, kas pieņemtas saskaņā ar VDAR 46. panta 2. punkta c) apakšpunktu.

103 Šajā ziņā, lai gan šajā tiesību normā nav uzskaitīti dažādie elementi, kas ir jāņem vērā, lai novērtētu, vai aizsardzības līmenis, kas jāievēro šādas nosūtīšanas ietvaros, ir pietiekams, šīs regulas 46. panta 1. punktā ir precizēts, ka datu subjektiem ir jāsaņem atbilstīgas garantijas un jābūt pieejamām īstenojamām datu subjekta tiesībām un efektīviem tiesiskās aizsardzības līdzekļiem.

104 Veicot tam nepieciešamo izvērtējumu šādas pārsūtīšanas kontekstā, tostarp ir jāņem vērā gan līguma noteikumi, par kuriem ir panākta vienošanās starp Savienībā reģistrēto personas datu pārzini vai apstrādātāju un attiecīgajā trešajā valstī reģistrēto pārsūtīto datu saņēmēju, gan arī – attiecībā uz šīs trešās valsts publisko iestāžu iespējamo piekļuvi nosūtītajiem personas datiem – šīs trešās valsts tiesību sistēmas atbilstošie elementi. Šajā pēdējā aspektā jānorāda, ka minētās regulas 46. panta kontekstā ir jāņem vērā tie paši elementi, kas izsmeļoši uzskaitīti tās 45. panta 2. punktā.

105 Līdz ar to uz otro, trešo un sesto jautājumu ir jāatbild, ka VDAR 46. panta 1. punkts un 2. punkta c) apakšpunkts ir jāinterpretē tādējādi, ka šajās tiesību normās paredzētajām atbilstošajām garantijām, izmantojamajām tiesībām un efektīvajiem tiesību aizsardzības līdzekļiem ir jānodrošina, lai to personu tiesībām, kuru personas dati tiek pārsūtīti uz trešo valsti, pamatojoties uz datu aizsardzības standartklauzulām, tiktu piemērots būtībā līdzvērtīgs aizsardzības līmenis tam, kāds ir garantēts Savienībā ar šo regulu, lasot to kopā ar Hartu. Šajā ziņā, novērtējot aizsardzības līmeni, kāds tiek nodrošināts šādas pārsūtīšanas kontekstā, it īpaši ir jāņem vērā gan līguma noteikumi, par kuriem ir panākta vienošanās starp personas datu pārzini vai apstrādātāju, kas reģistrēts Savienībā, un attiecīgajā trešajā valstī reģistrēto saņēmēju, gan – attiecībā uz iespējamu šīs trešās valsts publisko iestāžu piekļuvi šādi pārsūtītajiem personas datiem – šīs trešās tiesību sistēmas būtiskie elementi, it īpaši minētās regulas 45. panta 2. punktā nosauktie.

Par astoto jautājumu

106 Ar astoto jautājumu iesniedzējtiesa būtībā vēlas noskaidrot, vai VDAR 58. panta 2. punkta f) un j) apakšpunkts ir jāinterpretē tādējādi, ka kompetentajai uzraudzības iestādei ir jāaptur vai jāaizliedz tāda personas datu pārsūtīšana uz trešo valsti, kuras pamatā ir Komisijas pieņemtās datu aizsardzības standartklauzulas, ja šī uzraudzības iestāde uzskata, ka šīs klauzulas šajā trešajā valstī netiek vai nevar tikt ievērotas un ka pārsūtīto datu aizsardzība, kāda tā prasīta Savienības tiesībās, konkrēti, VDAR 45. un 46. pantā un Hartā, nevar tikt nodrošināta, vai arī šīs iestādes pilnvaru izmantošana aprobežojas vien ar ārkārtas gadījumiem.

107 Saskaņā ar Hartas 8. panta 3. punktu, kā arī VDAR 51. panta 1. punktu un 57. panta 1. punkta a) apakšpunktu valsts uzraudzības iestāžu pienākums ir pārbaudīt, vai ir ievēroti Savienības noteikumi par fizisku personu aizsardzību attiecībā uz personas datu apstrādi. Tādējādi katrai no tām ir kompetence pārbaudīt, vai personas datu pārsūtīšana no dalībvalsts, kurā tā atrodas, uz trešo valsti atbilst šajā regulā noteiktajām prasībām (pēc analoģijas attiecībā uz Direktīvas 95/46 28. pantu skat. spriedumu, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 47. punkts).

108 No šīm tiesību normām izriet, ka uzraudzības iestāžu pirmais uzdevums ir kontrolēt VDAR piemērošanu un uzraudzīt tās ievērošanu. Šī uzdevuma veikšanai ir īpaša nozīme personas datu pārsūtīšanas uz trešo valsti kontekstā, jo, kā izriet no šīs regulas 116. apsvēruma paša formulējuma, "personas datu pārvietošanās pāri robežām ārpus Savienības var ievērojami ietekmēt fizisko personu spējas īstenot tiesības uz datu aizsardzību, jo īpaši, lai aizsargātu sevi pret nelikumīgu izmantošanu vai šādas informācijas atklāšanu". Šādā gadījumā, kā precizēts tajā pašā apsvērumā, "vienlaikus uzraudzības iestādes var saskarties ar situāciju, ka tās nevar reaģēt uz sūdzībām vai veikt izmeklēšanu saistībā ar darbībām, kas norisinās robežu otrā pusē".

109 Turklāt saskaņā ar VDAR 57. panta 1. punkta f) apakšpunktu katrai uzraudzības iestādei savā teritorijā ir pienākums izskatīt sūdzības, kuras ikvienai personai saskaņā ar šīs regulas 77. panta 1. punktu ir tiesības iesniegt, ja tā uzskata, ka tās personas datu apstrāde ir minētās regulas pārkāpums, un, ciktāl nepieciešams, izmeklēt attiecīgo jautājumu. Uzraudzības iestādei šāda sūdzība ir jāizskata ar pienācīgu rūpību (pēc analoģijas attiecībā uz Direktīvas 95/46 25. panta 6. punktu skat. spriedumu, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 63. punkts).

110 VDAR 78. panta 1. un 2. punktā ikvienai personai ir atzītas tiesības uz efektīvu tiesību aizsardzību, tostarp tad, ja uzraudzības iestāde neizskata tās sūdzību. Šīs regulas 141. apsvērumā ir arī atsauce uz šīm "tiesībām uz efektīvu tiesību aizsardzību tiesā saskaņā ar Hartas 47. pantu", ja šī uzraudzības iestāde "nerīkojas, kad šāda rīcība ir nepieciešama, lai aizsargātu datu subjekta tiesības".

111 Iesniegto sūdzību izskatīšanai VDAR 58. panta 1. punktā katrai uzraudzības iestādei ir piešķirtas ievērojamas izmeklēšanas pilnvaras. Ja šī iestāde izmeklēšanas noslēgumā uzskata, ka attiecīgajai personai, kuras personas dati ir pārsūtīti uz trešo valsti, tajā nav pieejams pietiekams aizsardzības līmenis, šai iestādei, piemērojot Savienības tiesības, ir atbilstoši jārīkojas, lai labotu konstatēto trūkumu, neatkarīgi no šī trūkuma izcelsmes vai rakstura. Šajā nolūkā šīs regulas 58. panta 2. punktā ir uzskaitīti dažādi koriģējošie pasākumi, ko uzraudzības iestāde var veikt.

112 Lai gan piemērota un nepieciešama līdzekļa izvēle ir uzraudzības iestādes kompetencē un tai šī izvēle ir jāizdara, ņemot vērā visus attiecīgos personas datu pārsūtīšanas apstākļus, šai iestādei tomēr ir pienākums ar pienācīgu rūpību izpildīt savu uzdevumu nodrošināt pilnīgu VDAR ievērošanu.

113 Šajā ziņā, kā ģenerāladvokāts arī ir norādījis secinājumu 148. punktā, minētajai iestādei saskaņā ar šīs regulas 58. panta 2. punkta f) un j) apakšpunktu ir jāaptur vai jāaizliedz personas datu pārsūtīšana uz trešo valsti, ja tā, ņemot vērā visus ar šo pārsūtīšanu saistītos apstākļus, uzskata, ka datu aizsardzības standartklauzulas šajā trešajā valstī netiek vai nevar tikt ievērotas un ka Savienības tiesībās prasīto pārsūtīto datu aizsardzību nav iespējams nodrošināt ar citiem līdzekļiem, ja Savienībā reģistrētais datu pārzinis vai apstrādātājs paši nav apturējuši vai izbeiguši pārsūtīšanu.

114 Iepriekšējā punktā ietverto interpretāciju neatspēko komisāra argumentācija, saskaņā ar kuru Lēmuma 2010/87 4. pantā, redakcijā, kas bija spēkā pirms Īstenošanas lēmuma 2016/2297 stāšanās spēkā, ņemot vērā šī lēmuma 11. apsvērumu, uzraudzības iestāžu pilnvaras apturēt vai aizliegt personas datu pārsūtīšanu uz trešo valsti tika attiecinātas tikai uz noteiktiem izņēmuma gadījumiem. Minētajā LSK līguma 4. pantā – redakcijā, kas grozīta ar Īstenošanas lēmumu 2016/2297, – ir minētas šo iestāžu pilnvaras, kuras šobrīd tām ir saskaņā ar VDAR 58. panta 2. punkta f) un j) apakšpunktu, apturēt vai aizliegt šādu nosūtīšanu, nekādi neierobežojot šo pilnvaru īstenošanu tikai ar ārkārtas gadījumiem.

115 Katrā ziņā īstenošanas pilnvaras, kas Komisijai piešķirtas ar VDAR 46. panta 2. punkta c) apakšpunktu, lai pieņemtu datu aizsardzības standartklauzulas, nepiešķir tai kompetenci ierobežot pilnvaras, kuras uzraudzības iestādēm ir uzticētas saskaņā ar šīs regulas 58. panta 2. punktu (pēc analoģijas attiecībā uz Direktīvas 95/46 25. panta 6. punktu un 28. pantu skat. spriedumu 2015. gada 6. oktobra, *Schrems*, C-362/14, EU:C:2015:650, 102. un 103. punkts). Turklāt Īstenošanas lēmuma 2016/2297 5. apsvērumā ir apstiprināts, ka LSK lēmums "neliedz [uzraudzības iestādei] īstenot tās pilnvaras pārraudzīt datu plūsmas, tostarp pilnvaras apturēt vai aizliegt personas datu pārsūtīšanu, ja tā konstatē, ka pārsūtīšana notiek, pārkāpjot ES vai valsts datu aizsardzības tiesību aktus [..]".

116 Tomēr ir svarīgi precizēt, ka kompetentās uzraudzības iestādes pilnvaras ir pilnībā pakļautas lēmumam, ar kuru Komisija attiecīgā gadījumā, piemērojot VDAR 45. panta 1. punkta pirmo teikumu, konstatē, ka noteikta trešā valsts nodrošina pietiekamu aizsardzības līmeni. Šādā gadījumā no šīs regulas 45. panta 1. punkta otrā teikuma, lasot to kopsakarā ar tās 103. apsvērumu, izriet, ka personas datu pārsūtīšana uz attiecīgo trešo valsti var notikt bez īpašas atļaujas saņemšanas.

117 Saskaņā ar LESD 288. panta ceturto daļu Komisijas lēmums par aizsardzības līmeņa pietiekamību kopumā ir saistošs visām dalībvalstīm, kurām tas adresēts, un tādējādi tas ir saistošs visām to struktūrām, ciktāl tajā ir konstatēts, ka attiecīgā trešā valsts nodrošina pietiekamu aizsardzības līmeni un ka tā rezultātā ir atļauts pārsūtīt šādus datus (pēc analoģijas attiecībā uz Direktīvas 95/46 25. panta 6. punktu skat. spriedumu, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 51. punkts un tajā minētā judikatūra).

118 Tādējādi, kamēr Komisijas lēmumu Tiesa nav atzinusi par spēkā neesošu, dalībvalstis un to struktūras, pie kurām ir pieskaitāmas to neatkarīgās uzraudzības iestādes, protams, nedrīkst veikt ar šādu lēmumu nesaderīgus pasākumus, piemēram, pieņemt tiesību aktus, kuros ar saistošām sekām būtu noteikts, ka minētajā lēmumā norādītajās trešajās valstīs netiek nodrošināts pietiekams aizsardzības līmenis (spriedums, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 52. punkts un tajā minētā judikatūra), un līdz ar to apturēt vai aizliegt personas datu pārsūtīšanu uz šo trešo valsti.

119 Tomēr Komisijas lēmums par aizsardzības līmeņa pietiekamību, kas pieņemts saskaņā ar VDAR 45. panta 3. punktu, nevar liegt personām, kuru personas dati ir tikuši vai varētu tikt pārsūtīti uz trešo valsti, saskaņā ar VDAR 77. panta 1. punktu kompetentajā valsts uzraudzības iestādē iesniegt sūdzību par viņu tiesību un brīvību aizsardzību attiecībā uz šo datu apstrādi. Tāpat šāda veida lēmums nevar ne atcelt, ne mazināt pilnvaras, kas valsts uzraudzības iestādēm ir skaidri piešķirtas Hartas 8. panta 3. punktā, kā arī minētās regulas 51. panta 1. punktā un 57. panta 1. punkta a) apakšpunktā (pēc analoģijas attiecībā uz Direktīvas 95/46 25. panta 6. punktu un 28. pantu skat. spriedumu, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 53. punkts).

120 Tādējādi, pat ja pastāv Komisijas lēmums par aizsardzības līmeņa pietiekamību, kompetentajai valsts uzraudzības iestādei, kurā ir vērsusies persona ar sūdzību par tās tiesību un brīvību aizsardzību attiecībā uz personas datu apstrādi, ir jābūt iespējai pilnīgi neatkarīgi pārbaudīt, vai šo datu nodošana atbilst VDAR noteiktajām prasībām, un vajadzības gadījumā celt prasību valsts tiesās, lai pēdējās minētās, ja tās piekrīt šīs iestādes viedoklim attiecībā uz lēmuma par aizsardzības līmeņa pietiekamību spēkā esamību, iesniegtu lūgumu sniegt prejudiciālu nolēmumu nolūkā pārbaudīt šo spēkā esamību (pēc analoģijas attiecībā uz Direktīvas 95/46 25. panta 6. punktu un 28. pantu skat. spriedumu, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 57. un 65. punkts).

121 Ņemot vērā iepriekš minētos apsvērumus, uz astoto jautājumu ir jāatbild, ka VDAR 58. panta 2. punkta f) un j) apakšpunkts ir jāinterpretē tādējādi, ka, ja vien pastāv likumīgi pieņemts Komisijas lēmums par aizsardzības līmeņa pietiekamību, kompetentajai uzraudzības iestādei ir jāaptur vai jāaizliedz tāda personas datu pārsūtīšana uz trešo valsti, kas pamatota ar Komisijas pieņemtajām datu aizsardzības standartklauzulām, ja šī uzraudzības iestāde, ievērojot visus šīs pārsūtīšanas īpašos apstākļus, uzskata, ka šīs klauzulas šajā trešā valstī netiek vai nevar tikt ievērotas un ka pārsūtīto datu aizsardzība, kāda tā prasīta Savienības tiesībās, konkrēti, VDAR 45. un 46. pantā un Hartā, nevar tikt nodrošināta ar citiem līdzekļiem, ja Savienībā reģistrētais datu pārzinis vai apstrādātājs nav pats apturējis vai izbeidzis šo pārsūtīšanu.

Par septīto un vienpadsmito jautājumu

122 Iesniedzējtiesa ar septīto un vienpadsmito jautājumu, kas ir jāizskata kopā, būtībā vaicā Tiesai par LSK lēmuma spēkā esamību, ņemot vērā Hartas 7., 8. un 47. pantu.

123 It īpaši, kā izriet no paša septītā jautājuma formulējuma un ar to saistītajiem paskaidrojumiem lūgumā sniegt prejudiciālu nolēmumu, iesniedzējtiesa jautā, vai LSK lēmums var nodrošināt pietiekamu uz trešajām valstīm pārsūtīto personas datu aizsardzības līmeni, ciktāl tajā paredzētās datu aizsardzības standartklauzulas nav saistošas šo trešo valstu iestādēm.

124 LSK lēmuma 1. pantā ir noteikts, ka tam pievienotās datu aizsardzības standartklauzulas ir uzskatāmas par pienācīgu nodrošinājumu attiecībā uz indivīdu privātās dzīves, pamattiesību un pamatbrīvību aizsardzību atbilstoši Direktīvas 95/46 26. panta 2. punkta prasībām. Pēdējā minētā norma ir būtībā pārņemta VDAR 46. panta 1. punktā un 2. punkta c) apakšpunktā.

125 Tomēr, lai gan šīs klauzulas ir saistošas Savienībā reģistrētam personas datu apstrādātājam un trešajā valstī reģistrētam personas datu saņēmējam gadījumā, kad tie ir noslēguši līgumu, atsaucoties uz šīm klauzulām, nav strīda par to, ka minētās klauzulas var nebūt saistošas šīs trešās valsts iestādēm, jo tās nav līguma puses.

126 Līdz ar to, lai arī pastāv situācijas, kurās atkarībā no attiecīgajā trešajā valstī spēkā esošajām tiesībām un valdošās prakses šādi pārsūtīto datu saņēmējs var nodrošināt tiem nepieciešamo aizsardzību, pamatojoties tikai uz datu aizsardzības standartklauzulām, pastāv citas situācijas, kurās šo klauzulu prasības varētu nebūt pietiekams līdzeklis, lai praksē attiecīgajā trešajā valstī nodrošinātu pārsūtīto personas datu efektīvu aizsardzību. Tā tas it īpaši ir tad, ja šīs trešās valsts tiesībās tās publiskajām iestādēm ir atļauts iejaukties datu subjektu tiesībās saistībā ar šiem datiem.

127 Tādējādi rodas jautājums, vai Komisijas lēmums par datu aizsardzības standartklauzulām, kurš pieņemts, pamatojoties uz VDAR 46. panta 2. punkta c) apakšpunktu, nav spēkā, ja šajā lēmumā nav garantiju, ko var īstenot pret to trešo valstu publiskajām iestādēm, uz kurām personas dati tiek vai varētu tikt pārsūtīti, pamatojoties uz šīm klauzulām.

128 VDAR 46. panta 1. punktā ir paredzēts, ka gadījumā, ja nav pieņemts lēmums par aizsardzības līmeņa pietiekamību, pārzinis vai apstrādātājs var nosūtīt personas datus uz trešo valsti tikai tad, ja tie ir snieguši atbilstošas garantijas, un ar nosacījumu, ka datu subjektiem ir pieejamas īstenojamas datu subjekta tiesības un efektīvi tiesiskās aizsardzības līdzekļi. Saskaņā ar šīs regulas 46. panta 2. punkta c) apakšpunktu šīs garantijas var nodrošināt ar Komisijas pieņemtajām datu aizsardzības standartklauzulām. Šajās tiesību normās nav noteikts, ka visas minētās garantijas noteikti ir jāparedz tādā Komisijas lēmumā kā LSK lēmums.

129 Šajā ziņā ir svarīgi norādīt, ka šāds lēmums atšķiras no lēmuma par aizsardzības līmeņa pietiekamību atbilstoši VDAR 45. panta 3. punktam, kurā pēc attiecīgās trešās valsts tiesiskā regulējuma pārbaudes, it īpaši ņemot vērā atbilstošos tiesību aktus valsts drošības un publisko iestāžu piekļuves personas datiem jomā, ar saistošu spēku ir konstatēts, ka trešā valsts, teritorija vai viens vai vairāki konkrēti sektori nodrošina pietiekamu aizsardzības līmeni un ka līdz ar to minētās valsts publisko iestāžu piekļuve šiem datiem nav šķērslis to nosūtīšanai uz minēto valsti. Šādu lēmumu par aizsardzības līmeņa pietiekamību Komisija var pieņemt tikai ar nosacījumu, ka tā ir konstatējusi, ka šīs trešās valsts attiecīgie tiesību akti šajā jomā patiešām ietver visas nepieciešamās garantijas, kas ļauj uzskatīt, ka ar to tiek nodrošināts pietiekams aizsardzības līmenis.

130 Savukārt, runājot par Komisijas lēmumu, ar kuru ir pieņemtas tādas datu aizsardzības standartklauzulas kā LSK lēmums, ciktāl šāds lēmums neattiecas uz trešo valsti, teritoriju vai vienu vai vairākiem konkrētiem tās sektoriem, no VDAR 46. panta 1. punkta un 2. punkta c) apakšpunkta nevar secināt, ka Komisijai pirms šāda lēmuma pieņemšanas būtu jāizvērtē trešajās valstīs, uz kurām personas dati, pamatojoties uz minētajām klauzulām, varētu tikt pārsūtīti, nodrošinātā aizsardzības līmeņa pietiekamība.

131 Šajā ziņā ir jāatgādina, ka saskaņā ar šīs regulas 46. panta 1. punktu, ja Komisija nav pieņēmusi lēmumu par aizsardzības līmeņa pietiekamību, atbilstošās garantijas ir jāsniedz Savienībā reģistrētajam pārzinim vai apstrādātājam. Minētās regulas 108. un 114. apsvērumā ir apstiprināts, ka tad, ja Komisija nav lēmusi par datu aizsardzības līmeņa pietiekamību trešajā valstī, personas datu pārzinim vai, attiecīgā gadījumā, tā apstrādātājam "būtu jāveic pasākumi, kas kompensētu datu aizsardzības trūkumus trešā valstī, paredzot atbilstošas garantijas datu subjektam", un ka "šīm garantijām būtu

jānodrošina, lai tiktu ievērotas datu aizsardzības prasības un datu subjektu tiesības atbilstīgi Savienībā veiktai apstrādei, tostarp īstenojamu datu subjekta tiesību un efektīvu tiesiskās aizsardzības līdzekļu pieejamība [..] Savienībā un trešā valstī".

132 Tādējādi, kā izriet no šī sprieduma 125. punkta, datu aizsardzības standartklauzulu līgumiskā rakstura īpatnība ir tāda, ka tās nav saistošas trešo valstu publiskajām iestādēm, bet ka VDAR 44. pantā, 46. panta 1. punktā un 2. punkta c) apakšpunktā, tos interpretējot Hartas 7., 8. un 47. panta kontekstā, ir prasīts, lai netiktu apdraudēts šajā regulā garantētais fizisko personu aizsardzības līmenis, var izrādīties, ka šajās datu aizsardzības klauzulās ietvertās garantijas ir jāpapildina. Šajā ziņā minētās regulas 109. apsvērumā ir noteikts, ka "iespējai, ka pārzinis vai apstrādātājs var izmantot Komisijas [..] pieņemtās standarta datu aizsardzības klauzulas, nebūtu jāizslēdz [..], ka pārzinis vai apstrādātājs var pievienot citas klauzulas vai papildu garantijas", un īpaši precizēts, ka tie "būtu jāmudina nodrošināt papildu garantijas, [..] ar kurām papildina [datu] standarta aizsardzības klauzulas".

133 Tādējādi šķiet, ka datu aizsardzības standartklauzulu, kuras Komisija pieņēmusi saskaņā ar tās pašas regulas 46. panta 2. punkta c) apakšpunktu, mērķis ir vienīgi sniegt Savienībā reģistrētajiem personas datu pārziņiem vai apstrādātājiem līgumā paredzētās garantijas, kas ir piemērojamas vienveidīgi visās trešajās valstīs un tādējādi neatkarīgi no katrā no tām garantētā aizsardzības līmeņa. Ciktāl šīs datu aizsardzības standartklauzulas, ņemot vērā to raksturu, nevar sniegt garantijas, kas pārsniegtu līgumisko pienākumu nodrošināt, lai tiktu ievērots Savienības tiesībās prasītais aizsardzības līmenis, atkarībā no situācijas vienā vai citā trešajā valstī personas datu apstrādātājam var būt nepieciešams noteikt tās papildinošus pasākumus, lai nodrošinātu šī aizsardzības līmeņa ievērošanu.

134 Šajā ziņā, kā ģenerāladvokāts ir norādījis secinājumu 126. punktā, VDAR 46. panta 2. punkta c) apakšpunktā paredzētā līgumiskā mehānisma pamatā ir atbildības noteikšana Savienībā reģistrētajam personas datu pārzinim vai apstrādātājam, kā arī, pakārtoti, kompetentajai uzraudzības iestādei. Līdz ar to šim personas datu pārzinim vai tā apstrādātājam katrā atsevišķā gadījumā un, kad nepieciešams, sadarbībā ar pārsūtīto datu saņēmēju ir jāpārbauda, vai galamērķa trešās valsts tiesības nodrošina no Savienības tiesību aspekta pietiekamu aizsardzību personas datiem, kas tikuši pārsūtīti, pamatojoties uz datu aizsardzības standartklauzulām, vajadzības gadījumā sniedzot garantijas papildus šajās klauzulās ietvertajām.

135 Ja pārzinis vai apstrādātājs, kas reģistrēts Savienībā, nevar veikt vajadzīgos papildu pasākumus, lai nodrošinātu šādu aizsardzību, tad tiem vai, pakārtoti, kompetentajai uzraudzības iestādei ir jāaptur vai jāizbeidz personas datu pārsūtīšana uz attiecīgo trešo valsti. Tā tas it īpaši ir tad, ja šīs trešās valsts tiesībās no Savienības pārsūtītu personas datu saņēmējam ir noteikti pienākumi, kas ir pretrunā minētajām klauzulām un kas līdz ar to var likt apšaubīt līgumisko garantiju par pietiekamu aizsardzības līmeni pret minētās trešās valsts iestāžu piekļuvi šiem datiem.

136 Tādējādi tas vien, ka tādas datu aizsardzības standartklauzulas, kas ietvertas Komisijas lēmumā, kurš pieņemts atbilstoši VDAR 46. panta 2. punkta c) apakšpunktam, kā LSK lēmuma pielikumā ietvertās nav saistošas tādu trešo valstu iestādēm, uz kurām personas dati var tikt pārsūtīti, nevar ietekmēt šī lēmuma spēkā esamību.

137 Šī spēkā esamība savukārt ir atkarīga no tā, vai saskaņā ar prasību, kas izriet no VDAR 46. panta 1. punkta un 2. punkta c) apakšpunkta, tos interpretējot Hartas 7., 8. un 47. panta kontekstā, šāds lēmums ietver efektīvus mehānismus, kas praksē ļauj nodrošināt, ka tiek ievērots Savienības tiesībās prasītais aizsardzības līmenis un ka, pamatojoties uz šīm klauzulām īstenotā personas datu pārsūtīšana šo klauzulu pārkāpuma gadījumā tiek apturēta vai aizliegta.

138 Attiecībā uz garantijām, kas noteiktas LSK lēmuma pielikumā ietvertajās datu aizsardzības standartklauzulās, no 4. klauzulas a) un b) punkta, 5. klauzulas a) punkta, 9. klauzulas, kā arī 11. klauzulas 1. punkta izriet, ka Savienībā reģistrētais personas datu pārzinis, pārsūtīto datu saņēmējs, kā arī tā iespējamais apstrādātājs savstarpēji apņemas, lai šo datu apstrāde, tostarp to pārsūtīšana, tiktu

veikta un turpinātos saskaņā ar "piemērojamajiem tiesību aktiem datu aizsardzības jomā", kuri atbilstoši minētā lēmuma 3. panta f) punktam ir "ir tiesību akti, kas aizsargā personu pamattiesības un pamatbrīvības, un jo īpaši viņu tiesības uz privāto dzīvi attiecībā uz personas datu apstrādi, un kas attiecas uz atbildīgo par datu apstrādi dalībvalstī, kurā datu nosūtītājs ir reģistrēts". VDAR noteikumi, lasot tos kopā ar Hartu, ir daļa no šiem tiesību aktiem.

139 Turklāt trešajā valstī reģistrētais personas datu saņēmējs saskaņā ar 5. klauzulas a) punktu apņemas nekavējoties informēt datu nosūtītāju, ja tas kāda iemesla dēļ nevar izpildīt tam līgumā paredzētos pienākumus. It īpaši saskaņā ar 5. klauzulas b) punktu šis saņēmējs apliecina, ka tam nav iemesla uzskatīt, ka viņam piemērojamie tiesību akti neļauj tam izpildīt līgumā paredzētos pienākumus, un ka gadījumā, ja tiek izdarītas tādas izmaiņas datu saņēmēja valsts tiesību aktos, kas var negatīvi ietekmēt LSK lēmuma pielikumā ietvertajās datu aizsardzības standartklauzulās noteiktās garantijas un pienākumus, tas nekavējoties paziņos par šīm izmaiņām datu nosūtītājam, tiklīdz tās kļūs zināmas. Turklāt, lai gan 5. klauzulas d) punkta i) apakšpunkts ļauj personas datu saņēmējam gadījumā, kad piemērojams tiesiskais regulējums, kas tam nodrošina aizstāvību, kāds, piemēram, ir krimināltiesībās paredzētais aizliegums nolūkā saglabāt tiesībaizsardzības iestāžu veiktās izmeklēšanas konfidencialitāti, nepaziņot Savienībā reģistrētajam personas datu pārzinim par tiesībaizsardzības iestādes saistošu pieprasījumu izpaust personas datus, viņam tomēr atbilstoši LSK lēmuma pielikuma 5. klauzulas a) punktam ir jāinformē personas datu pārzinis par neiespējamību izpildīt datu aizsardzības standartklauzulu prasības.

140 Abos tajā paredzētajos gadījumos šīs 5. klauzulas a) un b) punktā Savienībā reģistrētajam datu pārzinim ir piešķirtas tiesības apturēt datu pārsūtīšanu un/vai izbeigt līgumu. Ņemot vērā prasības, kas izriet no VDAR 46. panta 1. punkta un 2. punkta c) apakšpunkta, lasot tos Hartas 7. un 8. panta kontekstā, datu pārsūtīšanas apturēšana un/vai līguma izbeigšana ir personas datu pārziņa pienākums, ja datu saņēmējs nespēj vai vairs nespēj izpildīt datu aizsardzības standartklauzulu prasības. Pretējā gadījumā personas datu pārzinis nepildītu prasības, kas noteiktas LSK lēmuma pielikuma 4. klauzulas a) punktā, interpretējot to kopsakarā ar VDAR un Hartas noteikumiem.

141 Tādējādi izrādās, ka šī pielikuma 4. klauzulas a) punktā, kā arī 5. klauzulas a) un b) punktā Savienībā reģistrētajam personas datu pārzinim un personas datu saņēmējam ir noteikts pienākums pārliecināties, ka galamērķa trešās valsts tiesību akti ļauj minētajam saņēmējam ievērot LSK lēmuma pielikumā ietvertās datu aizsardzības standartklauzulas vēl pirms personas datu pārsūtīšanas uz šo trešo valsti. Attiecībā uz šo pārbaudi zemsvītras piezīmē, kas attiecas uz minēto 5. klauzulu, ir precizēts, ka šo valsts tiesību aktu obligātās prasības, kas nepārsniedz prasības, kuras ir vajadzīgas demokrātiskā sabiedrībā, proti, ir nepieciešams aizsargpasākums valsts drošībai, aizsardzībai, sabiedrības drošībai, nav pretrunā datu aizsardzības standartklauzulām. Pretējā gadījumā, kā secinājumu 131. punktā norādījis ģenerāladvokāts, tāda pienākuma pildīšana, kurš izriet no galamērķa trešās valsts tiesībām un kurš pārsniedz to, kas nepieciešams minēto mērķu sasniegšanai, ir uzskatāma par minēto klauzulu pārkāpumu. Minētajiem tirgus dalībniekiem, izvērtējot, vai šāds pienākums ir samērīgs, attiecīgā gadījumā ir jāņem vērā Komisijas lēmumā par aizsardzības līmeņa pietiekamību, kas pieņemts atbilstoši VDAR 45. panta 3. punktam, ietvertais konstatējums par trešās valsts nodrošinātā aizsardzības līmeņa pietiekamību.

142 No tā izriet, ka Savienībā reģistrētajam personas datu pārzinim un personas datu saņēmējam vispirms ir jāpārbauda, vai attiecīgajā trešajā valstī ir ievērots Savienības tiesībās prasītais aizsardzības līmenis. Datu saņēmējam attiecīgā gadījumā ir pienākums saskaņā ar tās pašas 5. klauzulas b) punktu informēt personas datu pārzini par to, ka tam nav iespējams izpildīt šīs klauzulas, un datu pārzinim ir pienākums apturēt datu nosūtīšanu un/vai izbeigt līgumu.

143 Ja uz trešo valsti pārsūtīto personas datu saņēmējs saskaņā ar 5. klauzulas b) punktu ir darījis zināmu personas datu pārzinim, ka attiecīgās trešās valsts tiesību akti tam neļauj ievērot LSK lēmuma pielikumā ietvertās datu aizsardzības standartklauzulas, no šī pielikuma 12. klauzulas izriet, ka dati, kas

jau ir pārsūtīti uz šo trešo valsti, un to kopijas kopumā ir jāatdod vai jāiznīcina. Katrā ziņā ar šī paša pielikuma 6. klauzulu ir paredzēts sods par šo standartklauzulu neievērošanu, piešķirot datu subjektam tiesības uz nodarītā kaitējuma atlīdzināšanu.

144 Jāpiebilst, ka atbilstoši LSK lēmuma pielikuma 4. klauzulas f) punktam Savienībā reģistrētais datu pārzinis gadījumā, ja uz trešo valsti, kurā netiek piedāvāts pietiekams aizsardzības līmenis, varētu tik pārsūtīti īpašu kategoriju dati, apņemas par to informēt datu subjektu pirms datu pārsūtīšanas vai iespējami drīz pēc tam. Šī informācija var dot šai personai iespēju izmantot tai šī pielikuma 3. klauzulas 1. punktā paredzētās tiesības vērsties pret personas datu pārzini, lai tas apturētu paredzēto pārsūtīšanu, izbeigtu ar personas datu saņēmēju noslēgto līgumu vai vajadzības gadījumā lūgtu datu saņēmējam atdot vai iznīcināt pārsūtītos datus.

145 Visbeidzot, saskaņā ar minētā pielikuma 4. klauzulas g) punktu, ja personas datu saņēmējs, piemērojot tā 5. klauzulas b) punktu, Savienībā reģistrētajam datu pārzinim paziņo, ka viņam piemērojamajos tiesību aktos tiek izdarīti grozījumi, kas var būtiski negatīvi ietekmēt datu aizsardzības standartklauzulās ietvertās saistības un piedāvātās garantijas, pārzinim šis paziņojums ir jānosūta kompetentajai uzraudzības iestādei, ja viņš, neraugoties uz minēto paziņojumu, nolemj turpināt pārsūtīšanu vai atcelt aizliegumu. Šāda paziņojuma nosūtīšana minētajai uzraudzības iestādei un tās tiesības atbilstoši šī paša pielikuma 8. klauzulas 2. punktam veikt pārbaudes pie pārsūtīto personas datu saņēmēja ļauj minētajai uzraudzības iestādei pārbaudīt, vai plānotā pārsūtīšana ir jāaptur vai jāaizliedz, lai nodrošinātu pietiekamu aizsardzības līmeni.

146 Šajā kontekstā LSK lēmuma 4. pants, lasot to kopā ar Īstenošanas lēmuma 2016/2297 5. apsvērumu, apstiprina, ka LSK lēmums nekādi neliedz kompetentajai uzraudzības iestādei apturēt vai vajadzības gadījumā aizliegt pārsūtīt personas datus uz trešo valsti, pamatojoties uz šim lēmumam pievienotajām datu aizsardzības standartklauzulām. Šajā ziņā, kā izriet no atbildes uz astoto jautājumu, ja vien Komisija nav likumīgi pieņēmusi lēmumu par aizsardzības līmeņa pietiekamību, kompetentajai uzraudzības iestādei saskaņā ar VDAR 58. panta 2. punkta f) un j) apakšpunktu ir jāaptur vai jāaizliedz šāda datu pārsūtīšana, ja tā, ņemot vērā visus ar šo pārsūtīšanu saistītos apstākļus, uzskata, ka šajā trešajā valstī netiek vai nevar tikt ievērotas minētās klauzulas un ka Savienības tiesībās prasīto pārsūtīto datu aizsardzību nav iespējams nodrošināt ar citiem līdzekļiem, ja vien Savienībā reģistrētais pārzinis vai apstrādātājs paši jau nav pārsūtīšanu apturējuši vai izbeiguši.

147 Attiecībā uz komisāra norādīto apstākli, saskaņā ar kuru uz personas datu pārsūtīšanu uz šādu trešo valsti, iespējams, varētu attiekties atšķirīgi uzraudzības iestāžu lēmumi dažādās dalībvalstīs, ir jāpiebilst, kā izriet no VDAR 55. panta 1. punkta un 57. panta 1. punkta a) apakšpunkta, ka uzdevums nodrošināt šīs regulas ievērošanu principā tiek uzticēts katrai uzraudzības iestādei tās dalībvalsts teritorijā, kurā tā atrodas. Turklāt, lai izvairītos no atšķirīgiem lēmumiem, minētās regulas 64. panta 2. punktā uzraudzības iestādei, kura uzskata, ka datu pārsūtīšana uz trešo valsti vispārīgi ir jāaizliedz, ir paredzēta iespēja lūgt sniegt atzinumu Eiropas Datu aizsardzības komitejai (EDAK), kas, piemērojot tās pašas regulas 65. panta 1. punkta c) apakšpunktu, var pieņemt saistošu lēmumu, it īpaši, ja uzraudzības iestāde neievēro sniegto atzinumu.

148 No tā izriet, ka LSK lēmumā ir paredzēti efektīvi mehānismi, kas praksē ļauj nodrošināt, ka personas datu pārsūtīšana uz trešo valsti, pamatojoties uz šim lēmumam pievienotajām datu aizsardzības standartklauzulām, tiek apturēta vai aizliegta, ja pārsūtīto datu saņēmējs neievēro vai tam nav iespējams ievērot minētās klauzulas.

149 Ņemot vērā visus iepriekš minētos apsvērumus, uz septīto un vienpadsmito jautājumu ir jāatbild, ka, izvērtējot LSK lēmumu, ņemot vērā Hartas 7., 8. un 47. pantu, nav konstatēts neviens apstāklis, kas varētu ietekmēt šī lēmuma spēkā esamību.

Par ceturto, piekto, devīto un desmito jautājumu

150 Ar devīto jautājumu iesniedzējtiesa būtībā vēlas noskaidrot, vai un kādā mērā dalībvalsts uzraudzības iestādei ir saistoši PV lēmumā ietvertie konstatējumi, saskaņā ar kuriem ASV nodrošina pietiekamu aizsardzības līmeni. Ar ceturto, piekto un desmito jautājumu šī tiesa būtībā jautā, vai, ņemot vērā viņas pašas konstatējumus par ASV tiesībām, ar personas datu pārsūtīšanu uz šo trešo valsti, pamatojoties uz LSK lēmuma pielikumā ietvertajām datu aizsardzības standartklauzulām, tiek pārkāptas Hartas 7., 8. un 47. pantā garantētās tiesības, un it īpaši tā vaicā Tiesai, vai PV lēmuma III pielikumā minētā ombuda izveide ir saderīga ar šo 47. pantu.

151 Vispirms ir jānorāda, ka, lai gan komisāra pamatlietā celtajā prasībā tiek apšaubīta vienīgi LSK lēmuma spēkā esamība, šī prasība tika celta iesniedzējtiesā vēl pirms PV lēmuma pieņemšanas. Tā kā ar ceturto un piekto jautājumu šī tiesa vispārīgi jautā Tiesai par aizsardzību, kas ir jānodrošina saskaņā ar Hartas 7., 8. un 47. pantu šādas pārsūtīšanas kontekstā, Tiesas pārbaudē ir jāņem vērā sekas, ko rada starplaikā notikusī PV lēmuma pieņemšana. Tas tā ir vēl jo vairāk tāpēc, ka minētā tiesa ar desmito jautājumu skaidri jautā, vai šajā 47. pantā prasītā aizsardzība tiek nodrošināta ar šajā pēdējā minētajā lēmumā paredzētā ombuda starpniecību.

152 Turklāt no lūgumā sniegt prejudiciālu nolēmumu ietvertajām norādēm izriet, ka pamatlietā *Facebook Ireland* ir apgalvojusi, ka PV lēmums komisāram rada saistošas sekas attiecībā uz ASV nodrošinātā aizsardzības līmeņa pietiekamības konstatēšanu un līdz ar to attiecībā uz personas datu nosūtīšanas uz šo trešo valsti likumību, pamatojoties uz LSK lēmuma pielikumā ietvertajām datu aizsardzības standartklauzulām.

153 Kā izriet no šī sprieduma 59. punkta, savā 2017. gada 3. oktobra spriedumā, kas pievienots lūgumam sniegt prejudiciālu nolēmumu, iesniedzējtiesa ir uzsvērusi, ka tai ir pienākums ņemt vērā tiesību izmaiņas, kuras notikušas laikā starp prasības celšanu un tajā organizēto tiesas sēdi. Tādējādi šķiet, ka šai tiesai, lai atrisinātu pamatlietu, ir pienākums ņemt vērā apstākļu maiņu, kas izriet no PV lēmuma pieņemšanas, kā arī tā iespējamās saistošās sekas.

154 It īpaši, saistošu seku esamībai, kuras rada tas, ka PV lēmumā tiek konstatēts pietiekams aizsardzības līmenis ASV, ir nozīme, novērtējot gan šī sprieduma 141. un 142. punktā atgādinātos personas datu pārziņa un personas datu saņēmēja trešajā valstī pienākumus, pamatojoties uz LSK lēmumam pievienotajām datu aizsardzības standartklauzulām, gan pienākumus, kas attiecīgā gadījumā ir iestādei, kurai šī pārsūtīšana ir jāaptur vai jāaizliedz.

155 Attiecībā uz PV lēmuma saistošajām sekām tā 1. panta 1. punktā ir noteikts, ka VDAR 45. panta 1. punkta izpratnē "Amerikas Savienotās Valstis nodrošina pienācīgu aizsardzības līmeni personas datiem, kas [Eiropas Savienības] un [Amerikas Savienoto Valstu] privātuma vairoga ietvaros no Savienības tiek nosūtīti organizācijām Amerikas Savienotajās Valstīs". Saskaņā ar minētā lēmuma 1. panta 3. punktu personas dati tiek uzskatīti par pārsūtītiem šī vairoga ietvaros, ja tie tiek pārsūtīti no Savienības uz ASV reģistrētām organizācijām, kas ir iekļautas to organizāciju sarakstā, kuras pievienojas minētajam vairogam, ko atjaunina un publicējusi Amerikas Tirdzniecības ministrija saskaņā ar šī paša lēmuma II pielikumā izklāstīto principu I un III sadaļu.

156 Kā izriet no šī sprieduma 117. un 118. punktā atgādinātās judikatūras, PV lēmums ir saistošs attiecībā uz uzraudzības iestādēm, jo tajā ir konstatēts, ka ASV nodrošina pietiekamu aizsardzības līmeni, un tādējādi tā rezultātā ir atļauta personas datu pārsūtīšana, kas veikta Eiropas Savienības un ASV datu aizsardzības vairoga ietvaros. Līdz ar to, kamēr Tiesa šo lēmumu nav atzinusi par spēkā neesošu, kompetentā uzraudzības iestāde nevar apturēt vai aizliegt personas datu pārsūtīšanu organizācijai, kas pievienojusies šim vairogam, pamatojoties uz to, ka tā – pretēji Komisijas vērtējumam minētajā lēmumā – uzskata, ka ASV tiesību akti, kas reglamentē piekļuvi personas datiem, kuri pārsūtīti minētā vairoga ietvaros, un šo datu izmantošanu, ko valsts drošības nolūkos veic šīs trešās valsts publiskās iestādes, nenodrošina pietiekamu aizsardzības līmeni.

157 Tomēr saskaņā ar šī sprieduma 119. un 120. punktā atgādināto judikatūru, ja persona kompetentajai uzraudzības iestādei ir iesniegusi sūdzību, šai iestādei ir pilnīgi neatkarīgi jāpārbauda, vai attiecīgo personas datu nodošana atbilst VDAR noteiktajām prasībām, un gadījumā, ja tā atzīst par pamatotiem iebildumus, ko šī persona ir izvirzījusi, lai apstrīdētu lēmuma par aizsardzības līmeņa pietiekamību spēkā esamību, ir jāceļ prasība valsts tiesās, lai tās vēršas Tiesā ar lūgumu sniegt prejudiciālu nolēmumu par šī lēmuma spēkā esamības izvērtējumu.

158 Sūdzība atbilstoši VDAR 77. panta 1. punktam, ar ko persona, kuras personas dati ir tikuši vai var tikt pārsūtīti uz trešo valsti, norāda, ka šīs trešās valsts tiesības un prakse, neraugoties uz to, ko Komisija ir konstatējusi šīs regulas 45. panta 3. punktā, nenodrošina pienācīgu aizsardzības līmeni, ir jāsaprot kā tāda, kas būtībā attiecas uz šī lēmuma saderīgumu ar personu privātās dzīves neaizskaramību, kā arī pamattiesību un pamatbrīvību aizsardzību (pēc analoģijas attiecībā uz Direktīvas 95/46 25. panta 6. punktu un 28. panta 4. punktu skat. spriedumu, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 59. punkts).

159 Šajā gadījumā *M. Schrems* būtībā lūdza komisāru aizliegt vai apturēt *Facebook Ireland* īstenoto personas datu pārsūtīšanu uz ASV reģistrēto *Facebook Inc.* tādēļ, ka šī trešā valsts nenodrošinot pietiekamu aizsardzības līmeni. Tā kā komisārs izmeklēšanas par *M. Schrems* apgalvojumiem noslēgumā vērsās iesniedzējtiesā, šī tiesa, ņemot vērā iesniegtos pierādījumus un tajā notikušo uz sacīkstes principu balstīto procesu, šaubās par *M. Schrems* bažu pamatotību attiecībā uz minētajā trešajā valstī nodrošinātā aizsardzības līmeņa pietiekamību, neraugoties uz to, ko Komisija pa to laiku bija konstatējusi PV lēmumā, kā dēļ šī tiesa uzdeva Tiesai ceturto, piekto un desmito prejudiciālo jautājumu.

160 Kā ģenerāladvokāts norādījis secinājumu 175. punktā, šie prejudiciālie jautājumi tādējādi ir jāsaprot tādējādi, ka ar tiem būtībā tiek apšaubīts PV lēmumā ietvertais Komisijas konstatējums, ka ASV nodrošina pietiekamu no Savienības uz šo trešo valsti pārsūtīto personas datu aizsardzības līmeni, un līdz ar to šī lēmuma spēkā esamība.

161 Ņemot vērā šī sprieduma 121. un 157.–160. punktā paustos apsvērumus un lai sniegtu pilnīgu atbildi iesniedzējtiesai, ir jāizvērtē, vai PV lēmums ir saderīgs ar VDAR prasībām, to skatot Hartas kontekstā (pēc analoģijas skat. spriedumu, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 67. punkts).

162 Komisijas lēmuma par aizsardzības līmeņa pietiekamību atbilstīgi VDAR 45. panta 3. punktam pieņemšanas pamatā ir šīs iestādes pienācīgi pamatots secinājums par to, ka trešā valsts tik tiešām, pamatojoties uz savu iekšējo tiesisko kārtību vai savām starptautiskajām saistībām, nodrošina būtībā ekvivalentu pamatbrīvību un pamattiesību aizsardzības līmeni tam, kāds tiek garantēts Savienības tiesiskajā kārtībā (pēc analoģijas attiecībā uz Direktīvas 95/46 25. panta 6. punktu skat. spriedumu, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 96. punkts).

Par PV lēmuma saturu

163 PV lēmuma 1. panta 1. punktā Komisija ir konstatējusi, ka ASV nodrošina pietiekamu to personas datu aizsardzības līmeni, kas no Savienības tiek pārsūtīti organizācijām, kuras reģistrētas ASV, Eiropas Savienības un ASV privātuma vairoga ietvaros, ko saskaņā ar šī lēmuma 1. panta 2. punktu veido principi, kurus ASV Tirdzniecības ministrija izdevusi 2016. gada 7. jūlijā un kuri izklāstīti minētā lēmuma II pielikumā, un oficiālie apgalvojumi un saistības, kas iekļautas dokumentos I un III–VII pielikumā.

164 Katrā ziņā PV lēmuma II pielikuma "[Eiropas Savienības] un ASV privātuma vairoga principi [..]" I.5. punktā ir arī precizēts, ka šo principu ievērošanu var ierobežot, "ciktāl tas ir vajadzīgs, lai ievērotu valsts drošību, sabiedrības intereses vai izpildītu tiesībaizsardzības prasības". Tā šajā lēmumā, gluži kā

Lēmumā 2000/520, ir iedibināts šo prasību pārākums pār principiem, saskaņā ar kuru pašsertificētām ASV organizācijām, kas personas datus saņem no Savienības, bez jebkādiem ierobežojumiem no šiem principiem ir jāatkāpjas, ja tie nonāk pretrunā minētajām prasībām un tādējādi izrādās ar tām nesaderīgi (pēc analoģijas attiecībā uz Lēmumu 2000/520 skat. spriedumu, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 86. punkts).

165 Ņemot vērā PV lēmuma II pielikuma I.5. punktā ietvertās atkāpes vispārējo raksturu, ar to ir radīta iespēja, pamatojoties uz prasībām, kas saistītas ar valsts drošību un sabiedrības interesēm vai ASV tiesisko regulējumu, iejaukties to personu pamattiesībās, kuru personas dati ir vai var tikt pārsūtīti no Savienības uz ASV (pēc analoģijas attiecībā uz Lēmumu 2000/520 skat. spriedumu, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 87. punkts). Konkrētāk, kā ir konstatēts PV lēmumā, šāda iejaukšanās var izrietēt no piekļuves personas datiem, kas no Savienības ir pārsūtīti uz ASV, un no tā, ka šos datus izmanto ASV publiskās iestādes *PRISM* un *UPSTREAM* uzraudzības programmu ietvaros, kuru pamatā ir ĀIUL 702. pants, kā arī *E.O. 12333*.

166 Šādā kontekstā Komisija PV lēmuma 67.–135. apsvērumā ir analizējusi ASV tiesiskajā regulējumā paredzētos ierobežojumus un garantijas, tostarp arī ĀIUL 702. pantā, *E.O. 12333* un *PPD-28* ietvertos, attiecībā uz piekļuvi datiem, kuri tiek nosūtīti Eiropas Savienības un ASV privātuma vairoga ietvaros, un to izmantošanu ASV publiskajās iestādēs valsts drošības, tiesībaizsardzības un citu valsts interešu nolūkos.

167 Šī novērtējuma beigās Komisija šī lēmuma 136. apsvērumā ir konstatējusi, ka "Amerikas Savienotās Valstis nodrošina pienācīgu to personas datu aizsardzības līmeni, kurus [Savienība] pārsūta uz pašsertificētām organizācijām Amerikas Savienotajās Valstīs", un minētā lēmuma 140. apsvērumā tā ir paudusi, ka, "pamatojoties uz pieejamo informāciju par ASV tiesību sistēmu, tostarp ASV valdības apgalvojumiem un saistībām, Komisija uzskata, ka jebkāda ASV valsts iestāžu iejaukšanās to personu pamattiesībās, kuru dati privātuma vairoga ietvaros no Savienības tiek nosūtīti uz Amerikas Savienotajām Valstīm, ja tas notiek valsts drošības, tiesībaizsardzības vai citu valsts interešu nolūkos, un sekojošie ierobežojumi, kas piemēroti pašsertificētām organizācijām attiecībā uz to principialitāti, būs ierobežoti līdz tādam apmēram, kas ir absolūti nepieciešams, lai sasniegtu attiecīgo likumīgo mērķi, un tādējādi tie nodrošina efektīvu tiesisko aizsardzību pret šādu iejaukšanos".

Par pietiekama aizsardzības līmeņa konstatējumu

168 Ņemot vērā elementus, kurus Komisija ir minējusi PV lēmumā, kā arī iesniedzējtiesas konstatētos elementus pamatlietā, šai tiesai ir šaubas par to, vai ASV tiesības patiešām nodrošina pietiekamu aizsardzības līmeni, kas prasīts VDAR 45. pantā, skatot to Hartas 7., 8. un 47. pantā garantēto pamattiesību kontekstā. It īpaši minētā tiesa uzskata, ka šīs trešās valsts tiesībās nav paredzēti ierobežojumi un garantijas, kas nepieciešamas attiecībā uz valsts tiesiskajā regulējumā atļauto iejaukšanos, kā arī šīs valsts tiesības nenodrošina efektīvu tiesību aizsardzību tiesā pret šādu iejaukšanos. Šajā pēdējā ziņā tā piebilst, ka "privātuma vairoga" ombuda izveide, tās ieskatā, nevar novērst šīs nepilnības, jo šo ombudu nevar pielīdzināt tiesai Hartas 47. panta izpratnē.

169 Pirmkārt, runājot par Hartas 7. un 8. pantu, kas veido Savienībā prasīto aizsardzības līmeni, kura ievērošana Komisijai ir jākonstatē, pirms tā pieņem lēmumu par aizsardzības līmeņa pietiekamību saskaņā ar VDAR 45. panta 1. punktu, ir jāatgādina, ka Hartas 7. pantā ikvienai personai ir garantētas tiesības uz savas privātās un ģimenes dzīves, mājokļa un saziņas neaizskaramību. Turklāt Hartas 8. panta 1. punktā ikvienai personai ir skaidri piešķirtas tiesības uz savu personas datu aizsardzību.

170 Tādējādi piekļuve fiziskas personas datiem, lai tos saglabātu vai izmantotu, ietekmē šīs personas pamattiesības uz privātās dzīves neaizskaramību, kas garantētas Hartas 7. pantā, jo šīs tiesības attiecas uz jebkādu informāciju par identificētu vai identificējamu fizisku personu. Turklāt minētā datu apstrāde attiecas arī uz Hartas 8. pantu tāpēc, ka tā ir personas datu apstrāde šī panta izpratnē un līdz

ar to tai katrā ziņā ir jāatbilst šajā pantā paredzētajām datu aizsardzības prasībām (šajā nozīmē skat. spriedumus, 2010. gada 9. novembris, *Volker und Markus Schecke* un *Eifert*, C-92/09 un C-93/09, EU:C:2010:662, 49. un 52. punkts; 2014. gada 8. aprīlis, *Digital Rights Ireland* u.c., C-293/12 un C-594/12, EU:C:2014:238, 29. punkts, kā arī atzinumu 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 122. un 123. punkts).

171 Tiesa jau ir nospriedusi, ka personas datu izpaušana trešajai personai, piemēram, valsts iestādei, ir iejaukšanās Hartas 7. un 8. pantā noteiktajās pamattiesībās, lai kāda būtu izpaustās informācijas vēlāka izmantošana. Tas pats attiecas uz personas datu saglabāšanu, kā arī uz piekļuvi minētajiem datiem, lai valsts iestādes tos izmantotu, neatkarīgi no tā, vai attiecīgajai informācijai par privāto dzīvi ir vai nav sensitīvs raksturs un vai ieinteresētajām personām ir vai nav radītas iespējamas neērtības šīs iejaukšanās dēļ (šajā nozīmē skat. spriedumus, 2003. gada 20. maijs, *Österreichischer Rundfunk* u.c., C-465/00, C-138/01 un C-139/01, EU:C:2003:294, 74. un 75. punkts; 2014. gada 8. aprīlis, *Digital Rights Ireland* u.c., C-293/12 un C-594/12, EU:C:2014:238, 33.–36. punkts, kā arī atzinumu 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 124. un 126. punkts).

172 Tomēr Hartas 7. un 8. pantā noteiktās tiesības nav uztveramas kā absolūtas prerogatīvas, bet gan jāaplūko saistībā ar to funkciju sabiedrībā (šajā nozīmē skat. spriedumus, 2010. gada 9. novembris, *Volker und Markus Schecke* un *Eifert*, C-92/09 un C-93/09, EU:C:2010:662, 48. punkts un tajā minētā judikatūra; 2013. gada 17. oktobris, *Schwarz*, C-291/12, EU:C:2013:670, 33. punkts un tajā minētā judikatūra, kā arī atzinumu 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 136. punkts).

173 Šajā ziņā vēl ir jānorāda, ka saskaņā ar Hartas 8. panta 2. punktu personas dati "ir jāapstrādā godprātīgi, noteiktiem mērķiem un ar attiecīgās personas piekrišanu vai ar citu likumīgu pamatojumu, kas paredzēts tiesību aktos".

174 Turklāt saskaņā ar Hartas 52. panta 1. punkta pirmo teikumu visiem šajā hartā atzīto tiesību un brīvību izmantošanas ierobežojumiem ir jābūt noteiktiem tiesību aktos un tajos jārespektē šo tiesību un brīvību būtība. Atbilstoši Hartas 52. panta 1. punkta otrajam teikumam, ievērojot samērīguma principu, ierobežojumus šīm tiesībām un brīvībām drīkst uzlikt tikai tad, ja tie ir nepieciešami un patiešām atbilst vispārējo interešu mērķiem, ko atzinusi Savienība, vai vajadzībai aizsargāt citu personu tiesības un brīvības.

175 Šajā ziņā jāpiebilst, 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 (atzinums 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 139. punkts un tajā minētā judikatūra).

176 Visbeidzot, lai izpildītu samērīguma prasību, saskaņā ar kuru atkāpes no personas datu aizsardzības un tās ierobežojumi ir jāīsteno, stingri ievērojot vajadzīgās robežas, attiecīgajā tiesiskajā regulējumā, kas paredz iejaukšanos, ir jānosaka skaidri un precīzi noteikumi, kas reglamentē attiecīgā pasākuma tvērumu un piemērošanu un paredz minimālas prasības, lai tā rezultātā personām, kuru dati tikuši pārsūtīti, būtu pietiekamas garantijas, kas ļautu viņu personas 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 (šajā nozīmē skat. atzinumu 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 140. un 141. punkts, kā arī tajos minētā judikatūra).

177 Šajā ziņā VDAR 45. panta 2. punkta a) apakšpunktā ir precizēts, ka, izvērtējot trešās valsts nodrošinātā aizsardzības līmeņa pietiekamību, Komisija it īpaši ņem vērā to, vai pastāv "efektīvas un īstenojamas tiesības, kas attiecas uz datu subjektiem", kuru personas dati tiek pārsūtīti.

178 Šajā gadījumā Komisijas konstatējums PV lēmumā, ka ASV nodrošina būtībā līdzvērtīgu aizsardzības līmeni tam, kas Savienībā nodrošināts ar VDAR, skatot to Hartas 7. un 8. panta kontekstā, tika apšaubīts tostarp tādēļ, ka iejaukšanās, kura izriet no uzraudzības programmām, kas balstītas uz ĀIUL 702. pantu un *E.O. 12333*, nav pakļautas prasībām, kuras, ievērojot samērīguma principu, nodrošina aizsardzības līmeni, kas būtībā ir līdzvērtīgs Hartas 52. panta 1. punkta otrajā teikumā garantētajam. Līdz ar to ir jāpārbauda, vai šīs uzraudzības programmas tiek īstenotas, ievērojot šādas prasības, un nav vispirms jāpārbauda, vai šī trešā valsts ievēro nosacījumus, kas būtībā ir līdzvērtīgi tiem, kuri ir paredzēti Hartas 52. panta 1. punkta pirmajā teikumā.

179 Šajā ziņā attiecībā uz uzraudzības programmām, kas balstītas uz ĀIUL 702. pantu, PV lēmuma 109. apsvērumā Komisija konstatēja, ka atbilstoši minētajam pantam "ĀIUT neapstiprina individuālus uzraudzības pasākumus, bet gan uzraudzības programmas (piemēram, *PRISM*, *UPSTREAM*), pamatojoties uz ikgadējām sertifikācijām, kuras sagatavo ģenerālprokurors un nacionālās izlūkošanas direktors". Kā izriet no šī paša apsvēruma, ĀIUT kontrole ir vērsta uz to, lai pārbaudītu, vai šīs uzraudzības programmas atbilst mērķim iegūt informāciju par ārējo izlūkošanu, bet tā neattiecas uz jautājumu, "vai personas ir atbilstīgi izsekotas, lai iegūtu ārvalstu izlūkošanas informāciju".

180 Tādējādi šķiet, ka no ĀIUL 702. panta nekādā veidā neizriet ne tas, ka pastāv tajā paredzētie pilnvaru ierobežojumi attiecībā uz uzraudzības programmu īstenošanu ārējās izlūkošanas mērķiem, ne arī garantiju esamība personām, kuras nav Amerikas pilsoņi un kuras potenciāli skar šīs programmas. Šādos apstākļos un kā secinājumu 291., 292. un 297. punktā būtībā ir norādījis ģenerāladvokāts, ar šo pantu nevar tikt nodrošināts tāds aizsardzības līmenis, kas būtībā būtu līdzvērtīgs Hartā garantētajam, kā tas ir interpretēts šī sprieduma 175. un 176. punktā atgādinātajā judikatūrā, saskaņā ar kuru pašā juridiskajā pamatā, kas ļauj iejaukties pamattiesībās, lai tas atbilstu samērīguma principam, ir jānosaka attiecīgo tiesību īstenošanas ierobežojuma apjoms un tajā ir jāparedz skaidri un precīzi noteikumi attiecībā uz konkrētā pasākuma tvērumu un piemērošanu, un jāparedz minimālās prasības.

181 Atbilstoši PV lēmumā konstatētajam uz ĀIUL 702. pantu balstītās uzraudzības programmas, protams, ir jāīsteno atbilstoši no *PPD-28* izrietošajām prasībām. Taču, lai gan Komisija PV lēmuma 69. un 77. apsvērumā ir uzsvērusi, ka šādām prasībām ir saistošs raksturs Amerikas izlūkdienestiem, Amerikas valdība, atbildot uz Tiesas jautājumu, ir piekritusi, ka *PPD-28* datu subjektiem nepiešķir tiesības, kuras tās tiesās varētu īstenot pret Amerikas iestādēm. Līdz ar to pretēji tam, kas ir prasīts VDAR 45. panta 2. punkta a) apakšpunktā, saskaņā ar kuru šī aizsardzības līmeņa konstatējums ir atkarīgs it īpaši no tā, vai personām, kuru dati ir pārsūtīti uz attiecīgo trešo valsti, pastāv efektīvas un īstenojamas tiesības, ar to nevar nodrošināt būtībā līdzvērtīgu aizsardzības līmeni tam, kāds izriet no Hartas.

182 Attiecībā uz uzraudzības programmām, kas balstītas uz *E.O. 12333*, no Tiesas rīcībā esošajiem lietas materiāliem izriet, ka arī šajā dekrētā ASV iestādēm nav piešķirtas īstenojamas tiesības.

183 Ir jāpiebilst, ka *PPD-28*, kas ir jāievēro saistībā ar iepriekšējos divos punktos minēto programmu piemērošanu, ļauj ""lielapjoma" vākšanu [jeb] sakaru izlūkošanas informācijas vai datu iegūšanu relatīvi lielā daudzumā apstākļos, kad izlūkdienesti vākšanas fokusēšanai nevar izmantot identifikatoru, kas saistīts ar konkrētu mērķi", kā tas ir precizēts PV lēmuma VI pielikumā ietvertajā Valsts izlūkdienesta direktora biroja (*Office of the Director of National Intelligence*) 2016. gada 21. jūnija vēstulē ASV Tirdzniecības ministrijai, kā arī Starptautiskās tirdzniecības administrācijai. Tomēr šī iespēja, kas uz *E.O. 12333* balstīto uzraudzības programmu ietvaros ļauj piekļūt tranzītā uz ASV esošiem datiem bez jebkādas tiesas uzraudzības, katrā ziņā pietiekami skaidri un precīzi nenosaka šādas personas datu lielapjoma datu vākšanas tvērumu.

184 Tādēļ nedz ĀIUL 702. pants, nedz *E.O. 12333*, lasot tos kopā ar *PPD-28*, neatbilst minimālajām prasībām, kas Savienības tiesībās izriet no samērīguma principa, un līdz ar to nevar uzskatīt, ka uz šīm tiesību normām balstītās uzraudzības programmas ir ierobežotas ar absolūti nepieciešamo.

185 Šādos apstākļos personas datu aizsardzības ierobežojumi, kas izriet no ASV iekšējā tiesiskā regulējuma par ASV publisko iestāžu piekļuvi no Savienības uz ASV pārsūtītiem personas datiem un šādu datu izmantošanu, kurus Komisija ir izvērtējusi PV lēmumā, nav ierobežoti tādā veidā, lai atbilstu prasībām, kas būtībā ir līdzvērtīgas tām, kuras Savienības tiesībās ir izvirzītas Hartas 52. panta 1. punkta otrajā teikumā.

186 Otrkārt, attiecībā uz Hartas 47. pantu, kas atbilst arī Savienībā prasītajam aizsardzības līmenim, kura ievērošana Komisijai ir jākonstatē, pirms tā pieņem lēmumu par atbilstību saskaņā ar VDAR 45. panta 1. punktu, ir jāatgādina, ka šī 47. panta pirmajā daļā ir prasīts, lai ikvienai personai, kuras tiesības un brīvības, kas garantētas Savienības tiesībās, tikušas pārkāptas, būtu tiesības uz efektīvu tiesību aizsardzību tiesā, ievērojot šī panta nosacījumus. Saskaņā ar šī panta otro daļu ikvienai personai ir tiesības uz lietas izskatīšanu neatkarīgā un objektīvā tiesā.

187 Atbilstoši pastāvīgajai judikatūrai tiesiskai valstij ir raksturīga pārbaudes tiesā esamība, kuras mērķis ir nodrošināt Savienības tiesību normu ievērošanu. Šādi 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 (spriedums, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 95. punkts un tajā minētā judikatūra).

188 Šajā ziņā VDAR 45. panta 2. punkta a) apakšpunktā ir prasīts, ka, izvērtējot trešās valsts nodrošinātā aizsardzības līmeņa pietiekamību, Komisijai it īpaši ir jāņem vērā "efektīva aizsardzība administratīvā kārtā vai tiesā tiem datu subjektiem, kuru personas datus nosūta". VDAR 104. apsvērumā šai ziņā ir uzsvērts, ka trešajai valstij "būtu jānodrošina efektīva neatkarīga datu aizsardzības uzraudzība un būtu jāparedz sadarbības mehānismi ar dalībvalstu datu aizsardzības iestādēm", un precizēts, ka "datu subjektiem būtu jāparedz efektīvas un īstenojamas tiesības un efektīva aizsardzība administratīvā kārtā vai tiesā".

189 Šādu efektīvu tiesību aizsardzības līdzekļu esamībai attiecīgajā trešajā valstī ir īpaša nozīme saistībā ar personas datu pārsūtīšanu uz šo trešo valsti, jo, kā izriet no VDAR 116. apsvēruma, datu subjekti var saskarties ar dalībvalstu administratīvo un tiesu iestāžu pilnvaru un līdzekļu nepietiekamību, lai efektīvi izskatītu viņu sūdzības, kas ir pamatotas ar iespējami prettiesisku viņu šādi pārsūtīto datu apstrādi šajā trešajā valstī, un tas var likt tām vērsties šīs pašas trešās valsts iestādēs un tiesās.

190 Šajā gadījumā Komisijas konstatējums PV lēmumā, saskaņā ar kuru ASV nodrošina būtībā līdzvērtīgu aizsardzības līmeni tam, kas ir garantēts Hartas 47. pantā, tostarp tika apšaubīts tādēļ, ka datu aizsardzības vairoga ombuda izveide nevar kompensēt pašas Komisijas konstatētos trūkumus attiecībā uz to personu tiesisko aizsardzību, kuru personas dati tiek pārsūtīti uz šo trešo valsti.

191 Šajā ziņā Komisija PV lēmuma 115. apsvērumā ir norādījusi, ka, "lai arī [..] personām, tostarp [Savienības] datu subjektiem, ir vairākas tiesiskās aizsardzības iespējas, ja tās ir pakļautas nelikumīgai (elektroniskajai) uzraudzībai nacionālās drošības nolūkos, tikpat skaidrs ir tas, ka nav iekļauti atsevišķi juridiskie pamatojumi (piemēram, *E.O. 12333*), kurus var izmantot ASV izlūkošanas iestādes". Tādējādi attiecībā uz *E.O. 12333* tā minētajā 115. apsvērumā ir uzsvērusi jebkādas pārsūdzības iespējas neesamību. Taču saskaņā ar šī sprieduma 187. punktā atgādināto judikatūru šāds trūkums tiesību aizsardzībā tiesā attiecībā uz iejaukšanos, kas saistīta ar informācijas programmām, kuras balstītas uz šo prezidenta dekrētu, ir šķērslis secinājumam, kuru PV lēmumā ir izdarījusi Komisija, ka ASV tiesības nodrošina būtībā līdzvērtīgu aizsardzības līmeni tam, kas ir garantēts Hartas 47. pantā.

192 Turklāt attiecībā uz uzraudzības programmām, kas balstītas uz ĀIUL 702. pantu un *E.O. 12333*, šī sprieduma 181. un 182. punktā ir atzīmēts, ka nedz *PPD-28*, nedz *E.O. 12333* datu subjektiem nepiešķir tiesības, kuras tie tiesās varētu īstenot pret Amerikas iestādēm, un līdz ar to šīm personām nav tiesību uz efektīvu tiesību aizsardzību.

193 Tomēr PV lēmuma 115. un 116. apsvērumā Komisija konstatēja, ka ASV iestāžu ieviestā ombuda mehānisma esamības dēļ, kā tas ir aprakstīts šī lēmuma III pielikumā ietvertajā Amerikas valsts sekretāra 2016. gada 7. jūlija vēstulē Eiropas Tieslietu, patērētāju un dzimumu līdztiesības komisārei, un ņemot vērā ombudam, kas šajā gadījumā ir "vecākais koordinators starptautiskās informācijas tehnoloģijas diplomātijas jautājumos", uzticētā uzdevuma raksturu, var uzskatīt, ka ASV nodrošina aizsardzības līmeni, kas ir būtībā līdzvērtīgs Hartas 47. pantā garantētajam.

194 Izskatot jautājumu par to, vai PV lēmumā minētais ombuda mehānisms patiešām var kompensēt Komisijas konstatētos tiesību uz tiesību aizsardzību tiesā ierobežojumus, atbilstoši prasībām, kas izriet no Hartas 47. panta un šī sprieduma 187. punktā atgādinātās judikatūras, ir jābalstās uz principu, ka attiecīgajām personām ir jābūt iespējai izmantot tiesību aizsardzības līdzekļus neatkarīgā un objektīvā tiesā attiecībā uz piekļuvi to personas datiem, vai panākt šo datu labošanu vai dzēšanu.

195 Šī sprieduma 193. punktā minētajā vēstulē privātuma vairoga ombuds, lai gan tas ir aprakstīts kā "neatkarīgs no izlūkdienestiem", tika raksturots kā "tieši pakļauts valsts sekretāram, kas nodrošina, ka ombuds savus uzdevumus veic objektīvi un neatkarīgi no neatbilstīgas ietekmes, kas var ietekmēt sniedzamo atbildi". Turklāt papildus tam, kā Komisija ir konstatējusi šī lēmuma 116. apsvērumā, ka ombudu ir iecēlis valsts sekretārs un tas ir ASV Valsts departamenta neatņemama sastāvdaļa, minētajā lēmumā, kā ģenerāladvokāts ir norādījis secinājumu 337. punktā, nav nevienas norādes, ka ombuda atsaukšanu vai tā iecelšanas atcelšanu papildina īpašas garantijas (šajā nozīmē skat. spriedumu, 2020. gada 21. janvāris, *Banco de Santander*, C-274/14, EU:C:2020:17, 60. un 63. punkts, kā arī tajos minētā judikatūra).

196 Tāpat, kā ģenerāladvokāts ir uzsvēris secinājumu 338. punktā, lai gan PV lēmuma 120. apsvērumā ir norādīts uz ASV valdības apņemšanos, ka attiecīgajam izlūkdienestu elementam ir jānovērš jebkurš piemērojamo normu pārkāpums, ko konstatējis ombuds, minētajā lēmumā nav nekādu norāžu par to, ka ombuds būtu tiesīgs pieņemt saistošus lēmumus attiecībā uz šiem dienestiem, un nav arī tiesisko garantiju, kuras papildinātu šo apņemšanos un uz kurām datu subjekti tad varētu atsaukties.

197 Tādējādi PV lēmumā minētais ombuda mehānisms nesniedz iestādē izmantojamus tiesību aizsardzības līdzekļus, kas personām, kuru dati tiek pārsūtīti uz ASV, sniegtu garantijas, kas būtībā ir līdzvērtīgas tām, kuras ir prasītas Hartas 47. pantā.

198 Tādējādi, PV lēmuma 1. panta 1. punktā konstatējot, ka ASV nodrošina pienācīgu to personas datu aizsardzības līmeni, kas no Savienības tiek pārsūtīti šajā trešajā valstī reģistrētām organizācijām Eiropas Savienības un ASV datu aizsardzības vairoga ietvaros, Komisija nav ievērojusi prasības, kas izriet no VDAR 45. panta 1. punkta, lasot to kopā ar Hartas 7., 8. un 47. pantu.

199 No tā izriet, ka PV lēmuma 1. pants nav saderīgs ar VDAR 45. panta 1. punktu, lasot to Hartas 7., 8. un 47. panta kontekstā, un tādēļ tas nav spēkā.

200 Tā kā PV lēmuma 1. pants nav nodalāms no šī lēmuma 2.–6. panta, kā arī tā pielikumiem, tā spēkā neesamības rezultātā arī lēmums kopumā zaudē spēku.

201 Ņemot vērā visus iepriekš minētos apsvērumus, ir jāsecina, ka PV lēmums nav spēkā.

202 Attiecībā uz to, vai būtu jāsaglabā šī lēmuma sekas nolūkā izvairīties no tiesiskā vakuuma radīšanas (šajā nozīmē skat. spriedumu, 2016. gada 28. aprīlis, *Borealis Polyolefine* u.c., C-191/14, C-192/14, C-295/14, C-389/14 un no C-391/14 līdz C-393/14, EU:C:2016:311, 106. punkts), ir jānorāda, ka katrā ziņā, ņemot vērā VDAR 49. pantu, tāda lēmuma par aizsardzības līmeņa pietiekamību atcelšana, kāds ir PV lēmums, šādu tiesisko vakuumu nerada. Proti, šajā pantā ir ietverti precīzi nosacījumi, ar kādiem personas datu pārsūtīšana uz trešajām valstīm var notikt, ja nav lēmuma par aizsardzības līmeņa pietiekamību saskaņā ar minētās regulas 45. panta 3. punktu vai atbilstošas garantijas saskaņā ar šīs pašas regulas 46. pantu.

Par tiesāšanās izdevumiem

203 Attiecībā uz pamatlietas pusēm šī tiesvedība ir stadija procesā, kuru izskata iesniedzējtiesa, un tā lemj par tiesāšanās izdevumiem. Izdevumi, kas radušies, iesniedzot apsvērumus Tiesai, un kas nav minēto pušu izdevumi, nav atlīdzināmi.

Ar šādu pamatojumu Tiesa (virspalāta) nospriež:

1) **Eiropas Parlamenta un Padomes Regulas (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 (Vispārīgā datu aizsardzības regula), 2. panta 1. un 2. punkts ir jāinterpretē tādējādi, ka šīs regulas piemērošanas jomā ietilpst personas datu pārsūtīšana, ko kādā dalībvalstī reģistrēts tirgus dalībnieks komerciālā nolūkā veic citam tirgus dalībniekam, kurš ir reģistrēts trešajā valstī, neraugoties uz iespēju, ka šīs nosūtīšanas laikā vai pēc tam šos datus attiecīgās trešās valsts iestādes var apstrādāt sabiedriskās drošības, aizsardzības un valsts drošības nolūkā.**

2) **Regulas 2016/679 46. panta 1. punkts un 46. panta 2. punkta c) apakšpunkts ir jāinterpretē tādējādi, ka šajās tiesību normās paredzētajām atbilstošām garantijām, īstenojamām tiesībām un efektīvajiem tiesību aizsardzības līdzekļiem ir jānodrošina, lai to personu tiesībām, kuru personas dati tiek pārsūtīti uz trešo valsti, pamatojoties uz datu aizsardzības standartklauzulām, tiktu piemērots būtībā līdzvērtīgs aizsardzības līmenis, kāds ir garantēts Eiropas Savienībā ar šo regulu, lasot to kopā ar Eiropas Savienības Pamattiesību hartu. Tālab, novērtējot aizsardzības līmeni, kāds tiek nodrošināts šādas pārsūtīšanas kontekstā, it īpaši ir jāņem vērā gan līguma noteikumi, par kuriem ir panākta vienošanās starp personas datu pārzini vai apstrādātāju, kas reģistrēts Savienībā, un attiecīgajā trešajā valstī reģistrēto saņēmēju, gan – attiecībā uz iespējamu šīs trešās valsts publisko iestāžu piekļuvi šādi pārsūtītajiem personas datiem – šīs trešās tiesību sistēmas būtiskie elementi, it īpaši minētās regulas 45. panta 2. punktā nosauktie.**

3) **Regulas 2016/679 58. panta 2. punkta f) un j) apakšpunkts ir jāinterpretē tādējādi, ka, ja vien pastāv likumīgi pieņemts Eiropas Komisijas lēmums par aizsardzības līmeņa pietiekamību, kompetentajai uzraudzības iestādei ir jāaptur vai jāaizliedz tāda personas datu pārsūtīšana uz trešo valsti, kuru pamatā ir Komisijas pieņemtās datu aizsardzības standartklauzulas, ja šī uzraudzības iestāde, ievērojot visus šīs pārsūtīšanas īpašos apstākļus, uzskata, ka šīs klauzulas šajā trešajā valstī netiek vai nevar tikt ievērotas un ka pārsūtīto datu aizsardzība, kāda tā ir prasīta Savienības tiesībās, konkrēti, šīs regulas 45. un 46. pantā un Pamattiesību hartā, nevar tikt nodrošināta ar citiem līdzekļiem, ja Savienībā reģistrētais datu pārzinis vai apstrādātājs nav pats apturējis vai izbeidzis šo pārsūtīšanu.**

4) **Komisijas Lēmuma 2010/87/ES (2010. gada 5. februāris) par līguma standartklauzulām attiecībā uz personas datu pārsūtīšanu trešās valstīs reģistrētiem apstrādātājiem saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK, kurā grozījumi izdarīti ar Komisijas Īstenošanas lēmumu (ES) 2016/2297 (2016. gada 16. decembris), pārbaude Pamattiesību hartas 7., 8. un 47. panta kontekstā nav atklājusi nevienu elementu, kas varētu ietekmēt šī lēmuma spēkā esamību.**

5) **Komisijas Īstenošanas lēmums (ES) 2016/1250 (2016. gada 12. jūlijs) saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK par pienācīgu aizsardzību, ko nodrošina ES un ASV privātuma vairogs, nav spēkā.**

[Paraksti]