Zbornik sudske prakse

PRESUDA SUDA (veliko vijeće)

16. srpnja 2020.*

„Zahtjev za prethodnu odluku – Zaštita fizičkih osoba u vezi s obradom osobnih podataka – Povelja Europske unije o temeljnim pravima – Članci 7., 8. i 47. – Uredba (EU) 2016/679 – Članak 2. stavak 2. – Područje primjene – Prijenosi osobnih podataka trećim zemljama u komercijalne svrhe – Članak 45. – Komisijina odluka o primjerenosti – Članak 46. – Prijenosi uz odgovarajuće zaštitne mjere – Članak 58. – Ovlasti nadzornih tijela – Obrada prenesenih podataka koju za potrebe nacionalne sigurnosti izvršavaju javna tijela treće zemlje – Ocjena primjerenosti razine zaštite koju osigurava treća zemlja – Odluka 2010/87/EU – Standardne klauzule o zaštiti za prijenos osobnih podataka trećoj zemlji – Odgovarajuće mjere zaštite koje nudi voditelj obrade – Valjanost – Provedbena odluka (EU) 2016/1250 – Primjerenost zaštite koju osigurava europsko-američki sustav zaštite privatnosti – Valjanost – Pritužba fizičke osobe čiji su podaci preneseni iz Europske unije u Sjedinjene Američke Države”

U predmetu C-311/18,

povodom zahtjeva za prethodnu odluku na temelju članka 267. UFEU-a, koji je uputio High Court (Visoki sud, Irska), odlukom od 4. svibnja 2018., koju je Sud zaprimio 9. svibnja 2018., u postupku

Data Protection Commissioner

protiv

Facebook Ireland Ltd,

Maximilliana Schremsa,

uz sudjelovanje:

The United States of America,

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

SUD (veliko vijeće),

u sastavu: K. Lenaerts, predsjednik, R. Silva de Lapuerta, potpredsjednica, A. Arabadjiev, A. Prechal, M. Vilaras, M. Safjan, S. Rodin, P. G. Xuereb, L. S. Rossi i I. Jarukaitis, predsjednici vijeća, M. Ilešič, T. von Danwitz (izvjestitelj) i D. Šváby, suci,

* Jezik postupka: engleski

nezavisni odvjetnik: H. Saugmandsgaard Øe,

tajnik: C. Strömholm, administratorica,

uzimajući u obzir pisani postupak i nakon rasprave održane 9. srpnja 2019.,

uzimajući u obzir očitovanja koja su podnijeli:

– za Data Protection Commissioner, D. Young, *solicitor*, B. Murray i M. Collins, *SC*, i C. Donnelly, *BL*,

– za Facebook Ireland Ltd, P. Gallagher i N. Hyland, *SC*, A. Mulligan, i F. Kieran, *BL* te P. Nolan, C. Monaghan, C. O'Neill i R. Woulfe, *solicitors*,

– za M. Schremsa, H. Hofmann, *Rechtsanwalt*, E. McCullough, J. Doherty i S. O'Sullivan, *SC*, te G. Rudden, *solicitor*,

– za The United States of America, E. Barrington, *SC*, S. Kingston, *BL*, te S. Barton i B. Walsh, *solicitors*,

– Za Electronic Privacy Information Centre, S. Lucey, *solicitor*, G. Gilmore i A. Butler, *BL*, te C. O'Dwyer, *SC*,

– za BSA Business Software Alliance Inc., B. Van Vooren i K. Van Quathem, *advocaten*,

– za Digitaleurope, N. Cahill, *barrister*, J. Cahir, *solicitor*, i M. Cush, *SC*,

– za Irsku, A. Joyce i M. Browne, u svojstvu agenata, uz asistenciju D. Fennellyja, *BL*,

– za belgijsku vladu, J.-C. Halleux i P. Cottin, u svojstvu agenata,

– za češku vladu, M. Smolek, J. Vláčil, O. Serdula i A. Kasalická, u svojstvu agenata,

– za njemačku vladu, J. Möller, D. Klebs i T. Henze, u svojstvu agenata,

– za francusku vladu, A.-L. Desjonquères, u svojstvu agenta,

– za nizozemsku vladu, C. S. Schillemans, K. Bulterman i M. Noort, u svojstvu agenata,

– za austrijsku vladu, J. Schmoll i G. Kunnert, u svojstvu agenata,

– za poljsku vladu, B. Majczyna, u svojstvu agenta,

– za portugalsku vladu, L. Inez Fernandes, A. Pimenta i C. Vieira Guerra, u svojstvu agenata,

– za vladu Ujedinjene Kraljevine, S. Brandon, u svojstvu agenata, uz asistenciju J. Holmes, *QC*, i C. Knight, *barrister*,

– za Europski parlament, J. Martínez Iglesias i A. Caiola, u svojstvu agenata,

– za Europsku komisiju, D. Nardi, H. Krämer i H. Kranenborg, u svojstvu agenata,

– za Europski odbor za zaštitu podataka (EOZP), A. Jelinek i K. Behn, u svojstvu agenata,

saslušavši mišljenje nezavisnog odvjetnika na raspravi održanoj 19. prosinca 2019.,

donosi sljedeću

Presudu

1 Zahtjev za prethodnu odluku u bitnom se odnosi na:

– tumačenje članka 3. stavka 2. prve alineje, članaka 25. i 26. te članka 28. stavka 3. Direktive 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (SL 1995., L 281, str. 31.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 7., str. 88.), u vezi s člankom 4. stavkom 2. UEU-a i člancima 7., 8. i 47. Povelje Europske unije o temeljnim pravima (u daljnjem tekstu: Povelja).

– tumačenje i valjanost Odluke Komisije 2010/87/EU od 5. veljače 2010. o standardnim ugovornim klauzulama za prijenos osobnih podataka obrađivačima u trećim zemljama u skladu s Direktivom 95/46 (SL 2010., L 39, str. 5.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 52., str. 250.), kako je izmijenjena Provedbenom odlukom Komisije (EU) 2016/2297 od 16. prosinca 2016. (SL 2016., L 344, str. 100.) (u daljnjem tekstu: Odluka o standardnim ugovornim klauzulama) te na

– tumačenje i valjanost Provedbene odluke Komisije (EU) 2016/1250 od 12. srpnja 2016. o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti u skladu s Direktivom 95/46 (SL 2016., L 207, str. 1.) (u daljnjem tekstu: Odluka o sustavu zaštite privatnosti).

2 Zahtjev je upućen u okviru spora između Data Protection Commissionera (povjerenik za zaštitu podataka, Irska) (u daljnjem tekstu: povjerenik), s jedne strane, i društva Facebook Ireland Ltd i Maximilliana Schremsa, s druge strane, povodom pritužbe potonjeg u vezi s prijenosom njegovih osobnih podataka iz društva Facebook Ireland društvu Facebook Inc. u Sjedinjenim Američkim Državama.

Pravni okvir

Direktiva 95/46

3 Članak 3. Direktive 95/46, naslovljen „Područje primjene”, u svojem stavku 2. navodi:

„Ova se Direktiva ne primjenjuje na obradu osobnih podataka:

– tijekom aktivnosti koja je izvan područja primjene prava Zajednice, kao što je predviđeno u glavama V. i VI. Ugovora o Europskoj uniji i u svakom slučaju na postupke obrade koji se odnose na javnu sigurnost, obranu, nacionalnu sigurnost (uključujući gospodarsku dobrobit države kada se operacija obrade odnosi na pitanja nacionalne sigurnosti) i aktivnosti države u području kaznenog prava,

[…]”

4 Člankom 25. te direktive određivalo se:

„1. Države članice osiguravaju da se prijenos osobnih podataka […] može izvršiti jedino ako, ne dovodeći u pitanje nacionalne odredbe donesene u skladu s drugim odredbama ove Direktive, te treće zemlje osiguraju odgovarajuću razinu zaštite.

2. Odgovarajuća razina zaštite koju osiguravaju treće zemlje procjenjuje se ovisno o svim okolnostima u vezi s prijenosom podataka ili skupom postupaka prijenosa podataka; […].

[…]

6. Komisija može u skladu s postupkom iz članka 31. stavka 2. ove Direktive, utvrditi da treća zemlja temeljem domaćeg zakonodavstva ili međunarodnih obveza koje je preuzela, osigurava odgovarajuću razinu zaštite u smislu stavka 2. ovog članka, posebno nakon završetka pregovora iz stavka 5. ovog članka, za zaštitu privatnog života i osnovnih sloboda i prava pojedinaca.

Države članice poduzimaju mjere potrebne za usklađivanje s odlukom Komisije."

5 Članak 26. navedene direktive je u stavcima 2. i 4. propisivao:

„2. Ne dovodeći u pitanje stavak 1. ovog članka, država članica može odobriti prijenos ili skup prijenosa osobnih podataka trećoj zemlji koja ne osigurava odgovarajuću razinu zaštite u smislu članka 25. stavka 2. ove Direktive, kada nadzornik daje dovoljna jamstva u vezi zaštite privatnosti i temeljnih prava i sloboda pojedinaca te u vezi ostvarivanja tih prava; takva jamstva mogu posebno proizlaziti iz odgovarajućih ugovornih klauzula.

[…]

4. Ako Komisija odluči, u skladu s postupkom iz članka 31. stavka 2. ove Direktive, da neke standardne ugovorne klauzule daju dovoljna jamstva iz stavka 2. ovog članka, države članice poduzimaju odgovarajuće mjere za usklađivanje s odlukom Komisije."

6 U skladu s njezinim člankom 28. stavkom 3. iste direktive:

„Svako tijelo posebno ima:

– istražne ovlasti, kao što je ovlast pristupa podacima koji su predmet postupaka obrade i ovlasti za prikupljanje svih podataka potrebnih za izvršavanje svojih nadzornih dužnosti,

– učinkovite ovlasti za posredovanje, kao što je na primjer davanje mišljenja prije nego li se izvrše postupci obrade, u skladu s člankom 20. ove Direktive, te osiguranje odgovarajuće objave takvih mišljenja te ovlasti naređivanja blokiranja, brisanja ili uništavanja podataka, nametanja privremene ili konačne zabrane obrade, upozoravanja ili opominjanja nadzornika ili upućivanja predmeta nacionalnim parlamentima ili drugim političkim institucijama,

– ovlast za sudjelovanje u sudskim postupcima ako su prekršene nacionalne odredbe donesene u skladu s ovom direktivom ili za upoznavanje sudskih tijela s tim kršenjima.

[…]"

Opća uredba o zaštiti podataka (GDPR)

7 Direktiva 95/46 stavljena je izvan snage i zamijenjena Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46 (Opća uredba o zaštiti podataka) (SL 2016., L 119, str. 1. i ispravak SL 2018., L 127, str. 2.; u daljnjem tekstu: GDPR).

8 Uvodne izjave 6., 10., 101., 103., 104., 107. do 109., 114., 116. i 141. GDPR-a glase:

„6. Zbog brzog tehnološkog razvoja i globalizacije pojavili su se novi izazovi u zaštiti osobnih podataka. Opseg prikupljanja i razmjene osobnih podataka značajno se povećava. Tehnologijom se privatnim društvima i tijelima javne vlasti omogućuje uporaba osobnih podataka u dosada nedosegnutom opsegu radi ostvarenja njihovih djelatnosti. Pojedinci svoje osobne informacije sve više čine dostupnima javno i globalno. Tehnologija je preobrazila i gospodarstvo i društveni život te bi trebala dalje olakšavati slobodan protok osobnih podataka u Uniji i prijenos trećim zemljama i međunarodnim organizacijama, osiguravajući pri tome visoku razinu zaštite osobnih podataka.

[…]

10. Kako bi se osigurala postojana i visoka razina zaštite pojedinaca te uklonile prepreke protoku osobnih podataka unutar Unije, razina zaštite prava i sloboda pojedinaca u vezi s obradom takvih podataka trebala bi biti jednaka u svim državama članicama. U cijeloj Uniji trebalo bi osigurati dosljednu i ujednačenu primjenu pravila za zaštitu temeljnih prava i sloboda fizičkih osoba pri obradi osobnih podataka. U pogledu obrade osobnih podataka za usklađivanje s pravnom obvezom, za izvršavanje zadaće od javnog interesa ili pri obavljanju službene ovlasti dodijeljene voditelju obrade državama članicama trebalo bi dopustiti da zadrže ili uvedu nacionalne odredbe kako bi se dodatno odredila primjena pravila iz ove Uredbe. Zajedno s općim i horizontalnim zakonodavstvom o zaštiti podataka kojim se provodi Direktiva 95/46/EZ, države članice imaju nekoliko posebnih zakona za pojedine sektore u onim područjima u kojima su potrebne konkretnije odredbe. Ovom Uredbom također se državama članicama pruža prostor za djelovanje kako bi bolje odredile njezina pravila uključujući obradu posebnih kategorija osobnih podataka (‚osjetljivi podaci'). U tom smislu ovom se Uredbom ne isključuje pravo države članice kojim se utvrđuju okolnosti posebnih situacija obrade, što uključuje preciznije određivanje uvjeta pod kojima je obrada osobnih podataka zakonita.

[…]

101. Tokovi osobnih podataka u zemlje izvan Unije i međunarodne organizacije i iz njih neophodni su za širenje međunarodne trgovine i međunarodne suradnje. Povećanje tih prijenosa dovelo je do novih izazova i briga u vezi sa zaštitom osobnih podataka. Međutim kada se osobni podaci prenose iz Unije voditeljima obrade, izvršiteljima obrade ili drugim primateljima u trećim zemljama ili međunarodnim organizacijama, ne bi smjela biti narušena razina zaštite pojedinaca osigurana ovom Uredbom u Uniji, među ostalim u slučajevima daljnjih prijenosa osobnih podataka iz treće zemlje ili međunarodne organizacije voditeljima obrade, izvršiteljima obrade u istoj ili nekoj drugoj trećoj zemlji ili međunarodnoj organizaciji. U svakom slučaju, prijenosi u treće zemlje i međunarodne organizacije mogu se obavljati isključivo uz puno poštovanje ove Uredbe. Prijenos bi se smio obavljati isključivo ako, u skladu s drugim odredbama ove Uredbe, voditelj obrade ili izvršitelj obrade ispunjavaju uvjete utvrđene u odredbama ove Uredbe vezanim za prijenos osobnih podataka trećim zemljama ili međunarodnim organizacijama.

[…]

103. Komisija može odlučiti s učinkom na cijelu Uniju da treća zemlja, područje ili posebni sektor u trećoj zemlji, ili međunarodna organizacija pruža odgovarajuću razinu zaštite podataka te na taj način pruža pravnu sigurnost i ujednačenost u cijeloj Uniji kad je riječ o trećoj zemlji ili međunarodnoj organizaciji za koju se smatra da pruža takvu razinu zaštite. U takvim slučajevima prijenosi osobnih podataka u te treću zemlju ili međunarodnu organizaciju mogu se obavljati bez potrebe za dobivanjem daljnjeg ovlaštenja. Komisija također može odlučiti da povuče takvu odluku, nakon što trećoj zemlji ili međunarodnoj organizaciji uputi obavijest i izjavu u kojoj se navode razlozi.

104. Sukladno s temeljnim vrijednostima na kojima se temelji Unija, osobito zaštitom ljudskih prava, pri svojoj procjeni treće zemlje ili područja ili posebnog sektora u trećoj zemlji Komisija bi trebala uzeti u obzir kako određena treća zemlja poštuje vladavinu prava, pristup pravosuđu kao i međunarodne norme i standarde ljudskih prava i njihove opće i sektorske zakone, uključujući zakonodavstvo o javnoj sigurnosti, obrani i nacionalnoj sigurnosti kao i javni poredak i kazneno pravo. Pri donošenju odluke o primjerenosti u vezi s područjem ili posebnim sektorom u trećoj zemlji trebalo bi uzeti u obzir jasne i objektivne kriterije, kao što su specifične aktivnosti obrade i područje primjene mjerodavnih zakonskih normi i zakonodavstva koji su na snazi u trećoj zemlji. Treća zemlja trebala bi ponuditi jamstva kojima se osigurava primjerena razina zaštite, u načelu istovjetna onoj koja je osigurana u Uniji, posebno kada se osobni podaci obrađuju u jednom ili više određenih sektora. Konkretno, treća zemlja trebala bi osigurati učinkovit neovisan nadzor zaštite podataka te mehanizme suradnje s tijelima država članica za zaštitu podataka dok bi ispitanici trebali imati učinkovita i ostvariva prava te učinkovitu upravnu i sudsku zaštitu.

[…]

107. Komisija može utvrditi da treća zemlja, područje ili posebni sektor u trećoj zemlji, ili međunarodna organizacija više ne osiguravaju primjereni stupanj zaštite podataka. Stoga bi se prijenos osobnih podataka u tu treću zemlju ili međunarodnu organizaciju trebao zabraniti, osim ako su ispunjeni uvjeti iz ove Uredbe koji se odnose na prijenose koji podliježu odgovarajućim zaštitnim mjerama, uključujući obvezujuća korporativna pravila, te odstupanja za posebne situacije. U tom slučaju trebalo bi predvidjeti savjetovanje između Komisije i takvih trećih zemalja ili međunarodnih organizacija. Komisija bi trebala pravodobno obavijestiti treću državu ili međunarodnu organizaciju o razlozima i započeti savjetovanja s njom kako bi se riješila situacija.

108. Ako nije donesena odluka o primjerenosti voditelj obrade ili izvršitelj obrade trebali bi poduzeti mjere kojima će se nadomjestiti nedostatak zaštite podataka u trećoj zemlji putem odgovarajućih zaštitnih mjera za ispitanika. Takve odgovarajuće zaštitne mjere mogu obuhvaćati uporabu obvezujućih korporativnih pravila, standardne klauzule o zaštiti podataka koje je usvojila Komisija, standardne klauzule o zaštiti podataka koje je usvojilo nadzorno tijelo ili ugovorne klauzule koje je odobrilo nadzorno tijelo. Tim zaštitnim mjerama trebalo bi osigurati sukladnost sa zahtjevima za zaštitu podataka i prava ispitanikâ primjereno obradi unutar Unije, uključujući dostupnost provedivih prava ispitanika i učinkovitih pravnih lijekova, među ostalim onih za dobivanje učinkovite upravne ili sudske zaštite i traženje naknade, u Uniji ili u trećoj zemlji. One bi se trebale osobito odnositi na usklađivanje s općim načelima koja se odnose na obradu osobnih podataka, načela tehničke i integrirane zaštite podataka. […]

109. Mogućnost da se voditelj obrade ili izvršitelj obrade koristi standardnim klauzulama o zaštiti podataka koje je donijela Komisija ili nadzorno tijelo ne bi trebala sprečavati mogućnost voditelja obrade ili izvršitelja obrade ni da uključe standardne klauzule o zaštiti podataka u širi ugovor, kao što je ugovor između izvršitelja obrade i drugog izvršitelja obrade, ni da dodaju druge klauzule ili dodatne zaštitne mjere pod uvjetom da one izravno ili neizravno ne proturječe standardnim ugovornim klauzulama koje je donijela Komisija ili nadzorno tijelo ili ne dovode u pitanje temeljna prava ili slobode ispitanika. Voditelje obrade i izvršitelje obrade trebalo bi poticati da osiguraju dodatne zaštitne mjere putem dodatnih ugovornih obveza koje nadopunjuju standardne klauzule o zaštiti.

[…]

114. U svakom slučaju, ako Komisija nije donijela odluku o odgovarajućoj razini zaštite podataka u trećoj zemlji, voditelj obrade ili izvršitelj obrade trebali bi iskoristiti rješenja koja ispitanicima osiguravaju ostvariva i učinkovita prava u pogledu obrade njihovih podataka u Uniji nakon što su ti podaci preneseni tako da će i dalje uživati zaštitu koju nude temeljna prava i zaštitne mjere.

[…]

116. Kada se osobni podaci kreću preko granica izvan Unije, može se povećati rizik koji prijeti sposobnosti pojedinaca da ostvare svoja prava na zaštitu podataka, osobito da se zaštite od nezakonite uporabe ili otkrivanja tih informacija. Nadzorna tijela mogu istodobno ustanoviti da nisu u mogućnosti obraditi žalbe ili provesti istrage vezane uz aktivnosti izvan svojih granica. Njihove napore da rade zajedno u prekograničnom kontekstu također mogu omesti nedovoljne ovlasti za sprečavanje ili ispravljanje, nedosljedni pravni režimi i praktične prepreke kao što su ograničeni resursi. […]

[…]

141. Svaki bi ispitanik trebao imati pravo podnijeti pritužbu jednom nadzornom tijelu, posebno u državi članici u kojoj ima uobičajeno boravište i imati pravo na učinkoviti pravni lijek u skladu s člankom 47. Povelje ako ispitanik smatra da su prekršena njegova prava iz ove Uredbe ili ako nadzorno tijelo ne postupi po pritužbi, djelomično ili u potpunosti odbaci ili odbije pritužbu ili ne djeluje kada je takvo djelovanje nužno radi zaštite prava ispitanika. […]”

9 Člankom 2. stavcima 1. i 2. navedene uredbe propisuje se:

„1. Ova se Uredba primjenjuje na potpuno ili djelomično automatiziranu obradu osobnih podataka te na neautomatiziranu obradu osobnih podataka koji su dio sustava pohrane ili su namijenjeni da budu dio sustava pohrane.

2. Ova se Uredba ne odnosi na obradu osobnih podataka:

(a) tijekom djelatnosti koja nije obuhvaćena opsegom prava Unije;

(b) koju obavljaju države članice kada obavljaju aktivnosti koje su obuhvaćene područjem primjene glave V. poglavlja 2. UEU-a;

(c) koju provodi fizička osoba tijekom isključivo osobnih ili kućnih aktivnosti;

(d) koju obavljaju nadležna tijela u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihova sprečavanja.”

10 Člankom 4. navedene uredbe propisuje se:

„Za potrebe ove Uredbe:

[…]

2. ‚obrada’ znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje;

[…]

7. ‚voditelj obrade' znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice;

8. ‚izvršitelj obrade' znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade;

9. ‚primatelj' znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili bilo koje drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana. Međutim, tijela javne vlasti koja mogu primiti osobne podatke u okviru određene istrage u skladu s pravom Unije ili države članice ne smatraju se primateljima; obrada tih podataka koju obavljaju ta tijela javne vlasti mora biti u skladu s primjenjivim pravilima o zaštiti podataka prema svrhama obrade;

[…]"

11 U članku 23. iste uredbe navodi se:

„1. Na temelju prava Unije ili prava države članice kojem podliježu voditelj obrade podataka ili izvršitelj obrade zakonskom mjerom može se ograničiti opseg obveza i prava iz članaka od 12. do 22. i članka 34. te članka 5. ako te odredbe odgovaraju pravima i obvezama predviđenima u člancima od 12. do 22., ako se takvim ograničenjem poštuje bit temeljnih prava i sloboda te ono predstavlja nužnu i razmjernu mjeru u demokratskom društvu za zaštitu:

(a) nacionalne sigurnosti;

(b) obrane;

(c) javne sigurnosti;

(d) sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenopravnih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje;

[…]

2. Osobito, svaka zakonodavna mjera iz stavka 1. sadrži posebne odredbe, prema potrebi, najmanje o:

(a) svrhama obrade ili kategorijama obrade;

(b) kategorijama osobnih podataka;

(c) opsegu uvedenih ograničenja;

(d) zaštitnim mjerama za sprečavanje zlouporabe ili nezakonitog pristupa ili prijenosa;

(e) specifikaciji voditelja obrade ili kategorija voditeljâ obrade;

(f) razdoblju pohrane i zaštitnim mjerama koje se mogu primijeniti uzimajući u obzir prirodu, opseg i svrhe obrade ili kategorije obrade;

(g) rizicima za prava i slobode ispitanika; i

(h) pravu ispitanika da budu obaviješteni o ograničenju, osim ako može biti štetno za svrhu tog ograničenja.”

12 Poglavlje V. GDPR-a naslovljeno „Prijenosi osobnih podataka trećim zemljama ili međunarodnim organizacijama” obuhvaća članke 44. do 50. te uredbe. U skladu s njezinim člankom 44. naslovljenim „Opća načela prijenosa”:

„Svaki prijenos osobnih podataka koji se obrađuju ili su namijenjeni za obradu nakon prijenosa u treću zemlju ili međunarodnu organizaciju odvija se jedino ako u skladu s drugim odredbama ove Uredbe voditelj obrade i izvršitelj obrade djeluju u skladu s uvjetima iz ovog poglavlja koji vrijede i za daljnje prijenose osobnih podataka iz treće zemlje ili međunarodne organizacije u još jednu treću zemlju ili međunarodnu organizaciju. Sve se odredbe iz ovog poglavlja primjenjuju kako bi se osiguralo da se ne ugrozi razina zaštite pojedinaca zajamčena ovom Uredbom.”

13 Članak 45. te uredbe naslovljen „Prijenosi na temelju odluke o primjerenosti” u stavcima 1. do 3. predviđa:

„1. Prijenos osobnih podataka trećoj zemlji ili međunarodnoj organizaciji može se dogoditi kada Komisija odluči da treća zemlja, područje, ili jedan ili više određenih sektora unutar te treće zemlje, ili međunarodna organizacija o kojoj je riječ osigurava primjerenu razinu zaštite. Takav prijenos ne zahtijeva posebno odobrenje.

2. Prilikom procjene primjerenosti stupnja zaštite Komisija osobito uzima u obzir sljedeće elemente:

(a) vladavinu prava, poštovanje ljudskih prava i temeljnih sloboda, relevantno zakonodavstvo, i opće i sektorsko, što uključuje zakonodavstvo o javnoj sigurnosti, obrani, nacionalnoj sigurnosti, kaznenom pravu i pristupu tijela javne vlasti osobnim podacima, kao i provedbu tog zakonodavstva, pravila o zaštiti podataka, pravila struke i mjere sigurnosti, što uključuje pravila za daljnji prijenos osobnih podataka još jednoj trećoj zemlji ili međunarodnoj organizaciji, koja se poštuju u toj trećoj zemlji ili međunarodnoj organizaciji, sudsku praksu te postojanje djelotvornih i provedivih prava ispitanika te učinkovite upravne i sudske zaštite ispitanika čiji se osobni podaci prenose;

(b) postojanje i djelotvorno funkcioniranje jednog neovisnog nadzornog tijela ili više njih u trećoj zemlji, ili tijela kojem podliježe međunarodna organizacija, s odgovornošću osiguravanja i provođenja poštovanja pravila o zaštiti podataka, što uključuje primjerene provedbene ovlasti za pomoć ispitanicima i savjetovanje ispitanika u ostvarivanju njihovih prava te za suradnju s nadzornim tijelima država članica; i

(c) međunarodne obveze koje je dotična treća zemlja ili međunarodna organizacija preuzela, ili druge obveze koje proizlaze iz pravno obvezujućih konvencija ili instrumenata, kao i iz njezina sudjelovanja u multilateralnim ili regionalnim sustavima, osobito u vezi sa zaštitom osobnih podataka.

3. Komisija nakon procjene primjerenosti stupnja zaštite može putem provedbenog akta odlučiti da treća zemlja, područje, ili jedan ili više određenih sektora unutar treće zemlje, ili međunarodna organizacija osigurava primjerenu razinu zaštite u smislu stavka 2. ovog članka. U provedbenom aktu predviđa se mehanizam za periodično preispitivanje, najmanje svake četiri godine, kojim će se uzeti u obzir svi relevantni događaji u toj trećoj zemlji ili međunarodnoj organizaciji. U provedbenom aktu precizira se teritorijalna i sektorska primjena, a prema potrebi utvrđuje se i nadzorno tijelo ili nadzorna tijela iz stavka 2. točke (b) ovog članka. Provedbeni akt donosi se u skladu s postupkom ispitivanja iz članka 93. stavka 2.”

14 Članak 46. navedene uredbe naslovljen „Prijenosi koji podliježu odgovarajućim zaštitnim mjerama” u stavcima 1. do 3. određuje:

„1. Ako nije donesena odluka na temelju članka 45. stavka 3., voditelj obrade ili izvršitelj obrade trećoj zemlji ili međunarodnoj organizaciji osobne podatke mogu prenijeti samo ako je voditelj obrade ili izvršitelj obrade predvidio odgovarajuće zaštitne mjere i pod uvjetom da su ispitanicima na raspolaganju provediva prava i učinkoviti pravni lijekovi.

2. Odgovarajuće zaštitne mjere iz stavka 1. mogu, bez potrebe za ikakvim posebnim ovlaštenjem nadzornog tijela, pružati:

(a) pravno obvezujući i provedivi instrument između tijela javne vlasti ili javnih tijela;

(b) obvezujuća korporativna pravila u skladu s člankom 47.;

(c) standardne klauzule o zaštiti podataka koje donosi Komisija u skladu s postupkom ispitivanja iz članka 93. stavka 2.;

(d) standardne klauzule o zaštiti podataka koje donosi nadzorno tijelo i koje Komisija odobrava u skladu s postupkom ispitivanja iz članka 93. stavka 2.;

(e) odobreni kodeks ponašanja u skladu s člankom 40. zajedno s obvezujućim i provedivim obvezama voditelja obrade ili izvršitelja obrade u trećoj zemlji za primjenu odgovarajućih zaštitnih mjera, među ostalim u pogledu prava ispitanika; ili

(f) odobreni mehanizam certificiranja u skladu s člankom 42. zajedno s obvezujućim i provedivim obvezama voditelja obrade ili izvršitelja obrade u trećoj zemlji za primjenu odgovarajućih zaštitnih mjera, između ostalog u pogledu prava ispitanika.

3. Pod uvjetom da to odobri nadležno nadzorno tijelo, odgovarajuće zaštitne mjere iz stavka 1. konkretno mogu pružiti i:

(a) ugovorne klauzule između voditelja obrade ili izvršitelja obrade i voditelja obrade, izvršitelja obrade ili primatelja osobnih podataka u trećoj zemlji ili međunarodnoj organizaciji; ili

(b) odredbe koje treba unijeti u administrativne dogovore između tijela javne vlasti ili javnih tijela i koja sadrže provediva i djelotvorna prava ispitanika.”

15 Članak 49. te uredbe, naslovljen „Odstupanja za posebne situacije”, glasi:

„1. Ako ne postoji odluka o primjerenosti u skladu s člankom 45. stavkom 3., ili odgovarajuće zaštitne mjere u skladu s člankom 46., što uključuje obvezujuća korporativna pravila, prijenos ili skup prijenosa osobnih podataka u treću zemlju ili međunarodnu organizaciju ostvaruje se samo pod jednim od sljedećih uvjeta:

(a) ispitanik je izričito pristao na predloženi prijenos nakon što je bio obaviješten o mogućim rizicima takvih prijenosa za ispitanika zbog nepostojanja odluke o primjerenosti i odgovarajućih zaštitnih mjera;

(b) prijenos je nužan za izvršavanje ugovora između ispitanika i voditelja obrade ili provedbu predugovornih mjera na zahtjev ispitanika;

(c) prijenos je nužan radi sklapanja ili izvršavanja ugovora sklopljenog u interesu ispitanika između voditelja obrade i druge fizičke ili pravne osobe;

(d) prijenos je nužan iz važnih razloga od javnog interesa;

(e) prijenos je nužan za postavljanje, ostvarivanje ili obranu pravnih zahtjeva;

(f) prijenos je nužan za zaštitu životno važnih interesa ispitanika ili drugih osoba ako ispitanik fizički ili pravno nije u stanju dati privolu;

(g) prijenos se obavlja iz registra koji prema pravu Unije ili pravu države članice služi pružanju informacija javnosti i koji je otvoren na uvid javnosti ili bilo kojoj osobi koja može dokazati neki opravdani interes, ali samo u mjeri u kojoj su ispunjeni uvjeti propisani u pravu Unije ili pravu države članice za uvid u tom posebnom slučaju.

Kad se prijenos ne može temeljiti na nekoj odredbi iz članka 45. ili 46., uključujući odredbe obvezujućih korporativnih pravila, i kad nije primjenjivo nijedno odstupanje za posebne situacije iz prvog podstavka ovog stavka, prijenos u treću zemlju ili međunarodnu organizaciju može se ostvariti samo ako se prijenos ne ponavlja, ako se odnosi samo na ograničen broj ispitanika, nužan je za potrebe uvjerljivih, legitimnih interesa voditelja obrade koji nisu podređeni interesima ili pravima i slobodama ispitanika, a voditelj obrade procijenio je sve okolnosti prijenosa podataka te je na temelju te procjene predvidio odgovarajuće zaštitne mjere u pogledu zaštite osobnih podataka. Voditelj obrade obavješćuje nadzorno tijelo o tom prijenosu. Uz pružanje informacija iz članaka 13. i 14., voditelj obrade ispitanika obavješćuje o prijenosu i o uvjerljivim legitimnim interesima.

2. Prijenos na temelju prvog podstavka stavka 1. točke (g) ne uključuje osobne podatke u cjelini ni cijele kategorije osobnih podataka sadržanih u registru. Kada je registar namijenjen uvidu osoba koje imaju legitimni interes, prijenos se obavlja samo na zahtjev tih osoba ili ako su one primatelji.

3. Stavak 1. prvi podstavak točke (a), (b) i (c) i stavak 1. drugi podstavak ne primjenjuju se na aktivnosti koje provode tijela javne vlasti izvršavajući svoje javne ovlasti.

4. Javni interes iz prvog podstavka stavka 1. točke (d) mora biti priznat u pravu Unije ili u pravu države članice kojem podliježe voditelj obrade.

5. Ako nije donesena odluka o primjerenosti, pravo Unije ili pravo države članice mogu, iz važnih razloga javnog interesa, izričito odrediti ograničenja prijenosa određenih kategorija osobnih podataka trećoj zemlji ili međunarodnoj organizaciji. Države članice dužne su obavijestiti Komisiju o takvim odredbama.

6. Voditelj obrade ili izvršitelj obrade dokumentiraju procjenu kao i odgovarajuće mjere zaštite iz stavka 1. drugog podstavka ovog članka u evidencijama iz članka 30.”

16 U članku 51. stavku 1. GDPR-a:

„Svaka država članica osigurava da je jedno ili više neovisnih tijela javne vlasti odgovorno za praćenje primjene ove Uredbe kako bi se zaštitila temeljna prava i slobode pojedinaca u pogledu obrade i olakšao slobodan protok osobnih podataka unutar Unije (‚nadzorno tijelo’).”

17 U skladu s člankom 55. stavkom 1. te uredbe, „[s]vako nadzorno tijelo nadležno je za obavljanje zadaća koje su mu povjerene i izvršavanje ovlasti koje su mu dodijeljene u skladu s ovom Uredbom na državnom području vlastite države članice”.

18 Člankom 57. stavkom 1. navedene uredbe predviđa se:

„Ne dovodeći u pitanje ostale zadaće utvrđene u ovoj Uredbi, svako nadzorno tijelo na svom području:

(a) prati i provodi primjenu ove Uredbe;

[…]

(f) rješava pritužbe koje podnose ispitanik […], istražuje u odgovarajućoj mjeri predmet pritužbe te podnositelja pritužbe u razumnom roku izvješćuje o napretku i ishodu istrage, posebno ako je potrebna daljnja istraga ili koordinacija s drugim nadzornim tijelom;

[…]”

19 U skladu s člankom 58. stavcima 2. i 4. iste uredbe:

„2. Svako nadzorno tijelo ima sve sljedeće korektivne ovlasti:

[…]

(f) privremeno ili konačno ograničiti, čak i zabraniti obradu;

[…]

(j) narediti suspenziju protoka podataka primatelju u trećoj zemlji ili međunarodnoj organizaciji.

[…]

4. Izvršavanje ovlasti dodijeljenih nadzornom tijelu u skladu s ovim člankom podliježe odgovarajućim zaštitnim mjerama, među ostalim djelotvornom pravnom lijeku i odgovarajućem postupku utvrđenim u pravu Unije i pravu države članice u skladu s Poveljom.”

20 Članak 64. stavak 2. GDPR-a glasi:

„Svako nadzorno tijelo, predsjednik [Europskog odbora za zaštitu podataka (EOZP)] ili Komisija mogu zatražiti da svaki predmet opće primjene ili s učincima u više od jedne države članice pregleda Odbor kako bi on dao mišljenje, posebno ako nadležno nadzorno tijelo ne poštuje obveze o uzajamnoj pomoći u skladu s člankom 61. ili o zajedničkim operacijama u skladu s člankom 62.”

21 U skladu s člankom 65. stavkom 1. te uredbe:

„Kako bi se osigurala ispravna i dosljedna primjena ove Uredbe u pojedinačnim slučajevima, Odbor donosi obvezujuću odluku u sljedećim slučajevima:

[…]

(c) ako nadležno nadzorno tijelo ne zatraži mišljenje Odbora u slučaju navedenom u članku 64. stavku 1. ili ne uzme u obzir mišljenje Odbora dano u skladu s člankom 64. U tom slučaju svako predmetno nadzorno tijelo ili Komisija mogu o predmetu obavijestiti Odbor.”

22 Članak 77. navedene uredbe, naslovljen „Pravo na pritužbu nadzornom tijelu” glasi:

„1. Ne dovodeći u pitanje druga upravna ili sudska pravna sredstva, svaki ispitanik ima pravo podnijeti pritužbu nadzornom tijelu, osobito u državi članici u kojoj ima uobičajeno boravište, u kojoj je njegovo radno mjesto ili mjesto navodnog kršenja, ako ispitanik smatra da obrada osobnih podataka koja se odnosi na njega krši ovu Uredbu.

2. Nadzorno tijelo kojem je podnesena pritužba obavješćuje podnositelja pritužbe o napretku i ishodu pritužbe, uključujući mogućnost [podnošenja] pravn[og] lijek[a] na temelju članka 78.”

23 Članak 78. te uredbe, naslovljen „Pravo na učinkoviti pravni lijek protiv nadzornog tijela” u stavcima 1. i 2. predviđa:

„1. Ne dovodeći u pitanje nijedan drugi upravni ili izvansudski pravni lijek, svaka fizička ili pravna osoba ima pravo na učinkoviti pravni lijek protiv pravno obvezujuće odluke nekog nadzornog tijela koja se na nju odnosi.

2. Ne dovodeći u pitanje nijedan drugi upravni ili izvansudski pravni lijek svaki ispitanik ima pravo na učinkoviti pravni lijek ako nadzorno tijelo nadležno na temelju članaka 55. i 56. ne riješi pritužbu ili ne izvijesti ispitanika u roku od tri mjeseca o napretku ili ishodu pritužbe podnesene na temelju članka 77.”

24 Člankom 94. GDPR-a određuje se:

„1. Direktiva [95/46] stavlja se izvan snage s učinkom od 25. svibnja 2018.

2. Upućivanja na direktivu stavljenu izvan snage smatraju se upućivanjima na ovu Uredbu. Upućivanja na Radnu skupinu o zaštiti pojedinaca s obzirom na obradu osobnih podataka osnovanu člankom 29. Direktive [95/46] tumače se kao upućivanja na Europski odbor za zaštitu podataka osnovan ovom Uredbom.”

25 U skladu s člankom 99. te uredbe:

„1. Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

2. Primjenjuje se od 25. svibnja 2018.”

Odluka o standardnim ugovornim klauzulama

26 Uvodna izjava 11. Odluke o standardnim ugovornim klauzulama glasi kako slijedi:

„Nadzorna tijela država članica igraju ključnu ulogu u ovom ugovornom mehanizmu osiguravajući da su tijekom prijenosa osobni podaci odgovarajuće zaštićeni. U iznimnim slučajevima kada izvoznici podataka odbiju ili nisu u stanju dati odgovarajuće upute uvozniku podataka, te kada postoji neizbježna opasnost od nanošenja teške štete osobama na koje se odnose podaci, standardne ugovorne klauzule trebaju omogućiti nadzornim tijelima reviziju uvoznika podataka i podobrađivača te, gdje je to prikladno, don[ošenje] odluk[a] koje obvezuju uvoznike podataka i podobrađivače. Nadzorna tijela trebaju imati moć da zabrane ili obustave prijenos podataka ili skup prijenosa na temelju standardnih ugovornih klauzula u takvim iznimnim slučajevima u kojima se ustanovi da je vjerojatno da prijenos na ugovornoj osnovi ima značajan nepovoljni učinak na jamstva i obveze koji osiguravaju odgovarajuću zaštitu korisnika.”

27 Članak 1. te odluke određuje:

„Standardne ugovorne klauzule utvrđene u Prilogu pružaju odgovarajuće zaštitne mjere u smislu zaštite privatnosti i temeljnih prava i sloboda pojedinaca u pogledu izvršavanja odgovarajućih prava kako zahtijeva članak 26. stavak 2. Direktive [95/46].”

28 U skladu s člankom 2. drugim stavkom navedene odluke, ona se „primjenjuje na prijenos osobnih podataka od strane nadzornika s poslovnim nastanom u Europskoj uniji primateljima s poslovnim nastanom izvan teritorija Europske unije koji djeluju samo kao obrađivači”.

29 Članak 3. te odluke određuje:

„Za potrebe ove Odluke primjenjuju se sljedeće definicije:

[…]

(c) ‚izvoznik podataka’ znači nadzornik koji obavlja prijenos osobnih podataka;

(d) ‚uvoznik podataka’ znači obrađivač s poslovnim nastanom u trećoj zemlji koji je od izvoznika podataka suglasan primiti osobne podatke radi njihove obrade u korist izvoznika podataka po prijenosu, u skladu s njegovim uputama i uvjetima ove Odluke, i koji nije podložan sustavu treće zemlje koji osigurava odgovarajuću zaštitu u smislu članka 25. stavka 1. Direktive [95/46];

[…]

(f) ‚pravo koje se primjenjuje na zaštitu podataka’ znači zakonodavstvo, koje štiti temeljna prava i slobode pojedinaca i posebno njihovo pravo na privatnost u pogledu obrade osobnih podataka, koje primjenjuje nadzornik podataka u državi članici u kojoj izvoznik podataka ima poslovni nastan;

[…]”

30 U svojoj prvotnoj verziji, koja je prethodila stupanju na snagu Provedbene odluke 2016/2297, članak 4. Odluke 2010/87 predviđao je:

„1. Ne dovodeći u pitanje svoje ovlasti da poduzimaju mjere za osiguranje usklađenosti s nacionalnim odredbama usvojenima u skladu s poglavljima II., III., V. i VI. Direktive [95/46], nadležna tijela država članica mogu koristiti svoje postojeće ovlasti da zabrane ili obustave protok podataka u treće zemlje kako bi zaštitile pojedince s obzirom na obradu njihovih osobnih podataka u slučajevima gdje:

(a) je utvrđeno da pravo, kojem je uvoznik podataka ili podobrađivač podložan, njemu nameće zahtjeve koji odstupaju od prava koje se primjenjuje na zaštitu podataka, koji nadilaze ograničenja nužna u demokratskom društvu u skladu s člankom 13. [Direktive 95/46] gdje bi ti zahtjevi mogli imati bitne neželjene posljedice na jamstva utvrđena pravom koje se primjenjuje na zaštitu podataka i standardnim ugovornim klauzulama;

(b) je nadležno tijelo utvrdilo da uvoznik podataka ili podobrađivač nisu poštovali standardne ugovorne klauzule u Prilogu; ili

(c) postoji stvarna vjerojatnost da se standardne ugovorne klauzule u Prilogu nisu ili neće poštovati i da bi daljnji prijenos prouzročio neposrednu opasnost od nanošenja teške štete osobama na koje se odnose podaci.

2. Zabrana ili suspenzija prema stavku 1. se ukida čim prestanu postojati razlozi za suspenziju ili zabranu.

3. Kada države članice usvoje mjere prema stavcima 1. i 2. bez odgode obavijestit će Komisiju koja će proslijediti informacije drugim državama članicama."

31 Uvodna izjava 5. Provedbene odluke 2016/2297, donesene nakon objave presude od 6. listopada 2015., Schrems (C-362/14, EU:C:2015:650), glasi:

„*Mutatis mutandis*, Odluka Komisije donesena u skladu s člankom 26. stavkom 4. Direktive [95/46] obvezujuća je za sva tijela država članica kojima je upućena, uključujući njihova neovisna nadzorna tijela, jer se njome priznaje da se prijenosima koji se provode na temelju standardnih ugovornih klauzula utvrđenih u Direktivi pružaju dovoljna jamstva kao što je propisano člankom 26. stavkom 2. te Direktive. To ne sprječava nacionalno nadzorno tijelo da izvršava svoje ovlasti nadzora tokova podataka, uključujući ovlasti obustave ili zabrane prijenosa osobnih podataka ako utvrdi da se tim prijenosom krši zakon o zaštiti podataka u EU-u ili pojedinačnoj državi članici, primjerice, ako uvoznik podataka ne poštuje standardne ugovorne klauzule."

32 U svojoj trenutačnoj verziji, proizašloj iz Provedbene odluke 2016/2297, članak 4. Odluke o standardnim ugovornim klauzulama određuje:

„Kad god nadležna tijela država članica izvršavaju svoje ovlasti u skladu s člankom 28. stavkom 3. Direktive [95/46] a čiji je ishod suspenzija ili potpuna zabrana protoka podataka prema trećim zemljama radi zaštite osoba u pogledu obrade njihovih osobnih podataka, predmetna država članica bez odgode o tome obavješćuje Komisiju koja informacije prosljeđuje drugim državama članicama."

33 Prilog Odluci o standardnim ugovornim klauzulama, nazvan „Standardne ugovorne klauzule (obrađivači)", sadržava dvanaest standardnih klauzula. Klauzula 3. tog priloga, naslovljena „Klauzula u korist treće strane", predviđa:

„1. Subjekt podataka može protiv izvoznika podataka upotrijebiti ovu klauzulu i klauzulu 4. točke (b) do (i), klauzulu 5. točke (a) do (e) i (g) do (j), klauzulu 6. stavke 1. i 2., klauzulu 7., klauzulu 8. stavak 2. i klauzule 9. do 12. u korist treće stranke.

2. Subjekt podataka može protiv uvoznika podataka upotrijebiti ovu klauzulu, klauzulu 5. točke (a) do (e) i (g), klauzulu 6., klauzulu 7., klauzulu 8. stavak 2. i klauzule 9. do 12. u slučaju kada izvoznik podataka prestane postojati ili prestane postojati pred zakonom, osim ako bilo koji pravni nasljednik ne preuzme sve zakonske obveze izvoznika podataka prema ugovoru ili zakonu; u tom slučaju [taj pravni nasljednik] preuzima prava i obveze izvoznika podataka te [subjekt podataka] može upotrijebiti [navedene klauzule] protiv pravnih nasljednika.

[…]"

34 U skladu s klauzulom 4. tog priloga, naslovljenom „Obveze izvoznika podataka":

„Izvoznik podataka suglasan je i jamči:

(a) da se obrada osobnih podataka, uključujući i sam prijenos podataka, obavljala i da će se obavljati u skladu s odgovarajućim odredbama prava primjenjivog na zaštitu podataka (te da su, prema potrebi, o tome obaviještena odgovarajuća nadležna tijela država članica u kojima izvoznik podataka ima poslovni nastan) i da neće kršiti odgovarajuće odredbe te države;

(b) da je dao upute i da će davati upute uvozniku podataka tijekom trajanja usluga obrade osobnih podataka kako bi [potonji] obradio osobne podatke koji su preneseni jedino u korist izvoznika podataka i u skladu s odgovarajućim odredbama prava primjenjivog na zaštitu podataka i klauzulama;

[…]

(f) da je u slučaju kada prijenos uključuje posebne kategorije podataka, obavijestio subjekta podataka ili će ga unaprijed obavijestiti ili netom poslije prijenosa [da] bi podaci mogli biti preneseni u treću zemlju bez odgovarajuće zaštite u skladu s [Direktivom 95/46];

(g) da će u skladu s klauzulom 5. točkom (b) i klauzulom 8. stavkom 3. proslijediti svaku obavijest zaprimljenu od uvoznika podataka ili podobrađivača nadzornim tijelima za zaštitu podataka ako izvoznik podataka odluči nastaviti s prijenosom ili ukinuti suspenziju;

[…]”

35 Klauzula 5. navedenog priloga, naslovljena „Obveze uvoznika podataka […]”, propisuje:

„Uvoznik podataka suglasan je i jamči:

(a) obradu osobnih podatke jedino u korist izvoznika podataka i u skladu s njegovim uputama i klauzulama; ako to iz bilo kojih razloga ne može osigurati, suglasan je da o tome odmah obavijesti izvoznika podataka, te u tom slučaju izvoznik podataka ima pravo obustaviti prijenos podataka i/ili prekinuti ugovor;

(b) da nema razloga za vjerovanje da ga zakonodavstvo koje se na njega primjenjuje onemogućava u ispunjavanju uputa primljenih od izvoznika podataka i njegovih obveza prema ugovoru te da će u slučaju promjene u zakonodavstvu koja bi mogla imati bitan negativan učinak na jamstva i obveze iz klauzula, o promjeni odmah obavijestiti izvoznika podataka čim toga postane svjestan, te u tom slučaju izvoznik podataka ima pravo obustaviti prijenos podataka i/ili prekinuti ugovor;

[…]

(d) da će odmah obavijestiti izvoznika podataka o:
   i. svakom pravno obvezujućem zahtjevu od strane tijela kaznenog progona za otkrivanje osobnih podataka osim ako drukčije nije zabranjeno poput zabrane prema kaznenom pravu radi očuvanja povjerljivosti kaznene istrage;
   ii. svakom slučajnom ili neovlaštenom pristupu; i
   iii. svakom zahtjevu primljenom izravno od osoba čiji se podaci obrađuju bez odgovaranja na taj zahtjev osim ako za to nije ovlašten;

[…]”

36 U skladu s bilješkom na koju upućuje naslov klauzule 5.:

„Obvezni zahtjevi nacionalnog zakonodavstva primjenjivi na uvoznika podataka koji ne nadilaze neophodno u demokratskom društvu na temelju jednog od interesa navedenog u članku 13. stavku 1. Direktive 95/46/EZ, to jest, ako oni predstavljaju nužnu mjeru za očuvanje nacionalne sigurnosti, obrane, javne sigurnosti, prevencije, istrage, otkrivanja i progona kaznenih djela ili kršenje etike za zakonski zaštićena zanimanja, važan ekonomski ili financijski interes države ili zaštitu osoba na koje se odnose podaci ili prava i slobode drugih, a nisu protivni standardnim ugovornim klauzulama. […]”

37 Klauzula 6. Priloga Odluci o standardnim ugovornim klauzulama, naslovljena „Odgovornost”, predviđa:

„1. Stranke su suglasne da svaki subjekt podataka koji trpi štetu kao posljedicu svakog kršenja obveza navedenih u klauzuli 3. i klauzuli 11. od strane bilo koje stranke ili podobrađivača, ima pravo od izvoznika podataka primiti naknadu štete.

2. Ako subjekt podataka […] ne može podnijeti zahtjev za naknadu štete protiv izvoznika podataka u skladu sa stavkom 1. […] radi kršenja obveza navedenih u klauzuli 3. i klauzuli 11. od strane uvoznika podataka ili njegovog podobrađivača zbog toga što je izvoznik podataka prestao postojati ili prestao postojati pred zakonom ili postao nelikvidan, uvoznik podataka suglasan je da subjekt podataka može podnijeti zahtjev protiv uvoznika podataka umjesto izvoznika podataka […].

[…]”

38 Klauzula 8. tog priloga, naslovljena „Suradnja s nadležnim tijelima”, u stavku 2. određuje:

„Stranke su suglasne da nadležna tijela imaju pravo izvršiti reviziju uvoznika podataka i bilo kojeg podobrađivača koja ima jednako područje primjene i podložna je istim uvjetima koji se primjenjuju na reviziju izvoznika podataka sukladno pravu o zaštiti podataka koje se primjenjuje.”

39 Klauzula 9. navedenog priloga, naslovljena „Mjerodavno pravo”, određuje da se klauzule ravnaju pravom države članice u kojoj izvoznik podataka ima poslovni nastan.

40 U skladu s klauzulom 11. navedenog priloga, naslovljenom „Podobrada”:

„1. Uvoznik podataka bez prethodnog pisanog odobrenja izvoznika podataka neće napraviti ugovor o kooperaciji niti za jedan od svojih postupaka obrade [izvršenih] u korist izvoznika podataka sukladno klauzulama. Kada uvoznik podataka, uz pristanak izvoznika podataka, napravi ugovor o kooperaciji sukladno klauzulama, [taj ugovor s podobrađivačem mora sklopiti u pisanom obliku te on podobrađivaču nameće obveze istovjetne onima] koje ima uvoznik podataka sukladno klauzulama. […]

2. Prethodni pisani ugovor između uvoznika podataka i podobrađivača također sadrži klauzulu u korist treće stranke, kako je utvrđeno u klauzuli 3., za slučajeve u kojima osobe čiji se podaci obrađuju ne mogu tražiti zahtjev za nadoknadu štete iz članka 1. klauzule 6. protiv izvoznika podataka ili uvoznika podataka jer su prestali postojati ili prestali postojati pred zakonom ili postali nelikvidni te ni jedan pravni nasljednik nije preuzeo sve zakonske obveze izvoznika ili uvoznika podataka prema ugovoru ili po zakonu. Takva odgovornost podobrađivača ograničena je na njegove vlastite postupke obrade sukladno klauzulama.

[…]”

41 Stavak 1. klauzule 12. priloga Odluci o standardnim ugovornim klauzulama, naslovljene „Obveze nakon prestanka obavljanja djelatnosti obrade osobnih podataka”, glasi:

„Stranke su suglasne da uvoznik podataka i podobrađivač nakon prestanka obavljanja djelatnosti obrade osobnih podataka, po izboru izvoznika podataka, vrate sve prenesene osobne podatke i kopije u tu svrhu izvozniku podataka ili unište sve osobne podatke i jamči izvozniku podataka o tome osim ako zakonodavstvo važeće za uvoznika podataka ne sprečava da vrati ili uništi sve ili dio prenesenih osobnih podataka. […]”

Odluka o sustavu zaštite privatnosti

42 Presudom od 6. listopada 2015., Schrems (C-362/14, EU:C:2015:650), Sud je poništio Odluku Komisije 2000/520/EZ od 26. srpnja 2000., u skladu s Direktivom 95/46 o primjerenosti zaštite koju pružaju načela privatnosti „sigurne luke" i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a (SL 2000., L 215, str. 7.), u kojoj je Komisija utvrdila da ta treća zemlja osigurava primjerenu razinu zaštite.

43 Nakon objave te presude Komisija je donijela Odluku o sustavu zaštite privatnosti nakon što je, u svrhu njezina donošenja, izvršila ocjenu zakonodavstva SAD-a, kao što je navedeno u uvodnoj izjavi 65. navedene odluke:

„Komisija je procijenila ograničenja i zaštitne mjere dostupne u američkom pravu u vezi s pristupom američkih javnih tijela osobnim podacima prenesenima u okviru europsko-američkog sustava zaštite privatnosti i upotrebom tih podataka u svrhu nacionalne sigurnosti, kaznenog progona i drugih javnih interesa. Nadalje, američka vlada je posredstvom svog Ureda direktora nacionalne obavještajne službe (Office of the Director of National Intelligence, ODNI) […] Komisiji dostavila detaljne izjave i obveze koje se nalaze u Prilogu VI. ovoj Odluci. Dopisom koji je potpisao ministar vanjskih poslova (Secretary of State) (Prilog III. ovoj Odluci) američka vlada obvezala se uvesti novi mehanizam za nadzor povreda nacionalne sigurnosti, naime Pravobranitelja za sustav zaštite privatnosti, koji je neovisan o obavještajnoj zajednici. Naposljetku, u izjavi američkog Ministarstva pravosuđa, koja se nalazi u Prilogu VII. ovoj Odluci, opisana su ograničenja i zaštitne mjere koji se primjenjuju na pristup javnih tijela podacima i na njihovu upotrebu tih podataka u svrhu kaznenog progona i u druge svrhe od javnog interesa. Kako bi se povećala transparentnost i pokazala pravna priroda tih obveza, svi dokumenti popisani i priloženi ovoj Odluci objavljuju se u saveznom registru SAD-a."

44 Komisijina analiza tih ograničenja i jamstava sažeta je u uvodnim izjavama 67. do 135. Odluke o sustavu zaštite privatnosti, dok se zaključci te institucije o primjerenoj razini zaštite u okviru europsko-američkog sustava zaštite podataka nalaze u njezinim uvodnim izjavama 136. do 141.

45 Konkretno, uvodne izjave 68., 69., 76., 77., 109., 112. do 116., 120., 136. i 140. te odluke glase:

„68. U skladu s američkim Ustavom za osiguranje nacionalne sigurnosti nadležan je Predsjednik kao glavni zapovjednik i glavni predstavnik izvršne vlasti, kao i za američke vanjske poslove u pogledu stranih obavještajnih podataka […] Iako Kongres ima ovlasti određivati ograničenja i to je u mnogo pogleda i činio, unutar tih granica Predsjednik može usmjeravati rad američke obavještajne zajednice, posebno izvršnim nalozima ili predsjedničkim ukazima. […] Trenutačno su dva najvažnija pravna instrumenta u tom pogledu Izvršni nalog br. 12333 (Executive Order 12333) […] i Predsjednički ukaz br. 28 (Presidential Policy Directive 28).

69. Predsjedničkim ukazom br. 28 (dalje u tekstu: PPD-28), koji je objavljen 17. siječnja 2014., određuje se niz ograničenja za operacije ‚prikupljanja informacija elektroničkim izviđanjem' […]. Taj predsjednički ukaz obvezujuć je za američka obavještajna tijela […] i ostaje na snazi i nakon promjene vlade SAD-a […] PPD-28 od posebne je važnosti za osobe koje nisu državljani SAD-a, među ostalim za osobe iz EU-a čiji se podaci obrađuju. […]

[…]

76. Iako nisu oblikovana u takvom pravnom obliku, tim je načelima [PPD-28] obuhvaćena bit načela nužnosti i proporcionalnosti. […]

77. Budući da je riječ o ukazu Predsjednika kao glavnog predstavnika izvršne vlasti, tim se zahtjevima obvezuje cijela obavještajna zajednica te se oni dalje provode s pomoću pravila agencije i postupaka kojima se opća načela prenose u posebne upute za svakodnevni rad. […]

[…]

109. S druge strane, u skladu s člankom 702. [Foreign Intelligence Surveillance Act (FISA)], [United States Foreign Intelligence Surveillance Court (FISC) (Sud za nadzor stranih obavještajnih informacija, SAD9] ne odobrava pojedinačne mjere nadzora, već odobrava programe nadzora (npr. PRISM, UPSTREAM) na temelju godišnjih certifikacija koje pripremaju Glavni državni odvjetnik [United States Attorney General] i direktor Nacionalne obavještajne službe [Director of National Intelligence (DNI)]. […] Kako je navedeno, certifikacije koje će odobriti FISC ne sadržavaju informacije o pojedinim osobama čiji će se podaci ciljano prikupljati već se u njima navode kategorije stranih obavještajnih informacija […]. Iako FISC ne procjenjuje – zbog opravdane sumnje ili na nekoj drugoj osnovi – jesu li osobe čiji se podaci prikupljaju radi pribavljanja stranih obavještajnih podataka ispravno odabrane […], on provodi kontrolu pod uvjetom da je ‚važna svrha prikupljanja pribaviti strane obavještajne informacije'. […]

[…]

112. Prvo, u Zakonu o nadzoru stranih obavještajnih službi predviđen je niz mehanizama pravne zaštite koji su dostupni i osobama koje nisu američki državljani za osporavanje nezakonitog elektroničkog nadzora […]. To uključuje mogućnost pojedinaca da pokrenu građanski postupak za naknadu štete protiv Sjedinjenih Američkih Država ako su se informacije o njima nezakonito i samovoljno upotrebljavale ili otkrivale […]; da osobno tuže američke državne službenike (zbog prekoračenja ovlasti, ‚under color of law') tražeći novčanu odštetu […] i da ospore zakonitost nadzora (i traže uklanjanje informacija) ako američka vlada planira upotrijebiti ili otkriti prikupljene informacije ili podatke dobivene elektroničkim nadzorom osobe u sudskim ili upravnim postupcima u SAD-u […].

113. Drugo, američka vlada obavijestila je Komisiju o nizu dodatnih sredstava koje osobe iz EU-a čiji se podaci obrađuju mogu upotrijebiti za traženje pravne zaštite od državnih službenika zbog nezakonitog pristupa osobnim podacima ili njihove upotrebe, uključujući u svrhu navodne nacionalne sigurnosti […].

114. Naposljetku, američka vlada spominje [Freedom of information Act (FOIA) (Zakon o pravu na pristup informacijama)] kao sredstvo kojim osobe koje nisu američki državljani mogu tražiti pristup postojećoj evidenciji savezne agencije, uključujući i onoj koja sadržava njihove osobne podatke […]. S obzirom na svoju usmjerenost FOIA pojedincima ne osigurava pravnu zaštitu od neovlaštene upotrebe njihovih osobnih podataka, ali bi im u načelu mogla omogućiti pristup relevantnim podacima koje čuvaju nacionalne obavještajne agencije. […]

115. Iako prema tome pojedinci, uključujući osobe iz EU-a čiji se podaci obrađuju, imaju na raspolaganju različite oblike pravne zaštite ako su bili predmetom nezakonitog (elektroničkog) nadzora za potrebe nacionalne sigurnosti, očito je i da nisu obuhvaćene barem neke pravne osnove koje američka obavještajna tijela (npr. Izvršni nalog br. 12333) mogu upotrijebiti. Nadalje, čak i ako osobe koje nisu američki državljani u načelu imaju na raspolaganju mogućnosti sudske zaštite, kao u slučaju nadzora u skladu s FISA-om, dostupne pravne osnove ograničene su […] i tužbe koje podnose pojedinci (uključujući američke državljane) proglasit će se neprihvatljivima ako se ne može dokazati ‚osnovanost' […], kojom se ograničava pristup redovnim sudovima […].

116. Kako bi osigurala dodatni oblik pravne zaštite dostupan svim osobama iz EU-a čiji se podaci obrađuju, američka vlada odlučila je uspostaviti novi mehanizam u vidu pravobranitelja, kako je navedeno u dopisu američkog ministra vanjskih poslova Komisiji, koji se nalazi u Prilogu III. ovoj Odluci. Taj se mehanizam temelji na imenovanju, u okviru Predsjedničkog ukaza br. 28, višeg

koordinatora (na razini zamjenika ministra) u Ministarstvu vanjskih poslova kao kontaktne točke za strane vlade koji će postavljati pitanja u vezi s američkim obavještajnim aktivnostima prikupljanja informacija elektroničkim izviđanjem, ali on uvelike nadilazi taj prvobitni koncept.

[…]

120. [V]lada SAD-a obvezuje se osigurati da će se Pravobranitelj za sustav zaštite privatnosti u obavljanju svojih dužnosti moći osloniti na suradnju s drugim nadzornim mehanizmima i mehanizmima za preispitivanje usklađenosti koji postoje u pravu SAD-a. […] Ako neko od tih nadzornih tijela utvrdi neusklađenost, predmetni subjekt obavještajne zajednice (npr. obavještajna agencija) morat će ispraviti neusklađenost jer će Pravobranitelj tek tada moći dati ‚pozitivan' odgovor pojedincu (tj. da je svaka neusklađenost uklonjena) na koji se obvezala američka vlada. […]

[…]

136. S obzirom na te zaključke Komisija smatra da Sjedinjene Američke Države osiguravaju odgovarajuću razinu zaštite osobnih podataka koji se prenose iz Unije samocertificiranim organizacijama u SAD-u u okviru europsko-američkog sustava zaštite privatnosti.

[…]

140. Naposljetku, na temelju dostupnih informacija o pravnom poretku SAD-a, uključujući izjave i jamstva američke vlade, Komisija smatra da će svako zadiranje američkih javnih tijela u temeljna prava osoba čiji se podaci prenose iz Unije u Sjedinjene Američke Države u okviru europsko-američkog sustava zaštite privatnosti radi nacionalne sigurnosti, kaznenog progona ili drugih javnih interesa i povezana ograničenja koja se određuju samocertificiranim organizacijama u pogledu njihovog pridržavanja Načela biti ograničena na ono što je nužno za postizanje predmetnog legitimnog cilja te da postoji djelotvorna pravna zaštita od takvog zadiranja."

46 Članak 1. Odluke o sustavu zaštite privatnosti određuje:

„1. Za potrebe članka 25. stavka 2. Direktive [95/46] Sjedinjene Američke Države osiguravaju odgovarajuću razinu zaštite osobnih podataka koji se prenose iz Unije organizacijama u Sjedinjenim Američkim Državama u okviru europsko-američkog sustava zaštite privatnosti.

2. Europsko-američki sustav zaštite privatnosti uspostavljen je u skladu s Načelima koja je 7. srpnja 2016. izdalo američko Ministarstvo trgovine, kako je navedeno u Prilogu II. te u službenim izjavama i obvezama iz dokumenata navedenih u Prilogu I. i prilozima od III. do VII.

3. Za potrebe stavka 1. osobni se podaci u okviru europsko-američkog sustava zaštite privatnosti iz Unije prenose organizacijama u Sjedinjenim Američkim Državama koje se nalaze na ‚Popisu organizacija u sustavu zaštite privatnosti', koji vodi i objavljuje američko Ministarstvo trgovine u skladu s odjeljcima I. i III. Načela navedenih u Prilogu II."

47 Prilog II. Odluke o sustavu zaštite privatnosti, naslovljen „Načela okvira europsko-američkog sustava zaštite privatnosti koja je izdalo Ministarstvo trgovine SAD-a", u točki I.5 predviđa da pridržavanje tih načela može biti ograničeno, među ostalim, „u mjeri potrebnoj da se ispune zahtjevi u pogledu nacionalne sigurnosti, javnog interesa ili kaznenog progona."

48 Prilog III. toj odluci sadržava pismo Johna Kerryja, tadašnjeg Secretary of State (ministar vanjskih poslova, Sjedinjene Američke Države), povjerenici za pravosuđe, potrošačka prava i jednakost spolova, od 7. srpnja 2016., kojemu je priložen, u Prilogu A, memorandum naslovljen „Mehanizam pravobranitelja za europsko-američki sustav za zaštitu privatnosti u vezi prikupljanja obavještajnih podataka elektroničkim izviđanjem", koji sadržava sljedeći odjeljak:

„Kao priznanje važnosti okvira europsko-američkog sustava zaštite privatnosti, u ovom Memorandumu utvrđuje se postupak za provedbu ovog novog mehanizma u skladu s Predsjedničkim ukazom br. 28 (PPD-28) u vezi s prikupljanjem obavještajnih podataka elektroničkim izviđanjem.

[…] Predsjednik Obama najavio je donošenje novog predsjedničkog ukaza – PPD-28 – u kojem će ‚biti jasno propisano što smijemo, a što ne smijemo raditi, u slučaju prekomorskog nadzora'.

U odjeljku 4. točki (d) PPD-28 ministru vanjskih poslova određuje se zadaća da imenuje ‚Višeg koordinatora međunarodne diplomacije u području informacijske tehnologije' (Viši koordinator) ‚koji će … biti kontaktna točka […] u vezi s aktivnostima prikupljanja obavještajnih podataka elektroničkim izviđanjem koje obavljaju Sjedinjene Američke Države'.

[…]

1) Viši koordinator obavlja dužnost pravobranitelja za sustav zaštite privatnosti i […] blisko će surađivati s odgovarajućim dužnosnicima iz drugih odjela i agencija koji su odgovorni za obradu zahtjeva u skladu s primjenjivim američkim zakonodavstvom i politikom. Pravobranitelj djeluje neovisno od obavještajne zajednice. Pravobranitelj izravno izvješćuje ministra vanjskih poslova koji će pravobranitelju osigurati objektivno obavljanje dužnosti, neovisno od bilo kakvog neprimjerenog utjecaja koje bi moglo imati učinka na odgovor koji treba pružiti.

[…]".

49 Prilog VI. Odluke o sustavu zaštite privatnosti sadržava dopis Ureda direktora nacionalne obavještajne službe (Office of the Director of National Intelligence) američkom ministarstvu trgovine i Upravi za međunarodnu trgovinu od 21. lipnja 2016., u kojem je navedeno da PPD-28 omogućava „‚skupno' prikupljanje […] relativno velike količine elektronički prikupljenih obavještajnih informacija ili podataka u okolnostima u kojima se obavještajna zajednica ne može koristiti identifikatorom povezanim s određenom ciljanom osobom […]".

Glavni postupak i prethodna pitanja

50 M. Schrems austrijski je državljanin s boravištem u Austriji koji je od 2008. godine korisnik društvene mreže Facebook (u daljnjem tekstu: Facebook).

51 Svaka osoba s boravištem na području Unije koja se želi koristiti Facebookom dužna je prilikom registriranja sklopiti ugovor s Facebookom Ireland, društvom kćeri Facebooka Inc. koji ima sjedište u Sjedinjenim Američkim Državama. Osobni podaci korisnika Facebooka koji borave na državnom području Unije prenose se u cijelosti ili djelomično na poslužitelje koji pripadaju društvu Facebook Inc. i koji su smješteni na državnom području Sjedinjenih Američkih Država, gdje su ti podaci predmet obrade.

52 M. Schrems je 25. lipnja 2013. povjereniku uputio pritužbu kojom je u biti od njega zatražio da zabrani Facebooku Ireland da prenosi njegove osobne podatke u Sjedinjene Američke Države, navevši da važeće pravo i praksa u toj zemlji ne jamče dovoljnu razinu zaštite osobnih podataka pohranjenih na

njezinu državnom području od nadzornih aktivnosti koje tamo provode javna tijela. Ta pritužba je odbijena među ostalim zbog toga što je Komisija u svojoj Odluci 2000/520 utvrdila da Sjedinjene Američke Države osiguravaju primjerenu razinu zaštite.

53 High Court (Visoki sud, Irska), kojem je M. Schrems podnio tužbu protiv odluke o odbijanju njegove pritužbe, uputio je Sudu zahtjev za prethodnu odluku u vezi s tumačenjem i valjanošću Odluke 2000/520. Presudom od 6. listopada 2015., Schrems (C-362/14, EU:C:2015:650), Sud je tu odluku proglasio nevaljanom.

54 Nakon te presude sud koji je uputio zahtjev poništio je odluku o odbijanju pritužbe M. Schremsa i vratio je povjereniku na ponovno ispitivanje. U okviru istrage koju je potonji pokrenuo Facebook Ireland objasnio je da je velik dio osobnih podataka bio prenesen društvu Facebook Inc. na temelju standardnih klauzula o zaštiti priloženih Odluci o standardnim ugovornim klauzulama. S obzirom na te elemente, povjerenik je pozvao M. Schremsa da preformulira svoju pritužbu.

55 U svojoj tako preformuliranoj pritužbi, podnesenoj 1. prosinca 2015., M. Schrems tvrdio je, među ostalim, da američko pravo društvu Facebook Inc. nalaže da osobne podatke koji su mu preneseni stavi na raspolaganje američkim tijelima, kao što su National Security Agency (NSA) i Federal Bureau of Investigation (FBI). Naveo je da, budući da se ti podaci koriste u okviru različitih nadzornih programa na način koji nije u skladu s člancima 7., 8. i 47. Povelje, Odluka o standardnim ugovornim klauzulama ne može opravdati prijenos navedenih podataka u Sjedinjene Američke Države. U tim je okolnostima M. Schrems zatražio od povjerenika da zabrani ili obustavi prijenos njegovih osobnih podataka društvu Facebook Inc.

56 Povjerenik je 24. svibnja 2016. objavio „nacrt odluke” u kojoj su bili sažeti privremeni zaključci njegove istrage. U tom nacrtu odluke on je privremeno utvrdio da postoji opasnost da američka tijela pristupaju osobnim podacima građana Unije koji su preneseni u Sjedinjene Američke Države te ih obrađuju na način koji nije u skladu s člancima 7. i 8. Povelje i da pravo Sjedinjenih Američkih Država tim građanima ne nudi pravne lijekove u skladu s člankom 47. Povelje. Povjerenik je ocijenio da se standardnim klauzulama o zaštiti podataka koje se nalaze u prilogu Odluci o standardnim ugovornim klauzulama ne može riješiti taj nedostatak jer predmetnim osobama dodjeljuju samo ugovorna prava protiv uvoznika i izvoznika podataka a da pritom ne obvezuju američka tijela.

57 Smatrajući da je u tim okolnostima preformuliranom pritužbom M. Schremsa istaknuto pitanje valjanosti Odluke o standardnim ugovornim klauzulama, povjerenik je 31. svibnja 2016., oslanjajući se na sudsku praksu proizašlu iz presude od 6. listopada 2015., Schrems (C-362/14, EU:C:2015:650, t. 65.), pokrenuo postupak pred High Courtom (Visoki sud) kako bi potonji uputio Sudu zahtjev za prethodnu odluku o tom pitanju. Odlukom od 4. svibnja 2018. High Court (Visoki sud) uputio je Sudu ovaj zahtjev za prethodnu odluku.

58 High Court (Visoki sud) je tom zahtjevu za prethodnu odluku priložio presudu objavljenu 3. listopada 2017. u kojoj je iznio rezultate ocjene dokaza koji su mu podneseni u okviru nacionalnog postupka u kojoj je sudjelovala američka vlada.

59 U toj presudi, na koju zahtjev za prethodnu odluku upućuje nekoliko puta, sud koji je uputio zahtjev naveo je da on u načelu ima ne samo pravo već i obvezu razmatranja svih činjenica i argumenata koji su mu izloženi kako bi na temelju njih odlučio je li zahtjev za prethodnu odluku potreban ili ne. U svakom slučaju, dužan je uzeti u obzir eventualne izmjene prava do kojih je došlo u razdoblju između podnošenja tužbe i rasprave koja se pred njime održala. Taj sud pojasnio je da u okviru glavnog postupka njegova ocjena nije ograničena na razloge nevaljanosti koje je istaknuo povjerenik, tako da on može po službenoj dužnosti navesti i druge razloge nevaljanosti i na temelju njih uputiti zahtjev za prethodnu odluku.

60 U skladu s utvrđenjima koja se nalaze u navedenoj presudi, obavještajne aktivnosti američkih tijela u pogledu osobnih podataka prenesenih u Sjedinjene Američke Države temelje se, osobito, na članku 702. FISA-e i Izvršnom nalogu br. 12333.

61 Kad je riječ o članku 702. FISA-e, sud koji je uputio zahtjev u istoj presudi pojašnjava da taj članak državnom odvjetniku i direktoru Nacionalne obavještajne službe omogućuje da na temelju odobrenja FISC-a, u svrhu pribavljanja „stranih obavještajnih informacija", zajedno odobre nadzor osoba koje nisu američki građani koje se nalaze izvan državnog područja Sjedinjenih Američkih Država te služi, među ostalim, kao pravna osnova za programe nadzora PRISM i UPSTREAM. U okviru programa PRISM pružatelji internetskih usluga dužni su, u skladu s utvrđenjima tog suda, NSA-i podnijeti sve komunikacije koje šalje ili prima „čimbenik za odabir", pri čemu se dio tih komunikacija također prenosi FBI-u i Central Intelligence Agencyju (CIA) (Središnja obavještajna agencija).

62 Kad je riječ o programu UPSTREAM, navedeni sud utvrdio je da su u okviru tog programa telekomunikacijska društva koja koriste internetsku „kralježnicu", odnosno mrežu kablova, preklopnika i usmjerivača, obvezni NSA-i omogućiti kopiranje i filtriranje protoka internetskog prometa radi prikupljanja komunikacija koje šalje ili prima osoba koja nije američki državljanin na koju se odnosi „čimbenik za odabir" ili komunikacija koje su u vezi s tom osobom. Prema utvrđenjima tog suda, NSA u okviru navedenog programa ima pristup kako metapodacima tako i sadržaju predmetnih komunikacija.

63 Kad je riječ o Izvršnom nalogu br. 12333, sud koji je uputio zahtjev utvrđuje da se njime NSA-i dopušta pristup podacima koji su „u prijelazu" preko Sjedinjenih Američkih Država pristupanjem podmorskim kablovima koji se nalaze na dnu Atlantskog oceana, kao i prikupljanje i zadržavanje tih podataka prije nego što stignu u Sjedinjene Američke Države te tamo budu podvrgnuti odredbama FISA-e. Taj sud pojašnjava da aktivnosti koje se temelje na Izvršnom nalogu br. 12333 nisu uređene zakonom.

64 Kad je riječ o ograničavanju obavještajnih aktivnosti, sud koji je uputio zahtjev ističe da se na osobe koje nisu američki državljani odnosi isključivo PPD-28 te da je njegov jedini cilj da obavještajne aktivnosti budu „što usmjerenije" *(as tailored as feasible)*. Na temelju tih utvrđenja navedeni sud smatra da Sjedinjene Američke Države provode masovne obrade osobnih podataka a da pritom ne pružaju zaštitu koja je bitno ekvivalentna onoj zajamčenoj člancima 7. i 8. Povelje.

65 Kad je riječ o sudskoj zaštiti, taj isti sud navodi da građani Unije nemaju pristup istim pravnim lijekovima protiv obrada svojih osobnih podataka koje provode američka tijela kao američki državljani jer se četvrti amandman Constitution of the United States (Ustav Sjedinjenih Američkih Država), koji u američkom pravu čini najvažniju zaštitu protiv nezakonitog nadziranja, ne primjenjuje na građane Unije. U tom pogledu sud koji je uputio zahtjev pojašnjava da pravna sredstva koja su potonjima na raspolaganju nailaze na znatne prepreke, osobito na obvezu, koju taj sud smatra pretjerano teško ispunjivom, dokazivanja njihove aktivne procesne legitimacije. Nadalje, taj sud navodi da aktivnosti NSA-e koje se temelje na Izvršnom nalogu br. 12333 ne podliježu sudskom nadzoru niti se protiv njih može uložiti pravni lijek. Naposljetku, navedeni sud smatra da, s obzirom na to da, prema mišljenju tog suda, pravobranitelj za sustav zaštite podataka nije sud, u smislu članka 47. Povelje, američko pravo građanima Unije ne pruža razinu zaštite koja je bitno ekvivalentna onoj zajamčenoj temeljnim pravom iz tog članka.

66 U svojem zahtjevu za prethodnu odluku sud koji je uputio zahtjev nadalje pojašnjava da se stranke iz glavnog postupka spore, među ostalim, o pitanju primjenjivosti prava Unije na prijenose u treću zemlju osobnih podataka koje tijela te zemlje mogu obrađivati među ostalim za potrebe nacionalne sigurnosti te o elementima koje treba uzeti u obzir kako bi se ocijenila primjerena razina zaštite koju osigurava navedena zemlja. Konkretno, taj sud navodi da Facebook Ireland smatra da Komisijina utvrđenja koja se odnose na primjerenost razine zaštite koju osigurava treća zemlja, poput onih u

Odluci o sustavu zaštite privatnosti, obvezuju nadzorna tijela i u kontekstu prijenosa osobnih podataka koji se temelji na standardnim klauzulama o zaštiti podataka koje se nalaze u prilogu Odluci o standardnim ugovornim klauzulama.

67 Kad je riječ o tim standardnim klauzulama o zaštiti podataka, navedeni sud pita se može li se Odluka o standardnim ugovornim klauzulama smatrati valjanom, iako, prema mišljenju tog suda, navedene klauzule nisu obvezujuće za državna tijela dotične treće zemlje i stoga ne mogu nadomjestiti eventualno nepostojanje primjerene razine zaštite u toj zemlji. U tom pogledu smatra da mogućnost, koja je nadležnim tijelima država članica priznata člankom 4. stavkom 1. točkom (a) Odluke 2010/87, u njezinoj verziji koja prethodi stupanju na snagu Provedbene odluke 2016/2297, da zabrane prijenose osobnih podataka trećoj zemlji koja uvozniku nameće obveze koje nisu u skladu sa zaštitnim mjerama u tim istim klauzulama, dokazuje da stanje prava treće zemlje može opravdati zabranu prijenosa podataka čak i ako je do njega došlo na temelju standardnih klauzula o zaštiti podataka koje se nalaze u prilogu Odluci o standardnim ugovornim klauzulama i stoga dokazuje da te klauzule mogu biti nedostatne da se osigura primjerena zaštita. Međutim, sud koji je uputio zahtjev nastoji doznati koji je opseg ovlasti povjerenika da zabrani prijenos podataka koji se temelji na tim klauzulama, smatrajući pritom da diskrecijska ovlast ne može biti dostatna za osiguranje primjerene zaštite.

68 U tim je okolnostima High Court (Visoki sud) odlučio prekinuti postupak i uputiti Sudu sljedeća prethodna pitanja:

„1. Kada privatno trgovačko društvo iz države članice [Unije] u komercijalne svrhe prenosi osobne podatke privatnom trgovačkom društvu u trećoj zemlji na temelju Odluke [o standardnim ugovornim klauzulama] te bi tijela treće zemlje te podatke mogla podvrgnuti daljnjoj obradi za potrebe nacionalne sigurnosti, ali i za potrebe održavanja javnog reda i vođenja vanjskih poslova te treće zemlje, primjenjuje li se pravo Unije, uključujući Povelju, na prijenos podataka, neovisno o odredbama članka 4. stavka 2. UEU-a koje se odnose na nacionalnu sigurnost i odredbama članka 3. stavka 2. prve alineje Direktive [95/46] koje se odnose na javnu sigurnost, obranu i nacionalnu sigurnost?

2. (a) Pri utvrđivanju jesu li prava pojedinca povrijeđena prijenosom podataka na temelju Odluke [o standardnim ugovornim klauzulama] iz Unije u treću zemlju, gdje ti podaci mogu biti podvrgnuti daljnjoj obradi za potrebe nacionalne sigurnosti, je li za potrebe Direktive [95/46] relevantno mjerilo za usporedbu:
   (i.) Povelja, UEU, UFEU, Direktiva [95/46], [Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda, potpisana u Rimu 4. studenoga 1950.] (ili bilo koja druga odredba prava Unije); ili
   (ii.) nacionalno zakonodavstvo jedne ili više država članica?
   (b) Ako je (ii.) relevantno mjerilo za usporedbu, trebaju li dio takvog mjerila biti i prakse koje se u kontekstu nacionalne sigurnosti primjenjuju u jednoj ili više država članica?

3. Kada se za potrebe članka 26. Direktive [95/46] ocjenjuje osigurava li treća zemlja za podatke koji se prenose u tu zemlju razinu zaštite koju zahtijeva pravo Unije, treba li razinu zaštite u trećoj zemlji ocijeniti s obzirom na:
   (a) primjenjiva pravila u trećoj zemlji koja proizlaze iz domaćih propisa ili međunarodnih obveza i praksu kojoj je svrha osigurati poštovanje tih pravila, uključujući strukovna pravila i sigurnosne mjere u toj trećoj zemlji;

   ili
   (b) pravila pod (a) i upravne, regulatorne i provedbene prakse te jamstva, postupke, protokole, nadzorne mehanizme i izvansudske pravne lijekove koji postoje u trećoj zemlji?

4. S obzirom na utvrđenja High Courta [(Visoki sud)] u pogledu prava SAD-a, je li riječ o povredi pravâ pojedinaca iz članka 7. ili članka 8. Povelje ako se osobni podaci prenose iz Unije u SAD na temelju Odluke [o standardnim ugovornim klauzulama]?

5. S obzirom na utvrđenja High Courta [(Visoki sud)] u pogledu prava SAD-a, ako se osobni podaci prenose iz [Unije] u SAD na temelju Odluke [o standardnim ugovornim klauzulama]:
   (a) Poštuje li razina zaštite koju pruža SAD bit prava pojedinca na pravni lijek protiv povrede njegovih prava na privatnost zajamčen člankom 47. Povelje?

   Ako je odgovor na peto pitanje pod (a) potvrdan,
   (b) Jesu li ograničenja prava pojedinca na pravni lijek koja pravo SAD-a predviđa u kontekstu nacionalne sigurnosti SAD-a neproporcionalna u smislu članka 52. Povelje te prekoračuju li ono što je u demokratskom društvu nužno za potrebe nacionalne sigurnosti?

6. (a) Koju razinu zaštite, s obzirom na odredbe Direktive [95/46], a osobito s obzirom na njezine članke 25. i 26. tumačene u vezi s Poveljom, treba pružiti osobnim podacima koji se u treću zemlju prenose na temelju standardnih ugovornih klauzula usvojenih u skladu s odlukom Komisije utemeljenom na članku 26. stavku 4. [Direktive 95/46]?
   (b) Koje čimbenike treba uzeti u obzir u ocjeni ispunjava li razina zaštite podataka koji se prenose u treću zemlju na temelju Odluke [o standardnim ugovornim klauzulama] zahtjeve iz Direktive [95/46] i Povelje?

7. Onemogućuje li činjenica da se standardne ugovorne klauzule primjenjuju na odnos izvoznika podataka i uvoznika podataka te da ne obvezuju nacionalna tijela treće zemlje, koja od uvoznika podataka mogu zatražiti da sigurnosnim službama te zemlje stavi na raspolaganje, radi kasnije obrade, osobne podatke prenesene na temelju klauzula Odluke [o standardnim ugovornim klauzulama], da se u tim klauzulama predvide dovoljna jamstva u skladu s člankom 26. stavkom 2. Direktive [95/46]?

8. Ako uvoznik podataka iz treće zemlje podliježe zakonima o nadzoru koje tijelo za zaštitu podataka smatra suprotnima standardnim ugovornim klauzulama, člancima 25. i 26. Direktive [95/46] ili Povelji, mora li tijelo za zaštitu podataka upotrijebiti svoje provedbene ovlasti iz članka 28. stavka 3. Direktive [95/46] kako bi suspendiralo protoke podataka ili je upotreba tih ovlasti ograničena samo na iznimne slučajeve, s obzirom na uvodnu izjavu 11. Odluke [o standardnim ugovornim klauzulama], ili [nadzorno] tijelo može diskrecijski odlučiti da neće suspendirati protoke podataka?

9. (a) Za potrebe članka 25. stavka 6. Direktive [95/46], čini li Odluka [o sustavu zaštite privatnosti] utvrđenje opće primjene koje obvezuje nadzorna tijela i sudove država članica da smatraju da SAD u svojim propisima ili na temelju međunarodnih obveza osigurava odgovarajuću razinu zaštite u smislu članka 25. stavka 2. Direktive [95/46]?
   (b) Ako ne čini, koliko je Odluka [o sustavu zaštite privatnosti] relevantna, ako je uopće relevantna, u ocjeni dostatnosti jamstava predviđenih u pogledu podataka koji se u SAD prenose na temelju Odluke [o standardnim ugovornim klauzulama]?

10. S obzirom na utvrđenja High Courta [(Visoki sud)] u pogledu prava SAD-a, znači li uspostava mehanizma pravobranitelja za zaštitu podataka na temelju Priloga A Prilogu III. Odluci [o sustavu zaštite privatnosti], kada ju se promatra u vezi s postojećim uređenjem u Sjedinjenim Američkim Državama, da Sjedinjene Američke Države osobama čiji se podaci prenose u SAD na temelju Odluke [o standardnim ugovornim klauzulama] osiguravaju pravni lijek koji je u skladu s člankom 47. Povelje?

11. Povrjeđuje li se odlukom [o standardnim ugovornim klauzulama] članak 7., članak 8. ili članak 47. Povelje?”

Dopuštenost zahtjeva za prethodnu odluku

69 Facebook Ireland te njemačka vlada i vlada Ujedinjene Kraljevine navode da je zahtjev za prethodnu odluku nedopušten.

70 Kad je riječ o prigovoru koji je istaknuo Facebook Ireland, to društvo primjećuje da su odredbe Direktive 95/46 na kojima se temelje prethodna pitanja stavljene izvan snage GDPR-om.

71 U tom pogledu, iako je točno da je Direktiva 95/46 na temelju članka 94. stavka 1. GDPR-a bila stavljena izvan snage 25. svibnja 2018., ona je još uvijek bila na snazi 4. svibnja 2018. kad je sastavljen predmetni zahtjev za prethodnu odluku koji je Sud zaprimio 9. svibnja 2018. Osim toga, članak 3. stavak 2. prva alineja, članci 25. i 26. te članak 28. stavak 3. Direktive 95/46, na koja upućuju prethodna pitanja, u bitnom su preuzeti člankom 2. stavkom 2. te člancima 45., 46. i 58. GDPR-a. Nadalje, valja podsjetiti da je zadaća Suda tumačiti sve odredbe prava Unije kada je to potrebno nacionalnim sudovima radi rješavanja predmeta u kojima vode postupke, čak i ako oni te odredbe nisu izričito naveli u pitanjima koja su uputili Sudu (presuda od 2. travnja 2020., Ruska Federacija, C-897/19 PPU, EU:C:2020:262, t. 43. i navedena sudska praksa). Iz tih različitih razloga okolnost da je sud koji je uputio zahtjev formulirao prethodna pitanja pozivajući se samo na odredbe Direktive 95/46 ne može rezultirati nedopuštenošću ovog zahtjeva za prethodnu odluku.

72 Njemačka vlada, pak, svoj prigovor nedopuštenosti zasniva na okolnosti da je, s jedne strane, povjerenik izrazio samo sumnje, a ne konačno stajalište, u vezi s pitanjem valjanosti Odluke o standardnim ugovornim klauzulama i, s druge strane, da sud koji je uputio zahtjev nije provjerio je li M. Schrems nedvojbeno pristao na prijenose podataka iz glavnog postupka, što bi, kad bi to bilo točno, rezultiralo time da odgovor na to pitanje ne bi bio koristan. Naposljetku, vlada Ujedinjene Kraljevine smatra da su prethodna pitanja hipotetske naravi jer taj sud nije utvrdio da su ti podaci doista bili preneseni na temelju navedene odluke.

73 U skladu s ustaljenom sudskom praksom Suda isključivo je na nacionalnom sudu pred kojim se vodi postupak i koji mora preuzeti odgovornost za sudsku odluku koja će biti donesena da, uvažavajući posebnosti predmeta, ocijeni nužnost prethodne odluke za donošenje svoje presude i relevantnost pitanja koja postavlja Sudu. Posljedično, s obzirom na to da se postavljena pitanja odnose na tumačenje ili valjanost pravnog pravila Unije, Sud je u načelu dužan odlučiti. Iz navedenog proizlazi da pitanja koja postave nacionalni sudovi uživaju pretpostavku relevantnosti. Sud može odbiti odlučivati o zahtjevu za prethodnu odluku koji je uputio nacionalni sud samo ako je očito da zatraženo tumačenje prava Unije nema nikakve veze s činjeničnim stanjem ili predmetom spora u glavnom postupku, ako je problem hipotetski ili ako Sud ne raspolaže činjeničnim i pravnim elementima potrebnima da bi mogao dati koristan odgovor na upućena pitanja (presude od 16. lipnja 2015., Gauweiler i dr., C-62/14, EU:C:2015:400, t. 24. i 25.; od 2. listopada 2018., Ministerio Fiscal, C-207/16, EU:C:2018:788, t. 45., i od 19. prosinca 2019., Dobersberger, C-16/18, EU:C:2019:1110, t. 18. i 19.).

74 U predmetnom slučaju zahtjev za prethodnu odluku sadržava činjenične i pravne elemente dostatne za razumijevanje dosega prethodnih pitanja. Nadalje i iznad svega, ni iz jednog elementa u spisu kojim raspolaže Sud ne može se zaključiti da zatraženo tumačenje prava Unije nema veze s činjeničnim stanjem ili predmetom spora u glavnom postupku ili da je hipotetske naravi, među ostalim zato što se prijenos osobnih podataka iz glavnog postupka možebitno temeljio na izričitom pristanku predmetne osobe na taj prijenos, a ne na odluci o standardnim ugovornim klauzulama. Naime, prema navodima iz tog zahtjeva, Facebook Ireland je priznao da je društvu Facebook Inc. prenio osobne podatke svojih pretplatnika s boravištem u Uniji i da je velik dio tih prijenosa, čiju zakonitost osporava M. Schrems, izvršen na temelju standardnih klauzula o zaštiti podataka koje se nalaze u prilogu Odluci o standardnim ugovornim klauzulama.

75 Osim toga, za dopuštenost ovog zahtjeva za prethodnu odluku irelevantno je da povjerenik nije izrazio konačno stajalište o valjanosti te odluke jer sud koji je uputio zahtjev smatra da je odgovor na prethodna pitanja o tumačenju i valjanosti pravnih pravila Unije nužan za rješenje spora u glavnom postupku.

76 Iz toga slijedi da je zahtjev za prethodnu odluku dopušten.

Prethodna pitanja

77 Najprije valja podsjetiti da ovaj zahtjev za prethodnu odluku proizlazi iz pritužbe M. Schremsa kojom se traži da povjerenik obustavi ili zabrani budući prijenos njegovih osobnih podataka iz društva Facebook Ireland na Facebook Inc. Iako se prethodna pitanja odnose na odredbe Direktive 95/46, nesporno je da povjerenik još nije bio donio konačnu odluku o toj pritužbi kada je ta direktiva stavljena izvan snage i zamijenjena GDPR-om, s učinkom od 25. svibnja 2018.

78 To nepostojanje odluke na nacionalnoj razini razlikuje situaciju u glavnom postupku od onih povodom kojih su donesene presude od 24. rujna 2019., Google (Teritorijalni doseg uklanjanja poveznica) (C-507/17, EU:C:2019:772), i od 1. listopada 2019., Planet49 (C-673/17, EU:C:2019:801), u kojima je bila riječ o odlukama donesenima prije stavljanja izvan snage navedene direktive.

79 Stoga na prethodna pitanja valja odgovoriti uzimajući u obzir odredbe GDPR-a, a ne Direktive 95/46.

Prvo pitanje

80 Svojim prvim pitanjem sud koji je uputio zahtjev u biti nastoji doznati treba li članak 2. stavak 1. i članak 2. stavak 2. točke (a), (b) i (d) GDPR-a, u vezi s člankom 4. stavkom 2. UEU-a, tumačiti na način da područje primjene te uredbe obuhvaća prijenos osobnih podataka koji provodi gospodarski subjekt s poslovnim nastanom u državi članici na drugi gospodarski subjekt s poslovnim nastanom u trećoj zemlji ako tijekom ili nakon tog prijenosa te podatke mogu obrađivati tijela te treće zemlje za potrebe javne sigurnosti, obrane i nacionalne sigurnosti.

81 U tom pogledu valja, kao prvo, navesti da se odredba iz članka 4. stavka 2. UEU-a prema kojoj u Uniji nacionalna sigurnost ostaje isključiva odgovornost svake države članice odnosi isključivo na države članice Unije. Posljedično tomu, ta odredba u predmetnom slučaju nije relevantna za tumačenje članka 2. stavka 1. i članka 2. stavka 2. točaka (a), (b) i (d) GDPR-a.

82 U skladu s člankom 2. stavkom 1. GDPR-a, ta uredba se primjenjuje na obradu osobnih podataka koja se u cijelosti obavlja automatizirano te na neautomatiziranu obradu osobnih podataka koji čine dio sustava pohrane ili im je namjena biti njegovim dijelom. Članak 4. stavak 2. te uredbe definira pojam „obrada” kao „svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima”, te kao primjer navodi „otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način” a da pritom ne pravi razliku ovisno o tome jesu li te transakcije izvršene u Uniji ili su povezane s trećom zemljom. Nadalje, navedena uredba podvrgava prijenose osobnih podataka trećim zemljama posebnim pravilima koja se nalaze u njezinu poglavlju V. naslovljenom „Prijenosi osobnih podataka trećim zemljama ili međunarodnim organizacijama” te, nadalje, nadzornim tijelima dodjeljuje posebne ovlasti u tu svrhu, navedene u članku 58. stavku 2. točki (j) te uredbe.

83 Iz toga slijedi da je postupak prijenosa osobnih podataka iz države članice u treću zemlju kao takav obrada osobnih podataka u smislu članka 4. točke 2. GDPR-a, koja se provodi na državnom području države članice i na koju se ta uredba primjenjuje na temelju njezina članka 2. stavka 1. (vidjeti po analogiji, kad je riječ o članku 2. točki (b) i članku 3. stavku 1. Direktive 95/46, presudu od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 45. i navedenu sudsku praksu).

84 Kad je riječ o tome može li se smatrati da je takav postupak isključen iz područja primjene GDPR-a na temelju njegova članka 2. stavka 2., valja podsjetiti da ta odredba predviđa iznimke od područja primjene te uredbe, kako je to područje definirano u njezinu članku 2. stavku 1., i da te iznimke treba usko tumačiti (vidjeti analogijom, kad je riječ o članku 3. stavku 2. Direktive 95/46, presudu od 10. srpnja 2018., Jehovan todistajat, C-25/17, EU:C:2018:551, t. 37. i navedenu sudsku praksu).

85 U predmetnom slučaju, budući da je prijenos osobnih podataka iz glavnog postupka izvršio Facebook Ireland društvu Facebook Inc., odnosno da je bila riječ o prijenosu između dviju pravnih osoba, taj prijenos nije obuhvaćen člankom 2. stavkom 2. točkom (c) GDPR-a koji se odnosi na obradu podataka koju je izvršila fizička osoba tijekom isključivo osobnih ili kućnih aktivnosti. Navedeni prijenos nije obuhvaćen ni izuzećima iz članka 2. stavka 2. točaka (a), (b) i (d) te uredbe s obzirom na to da su aktivnosti koje su ondje navedene kao primjer u svim slučajevima aktivnosti država ili državnih tijela koje ne ulaze u područje aktivnosti pojedinaca (vidjeti analogijom, kad je riječ o članku 3. stavku 2. Direktive 95/46, presudu od 10. srpnja 2018., Jehovan todistajat, C-25/17, EU:C:2018:551, t. 38. i navedenu sudsku praksu).

86 Međutim, mogućnost da tijela predmetne treće zemlje tijekom ili nakon komercijalnog prijenosa osobnih podataka između dvaju gospodarskih subjekata obrađuju te podatke za potrebe javne sigurnosti, obrane i nacionalne sigurnosti ne može navedeni prijenos isključiti iz područja primjene GDPR-a.

87 Nadalje, iz samog teksta članka 45. stavka 2. točke (a) te uredbe, iz kojeg proizlazi izričita Komisijina obveza da prilikom ocjene primjerenosti razine zaštite koju pruža treća zemlja uzme u obzir, među ostalim, „relevantno zakonodavstvo, i opće i sektorsko, što uključuje zakonodavstvo o javnoj sigurnosti, obrani, nacionalnoj sigurnosti, kaznenom pravu i pristupu tijela javne vlasti osobnim podacima, kao i provedbu tog zakonodavstva”, jasno je da činjenica da treća zemlja može obrađivati predmetne podatke za potrebe javne sigurnosti, obrane i nacionalne sigurnosti ne dovodi u pitanje primjenjivost navedene uredbe na prijenos o kojem je riječ.

88 Iz toga slijedi da takav prijenos ne može biti isključen iz područja primjene GDPR-a zbog toga što predmetne podatke tijekom ili nakon tog prijenosa mogu obrađivati tijela predmetne treće zemlje za potrebe javne sigurnosti, obrane ili nacionalne sigurnosti.

89 Stoga na prvo pitanje valja odgovoriti tako da članak 2. stavke 1. i 2. GDPR-a treba tumačiti na način da je područjem primjene te uredbe obuhvaćen prijenos osobnih podataka izvršen u komercijalne svrhe s gospodarskog subjekta s poslovnim nastanom u državi članici drugom gospodarskom subjektu s poslovnim nastanom u trećoj zemlji, bez obzira na to što tijekom ili nakon tog prijenosa te podatke mogu obrađivati tijela predmetne treće zemlje u svrhu javne sigurnosti, obrane ili nacionalne sigurnosti.

Drugo, treće i šesto pitanje

90 Svojim drugim, trećim i šestim pitanjem sud koji je uputio zahtjev u biti pita Sud o razini zaštite koja se zahtijeva člankom 46. stavkom 1. i člankom 46. stavkom 2. točkom (c) GDPR-a u okviru prijenosa osobnih podataka u treću zemlju na temelju standardnih klauzula o zaštiti podataka. Konkretno, taj sud traži od Suda da pojasni koje elemente valja uzeti u obzir kako bi se utvrdilo je li u kontekstu takvog prijenosa ta razina zaštite osigurana.

91 Kad je riječ o zahtijevanoj razini zaštite, iz zajedničkog tumačenja tih odredbi proizlazi da, s obzirom na to da ne postoji odluka o primjerenosti koja se donosi na temelju članka 45. stavka 3. te uredbe, voditelj obrade ili izvršitelj obrade može izvršiti prijenos osobnih podataka trećoj zemlji samo ako je predvidio „odgovarajuće zaštitne mjere" i pod uvjetom da su osobama na koje se odnose podaci na raspolaganju „provediva prava i učinkoviti pravni lijekovi", pri čemu te odgovarajuće zaštitne mjere mogu biti osigurane, među ostalim, standardnim klauzulama o zaštiti podataka koje je donijela Komisija.

92 Iako članak 46. GDPR-a ne pojašnjava prirodu zahtjeva koji proizlaze iz tog upućivanja na „odgovarajuće zaštitne mjere", „provediva prava" i „učinkovite pravne lijekove", valja navesti da se taj članak nalazi u poglavlju V. te uredbe. Stoga se navedeni članak mora tumačiti u vezi s člankom 44. navedene uredbe, koji se naziva „Opća načela prijenosa" i određuje da se „[s]ve odredbe iz [tog] poglavlja primjenjuju […] kako bi se osiguralo da se ne ugrozi razina zaštite pojedinaca zajamčena [tom] uredbom". Ta razina zaštite stoga mora biti zajamčena bez obzira na odredbu navedenog poglavlja na temelju koje se izvršava prijenos osobnih podataka u treću zemlju.

93 Naime, kao što je to naveo nezavisni odvjetnik u točki 117. svojeg mišljenja, odredbe poglavlja V. GDPR-a imaju za cilj osigurati kontinuirano visoku razinu zaštite osobnih podataka kada se ti podaci prenose u treću zemlju, u skladu s ciljem navedenim u uvodnoj izjavi 6. te uredbe.

94 Prva rečenica članka 45. stavka 1. GDPR-a predviđa da se prijenos osobnih podataka trećoj zemlji može odobriti Komisijinom odlukom da treća zemlja, područje ili jedan ili više određenih sektora unutar te treće zemlje osigurava primjerenu razinu zaštite. U tom pogledu izraz „primjerena razina zaštite" mora se razumjeti, kao što to potvrđuje uvodna izjava 104. te uredbe, tako da od treće zemlje zahtijeva da na temelju svojeg domaćeg zakonodavstva ili međunarodnih obveza osigura zaštitu temeljnih sloboda i prava koji su bitno ekvivalentni onima zajamčenima u okviru Unije na temelju navedene uredbe, tumačene u vezi s Poveljom, dakle od predmetne treće zemlje ne zahtijeva se razina zaštite koja je istovjetna onoj zajamčenoj u pravnom poretku Unije. Naime, kad ne bi postojao takav zahtjev, cilj naveden u prethodnoj točki bio bi povrijeđen (vidjeti analogijom, kad je riječ o članku 25. stavku 6. Direktive 95/46, presudu od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 73.).

95 U tom kontekstu uvodna izjava 107. GDPR-a određuje da kada „treća zemlja, područje ili posebni sektor u trećoj zemlji […] više ne osiguravaju primjereni stupanj zaštite podataka […] prijenos osobnih podataka u tu treću zemlju trebao [bi se] zabraniti, osim ako su ispunjeni uvjeti iz [te] uredbe koji se odnose na prijenose koji podliježu odgovarajućim zaštitnim mjerama […]". U tu svrhu uvodna izjava 108. navedene uredbe pojašnjava da bi, ako nije donesena odluka o primjerenosti, voditelj obrade ili izvršitelj obrade trebali poduzeti odgovarajuće zaštitne mjere na temelju članka 46. stavka 1. te uredbe kojima će se „nadomjestiti nedostatak zaštite podataka u trećoj zemlji" kako bi se „osigura[la] sukladnost sa zahtjevima za zaštitu podataka i prava ispitanikâ primjereno obradi unutar Unije."

96 Iz toga proizlazi, kao što je to nezavisni odvjetnik naveo u točki 115. svojeg mišljenja, da te odgovarajuće zaštitne mjere moraju biti takve da osiguraju da se na prava osoba čiji se osobni podaci prenose trećoj zemlji primjenjuje, kao u okviru prijenosa koji se temelji na odluci o primjerenosti, razina zaštite koja je bitno ekvivalentna razini zaštite zajamčene u Uniji.

97 Sud koji je uputio zahtjev također se pita treba li tu razinu zaštite koja je bitno ekvivalentna onoj zajamčenoj u Uniji određivati s obzirom na pravo Unije, osobito prava utvrđena Poveljom, i/ili s obzirom na temeljna prava zajamčena Europskom konvencijom za zaštitu ljudskih prava i temeljnih sloboda (u daljnjem tekstu: EKLJP) ili nacionalno pravo država članica.

98 U tom pogledu valja podsjetiti da, iako temeljna prava iz EKLJP-a kao opća načela predstavljaju dio pravnog poretka Unije, što potvrđuje i članak 6. stavak 3. UEU-a, te iako članak 52. stavak 3. Povelje određuje da u njoj sadržana prava koja odgovaraju pravima sadržanima u EKLJP-u imaju jednako značenje i opseg primjene kao i ona iz spomenute konvencije, navedena konvencija nije pravni

instrument koji formalno predstavlja dio pravnog poretka Unije jer joj Unija nije pristupila (presude od 26. veljače 2013., Åkerberg Fransson, C-617/10, EU:C:2013:105, t. 44. i navedena sudska praksa i od 20. ožujka 2018., Menci, C-524/15, EU:C:2018:197, t. 22.).

99 U tim okolnostima Sud je presudio da tumačenje prava Unije te ispitivanje valjanosti akata Unije treba izvršiti s obzirom na temeljna prava zajamčena Poveljom (vidjeti analogijom presudu od 20. ožujka 2018., Menci, C-524/15, EU:C:2018:197, t. 24.).

100 Nadalje, ustaljena je sudska praksa da se valjanost odredaba prava Unije i, u nedostatku izričitog upućivanja na nacionalno pravo država članica, njihovo tumačenje ne može ocjenjivati s obzirom na to nacionalno pravo, čak ni ustavno pravo, osobito s obzirom na temeljna prava kako su formulirana u njihovu nacionalnom ustavu (vidjeti u tom smislu presude od 17. prosinca 1970., Internationale Handelsgesellschaft, 11/70, EU:C:1970:114, t. 3.; od 13. prosinca 1979., Hauer, 44/79, EU:C:1979:290, t. 14. i od 18. listopada 2016., Nikiforidis, C-135/15, EU:C:2016:774, t. 28. i navedenu sudsku praksu).

101 Iz toga slijedi da, budući da, s jedne strane, komercijalni prijenos osobnih podataka, poput onog o kojem je riječ u glavnom postupku, s gospodarskog subjekta s poslovnim nastanom u državi članici na drugi gospodarski subjekt sa sjedištem u trećoj zemlji ulazi, kao što to proizlazi iz odgovora na prvo pitanje, u područje primjene GDPR-a i da, s druge strane, ta uredba ima za cilj, kao što to proizlazi iz njezine uvodne izjave 10., osigurati postojanu i visoku razinu zaštite pojedinaca u Uniji te u tu svrhu osigurati postojanu i homogenu primjenu pravila za zaštitu temeljnih prava i sloboda pojedinaca u vezi s obradom osobnih podataka u čitavoj Uniji, razina zaštite temeljnih prava koja se zahtijeva člankom 46. stavkom 1. te uredbe mora se utvrđivati na temelju odredbi te iste uredbe, tumačenih u vezi s temeljnim pravima zajamčenima Poveljom.

102 Sud koji je uputio zahtjev zatim nastoji doznati koje elemente valja uzeti u obzir kako bi utvrdio primjerenost razine zaštite u kontekstu prijenosa osobnih podataka trećoj zemlji na temelju standardnih klauzula za zaštitu podataka donesenih na temelju članka 46. stavka 2. točke (c) GDPR-a.

103 U tom pogledu, iako ta odredba ne nabraja različite elemente koje valja uzeti u obzir kako bi se ocijenila primjerenost razine zaštite koju treba poštovati u okviru takvog prijenosa, članak 46. stavak 1. te uredbe određuje da osobe na koje se odnose podaci moraju imati na raspolaganju provediva prava i učinkovite pravne lijekove.

104 U kontekstu takvog prijenosa zahtijevana ocjena u tu svrhu mora osobito uzeti u obzir ugovorne odredbe koje su ugovorili voditelj obrade ili izvršitelj obrade s poslovnim nastanom u Uniji i primatelj podataka s poslovnim nastanom u predmetnoj trećoj zemlji te, kad je riječ o eventualnom pristupu javnih tijela te treće zemlje prenesenim osobnim podacima, relevantne elemente njezina pravnog sustava. U potonjem smislu elementi koje valja uzeti u obzir u kontekstu članka 46. navedene uredbe odgovaraju onima koji su na neiscrpan način navedeni u članku 45. stavku 2. navedene uredbe.

105 Stoga na drugo, treće i šesto pitanje valja odgovoriti tako da članak 46. stavak 1. i članak 46. stavak 2. točku (c) GDPR-a valja tumačiti tako da odgovarajuće zaštitne mjere, provediva prava i djelotvorne pravne lijekove koji se zahtijevaju tim odredbama moraju osigurati da prava osoba čiji se osobni podaci prenose trećoj zemlji na temelju standardnih klauzula o zaštiti podataka uživaju razinu zaštite koja je bitno ekvivalentna onoj zajamčenoj u okviru Unije tom uredbom, tumačenom u vezi s Poveljom. U tom smislu ocjena razine zaštite koja se osigurava u kontekstu takvog prijenosa mora, osobito, uzeti u obzir kako ugovorne odredbe koje su ugovorili voditelj obrade ili izvršitelj obrade s poslovnim nastanom u Uniji i primatelj podataka s poslovnim nastanom u predmetnoj trećoj zemlji tako i, kad je riječ o eventualnom pristupu javnih tijela te treće zemlje tako prenesenim osobnim podacima, relevantne elemente njezina pravnog sustava, osobito one navedene u članku 45. stavku 2. navedene uredbe.

Osmo pitanje

106 Svojim osmim pitanjem sud koji je uputio zahtjev želi u biti znati treba li članak 58. stavak 2. točke (f) i (j) GDPR-a tumačiti na način da je nadležno nadzorno tijelo dužno obustaviti ili zabraniti prijenos osobnih podataka trećoj zemlji koji se temelji na standardnim klauzulama o zaštiti podataka koje je donijela Komisija ako to nadzorno tijelo smatra da te odredbe nisu ili ne mogu biti poštovane u toj trećoj zemlji i da se zaštita prenesenih podataka koja se zahtijeva pravom Unije, osobito člancima 45. i 46. GDPR-a i Poveljom, ne može osigurati, ili ga treba tumačiti na način da je izvršavanje tih ovlasti ograničeno na izvanredne situacije.

107 U skladu s člankom 8. stavkom 3. Povelje te člankom 51. stavkom 1. i člankom 57. stavkom 1. točkom (a) GDPR-a, nacionalna nadzorna tijela odgovorna su za nadzor poštovanja pravila Unije o zaštiti pojedinaca u vezi s obradom osobnih podataka. Stoga je svako od njih nadležno provjeriti poštuje li prijenos osobnih podataka iz države članice kojoj to tijelo pripada u treću zemlju zahtjeve postavljene tom uredbom (vidjeti analogijom, kad je riječ o članku 28. Direktive 95/46, presudu od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 47.).

108 Iz tih odredbi proizlazi da je primarna zadaća nadzornih tijela kontrolirati primjenu GDPR-a i nadzirati njegovo poštovanje. Izvršavanje te zadaće ima posebnu važnost u kontekstu prijenosa osobnih podataka trećoj zemlji jer, kao što to proizlazi iz samog teksta uvodne izjave 116. te uredbe, „[k]ada se osobni podaci kreću preko granica izvan Unije, može se povećati rizik koji prijeti sposobnosti pojedinaca da ostvare svoja prava zaštite podataka, osobito da se zaštite od nezakonite uporabe ili otkrivanja tih informacija”. U tom slučaju, kao što je navedeno u toj uvodnoj izjavi, „[n]adzorna tijela mogu istodobno otkriti da nisu u stanju rješavati pritužbe ili voditi istrage u vezi s aktivnostima izvan svojih granica”.

109 Nadalje, na temelju članka 57. stavka 1. točke (f) GDPR-a, svako nadzorno tijelo dužno je, na svojem području, rješavati pritužbe koje u skladu s člankom 77. stavkom 1. te uredbe može podnijeti svaka osoba kad smatra da obrada osobnih podataka koja se odnosi na nju predstavlja povredu navedene uredbe, te ispitati njezin predmet u mjeri u kojoj je to potrebno. Nadzorno tijelo mora postupati s takvom pritužbom uz svu dužnu pažnju (vidjeti analogijom, kad je riječ o članku 25. stavku 6. Direktive 95/46, presudu od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 63.).

110 Člankom 78. stavcima 1. i 2. GDPR-a svakoj osobi priznaje se pravo na učinkoviti pravni lijek među ostalim ako nadzorno tijelo ne riješi njezinu pritužbu. Uvodna izjava 141. te uredbe također upućuje na to „pravo na učinkoviti pravni lijek u skladu s člankom 47. Povelje” u slučaju da to nadzorno tijelo „ne djeluje kada je takvo djelovanje nužno radi zaštite prava ispitanika”.

111 Kako bi rješavalo podnesene pritužbe, članak 58. stavak 1. GDPR-a svakom nadzornom tijelu dodjeljuje znatne istražne ovlasti. Kada takvo tijelo po okončanju svoje istrage ocijeni da predmetna osoba čiji su osobni podaci preneseni u treću zemlju u njoj ne uživa primjerenu razinu zaštite, to je tijelo dužno, na temelju prava Unije, na odgovarajući način postupati kako bi otklonilo utvrđeni nedostatak, i to neovisno o podrijetlu ili naravi tog nedostatka. U tu svrhu članak 58. stavak 2. te uredbe navodi različite korektivne ovlasti koje nadzorno tijelo može usvojiti.

112 Iako je izbor prikladnog i nužnog sredstva na nadzornom tijelu te ono mora izvršiti taj izbor uzimajući u obzir sve okolnosti predmetnog prijenosa osobnih podataka, to tijelo i dalje mora, uz svu dužnu pažnju, ispunjavati svoju zadaću nadziranja punog poštovanja GDPR-a.

113 U tom pogledu i kao što je to nezavisni odvjetnik također istaknuo u točki 148. svojeg mišljenja, navedeno tijelo dužno je, na temelju članka 58. stavka 2. točaka (f) i (j) te uredbe, obustaviti ili zabraniti prijenos osobnih podataka trećoj zemlji kada, s obzirom na sve okolnosti svojstvene tom prijenosu, smatra da se u toj trećoj zemlji ne poštuju ili ne mogu poštovati standardne odredbe o

zaštiti podataka i da se zaštita prenesenih podataka koja se zahtijeva pravom Unije ne može osigurati drugim sredstvima, ako voditelj obrade ili izvršitelj obrade s poslovnim nastanom u Uniji sam nije obustavio ili okončao prijenos.

114 Tumačenje iz prethodne točke nije dovedeno u pitanje argumentacijom povjerenika prema kojem je članak 4. Odluke 2010/87, u svojoj verziji koja je prethodila stupanju na snagu Provedbene odluke 2016/2297, tumačen u vezi s uvodnom izjavom 11. te odluke, ograničavao ovlast nadzornih tijela da obustave ili zabrane prijenos osobnih podataka trećoj zemlji na određene izvanredne slučajeve. Naime, u svojoj verziji proizašloj iz Provedbene odluke 2016/2297, članak 4. Odluke o standardnim ugovornim klauzulama upućuje na ovlast tih tijela, koja se sada temelji na članku 58. stavku 2. točkama (f) i (j) GDPR-a, da obustave ili zabrane takav prijenos a da pritom ni na koji način ne ograničava izvršavanje te ovlasti na izvanredne okolnosti.

115 U svakom slučaju, provedbena ovlast koja je člankom 46. stavkom 2. točkom (c) GDPR-a Komisiji dodijeljena kako bi donijela standardne klauzule o zaštiti podataka ne daje joj nadležnost za ograničavanje ovlasti kojima raspolažu nadzorna tijela na temelju članka 58. stavka 2. te uredbe (vidjeti analogijom, kad je riječ o članku 25. stavku 6. i članku 28. Direktive 95/46, presudu od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 102. i 103.). Uostalom, uvodna izjava 5. Provedbene odluke 2016/2297 potvrđuje da odluka o standardnim klauzulama „ne sprječava [nadzorno tijelo] da izvršava svoje ovlasti nadzora tokova podataka, uključujući ovlasti obustave ili zabrane prijenosa osobnih podataka ako utvrdi da se tim prijenosom krši zakon[odavstvo] o zaštiti podataka u EU-u ili pojedinačnoj državi članici”.

116 Međutim, valja pojasniti da nadležno nadzorno tijelo mora u potpunosti poštovati odluku kojom Komisija u slučaju potrebe utvrđuje, na temelju članka 45. stavka 1. prve rečenice GDPR-a, da određena treća zemlja osigurava primjerenu razinu zaštite. Naime, u takvoj situaciji iz članka 45. stavka 1. druge rečenice te uredbe, u vezi s njezinom uvodnom izjavom 103., proizlazi da se prijenosi osobnih podataka predmetnoj trećoj zemlji mogu izvršiti a da ne zahtijevaju posebno odobrenje.

117 Na temelju članka 288. četvrtog stavka UFEU-a, Komisijina odluka o primjerenosti u cijelosti je obvezujuća za sve države članice kojima je upućena i stoga je obvezujuća za sva njihova tijela jer se njome utvrđuje da dotična treća zemlja jamči odgovarajuću razinu zaštite i jer ima za učinak odobravanje tih prijenosa podataka (vidjeti analogijom, kad je riječ o članku 25. stavku 6. Direktive 95/46, presudu od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 51. i navedenu sudsku praksu).

118 Sve dok odluku o primjerenosti Sud ne proglasi nevaljanom, države članice i njihova tijela, uključujući neovisna nadzorna tijela, ne mogu donositi mjere koje su suprotne toj odluci, kao što su to akti kojima se s obvezujućim učinkom utvrđuje da treća zemlja na koju se odnosi ta odluka ne osigurava odgovarajuću razinu zaštite (presuda od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 52. i navedena sudska praksa) i, posljedično tomu, obustaviti ili zabraniti prijenose osobnih podataka toj trećoj zemlji.

119 Međutim, Komisijina odluka o primjerenosti donesena na temelju članka 45. stavka 3. GDPR-a ne može spriječiti osobe čiji su osobni podaci preneseni ili bi mogli biti preneseni trećoj zemlji da podnesu pritužbu nacionalnim nadzornim tijelima, u smislu članka 77. stavka 1. GDPR-a, u vezi sa zaštitom njihovih prava i sloboda u odnosu na obradu tih podataka. Isto tako, takva odluka ne može ni ukinuti ni smanjiti ovlasti koje su člankom 8. stavkom 3. Povelje te člankom 51. stavkom 1. i člankom 57. stavkom 1. točkom (a) navedene uredbe izričito priznate nacionalnim nadzornim tijelima (vidjeti analogijom, što se tiče članka 25. stavka 6. i članka 28. Direktive 95/46, presudu od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 53.).

120 Stoga, čak i kada postoji Komisijina odluka o primjerenosti, nadležno nacionalno nadzorno tijelo, kojem je osoba podnijela pritužbu u vezi sa zaštitom svojih prava i sloboda u odnosu na obradu osobnih podataka koji se na nju odnose, mora biti u mogućnosti potpuno neovisno ispitati poštuje li prijenos tih podataka zahtjeve iz GDPR-a i, prema potrebi, pokrenuti postupak pred nacionalnim sudovima kako bi potonji, ako dijele sumnje tog tijela u valjanost odluke o primjerenosti, uputili zahtjev za prethodnu odluku u svrhu ispitivanja te valjanosti (vidjeti analogijom, kad je riječ o članku 25. stavku 6. i članku 28. Direktive 95/46, presudu od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 57. i 65.).

121 S obzirom na prethodna razmatranja, na osmo pitanje valja odgovoriti tako da članak 58. stavak 2. točke (f) i (j) GDPR-a treba tumačiti na način da je nadležno nadzorno tijelo, osim ako postoji odluka o primjerenosti koju je Komisija valjano donijela, dužno obustaviti ili zabraniti prijenos podataka trećoj zemlji na temelju standardnih klauzula o zaštiti podataka koje je donijela Komisija, kada to nadzorno tijelo smatra, u vezi sa svim okolnostima tog prijenosa, da te klauzule nisu ili ne mogu biti poštovane u toj trećoj zemlji i da zaštita prenesenih podataka koja se zahtijeva pravom Unije, osobito člancima 45. i 46. GDPR-a i Poveljom, ne može biti osigurana drugim sredstvima, ako voditelj obrade ili izvršitelj obrade s poslovnim nastanom u Uniji sam nije obustavio prijenos ili ga okončao.

Sedmo i jedanaesto pitanje

122 Svojim sedmim i jedanaestim pitanjem, koja valja razmotriti zajedno, sud koji je uputio zahtjev u biti pita Sud o valjanosti Odluke o standardnim ugovornim klauzulama s obzirom na članke 7., 8. i 47. Povelje.

123 Konkretno, kao što proizlazi iz samog teksta sedmog pitanja i s njime povezanih pojašnjenja u zahtjevu za prethodnu odluku, sud koji je uputio zahtjev pita se može li odluka o standardnim ugovornim klauzulama osigurati primjerenu razinu zaštite osobnih podataka prenesenih trećoj zemlji s obzirom na to da standardne klauzule o zaštiti podataka koje predviđa ne obvezuju tijela te treće zemlje.

124 Članak 1. Odluke o standardnim ugovornim klauzulama određuje da standardne klauzule o zaštiti podataka koje se nalaze u njezinu prilogu pružaju odgovarajuće zaštitne mjere u smislu zaštite privatnosti i temeljnih prava i sloboda pojedinaca, u skladu sa zahtjevima članka 26. stavka 2. Direktive 95/46. Potonja odredba u bitnom je preuzeta u članku 46. stavku 1. i članku 46. stavku 2. točki (c) GDPR-a.

125 Međutim, iako su te klauzule obvezujuće za voditelja obrade s poslovnim nastanom u Uniji i primatelja osobnih podataka s poslovnim nastanom u trećoj zemlji u slučaju da su sklopili ugovor pozivanjem na te klauzule, nesporno je da navedene klauzule ne mogu obvezivati tijela te treće zemlje jer potonja nisu ugovorna stranka.

126 Iako stoga postoje situacije u kojima, ovisno o postojećem pravu i praksama u predmetnoj trećoj zemlji, primatelj takvih podataka može jamčiti potrebnu zaštitu podataka isključivo na temelju standardnih klauzula o zaštiti podataka, postoje i drugačije situacije u kojima sadržaj tih klauzula može biti nedostatno sredstvo kojim bi se u praksi mogla osigurati učinkovita zaštita osobnih podataka prenesenih predmetnoj trećoj zemlji. To je slučaj osobito kad pravo te treće zemlje njezinim javnim tijelima dopušta zadiranje u prava osoba na koje se podaci odnose.

127 Tako se postavlja pitanje je li Komisijina odluka o standardnim klauzulama o zaštiti podataka, donesena na temelju članka 46. stavka 2. točke (c) GDPR-a, nevaljana jer u toj odluci ne postoje zaštitne mjere na koje bi se bilo moguće pozvati protiv javnih tijela treće zemlje kojoj su na temelju tih klauzula osobni podaci preneseni ili bi to mogli biti.

128 Članak 46. stavak 1. GDPR-a propisuje da ako nije donesena odluka o primjerenosti, voditelj obrade ili izvršitelj obrade može prenijeti osobne podatke trećoj zemlji samo ako je predvidio odgovarajuće zaštitne mjere i pod uvjetom da su osobama na koje se odnose podaci na raspolaganju provediva prava i učinkoviti pravni lijekovi. U skladu s člankom 46. stavkom 2. točkom (c) te uredbe, te zaštitne mjere mogu se osigurati standardnim klauzulama o zaštiti podataka koje je donijela Komisija. Međutim, te odredbe ne određuju da sve navedene zaštitne mjere moraju nužno biti predviđene Komisijinom odlukom poput odluke o standardnim ugovornim klauzulama.

129 U tom pogledu valja navesti da se takva odluka razlikuje od odluke o primjerenosti donesene na temelju članka 45. stavka 3. GDPR-a čiji je cilj, nakon ispitivanja propisa predmetne treće zemlje uzimanjem u obzir osobito relevantnog zakonodavstva u području nacionalne sigurnosti i pristupa javnih tijela osobnim podacima, utvrditi s obvezujućim učinkom da treća zemlja, područje ili jedan ili više određenih sektora unutar treće zemlje osigurava primjerenu razinu zaštite i da stoga pristup javnih tijela navedene treće zemlje takvim podacima nije prepreka prijenosima tih podataka toj trećoj zemlji. Komisija može donijeti takvu odluku o primjerenosti dakle samo pod uvjetom da je utvrđeno da relevantno zakonodavstvo te treće zemlje u tom području stvarno sadržava sve potrebne zaštitne mjere na temelju kojih se može utvrditi da osigurava primjerenu razinu zaštite.

130 Nasuprot tomu, kad je riječ o Komisijinoj odluci kojom se donose standardne klauzule o zaštiti podataka, poput Odluke o standardnim ugovornim klauzulama, u mjeri u kojoj se takva odluka ne odnosi na određenu treću zemlju, područje ili jedan ili više određenih sektora unutar treće zemlje, iz članka 46. stavka 1. i članka 46. stavka 2. točke (c) GDPR-a ne može se zaključiti da je Komisija dužna prije donošenja takve odluke izvršiti ocjenu primjerenosti razine zaštite koju osigurava treća zemlja kojoj bi osobni podaci mogli biti preneseni na temelju takvih klauzula.

131 U tom pogledu valja podsjetiti da na temelju članka 46. stavka 1. te uredbe, ako Komisija nije donijela odluku o primjerenosti, na voditelju obrade ili izvršitelju obrade s poslovnim nastanom u Uniji je da predvidi odgovarajuće zaštitne mjere. Uvodne izjave 108. i 114. navedene uredbe potvrđuju da, kada Komisija nije donijela odluku o primjerenoj razini zaštite podataka u trećoj zemlji, voditelj obrade ili, prema potrebi, izvršitelj obrade „trebali bi poduzeti mjere kojima će se nadomjestiti nedostatak zaštite podataka u trećoj zemlji putem odgovarajućih zaštitnih mjera za ispitanika” i da bi se „[t]im zaštitnim mjerama trebalo […] osigurati sukladnost sa zahtjevima za zaštitu podataka i prava ispitanikâ primjereno obradi unutar Unije, uključujući dostupnost provedivih prava ispitanika i učinkovitih pravnih lijekova […] u Uniji ili u trećoj zemlji”.

132 Budući da je, kao što to proizlazi iz točke 125. ove presude, ugovornoj naravi standardnih klauzula o zaštiti podataka svojstveno da one ne mogu obvezivati javna tijela treće zemlje, nego da članak 44., članak 46. stavak 1. i članak 46. stavak 2. točka (c) GDPR-a, tumačeni u vezi s člancima 7., 8. i 47. Povelje, zahtijevaju da razina zaštite fizičkih osoba zajamčena tom uredbom ne bude ugrožena, može se pokazati nužnim dopuniti zaštitne mjere sadržane u tim standardnim klauzulama o zaštiti podataka. U tom smislu uvodna izjava 109. te uredbe određuje da „[m]ogućnost da se voditelj obrade […] koristi standardnim klauzulama o zaštiti podataka koje je donijela Komisija […] ne bi trebala sprečavati mogućnost voditelja obrade […] da dodaju druge klauzule ili dodatne zaštitne mjere” te među ostalim navodi da bi voditelje obrade „trebalo […] poticati da osiguraju dodatne zaštitne mjere […] koje nadopunjuju standardne klauzule o zaštiti [podataka]”.

133 Tako proizlazi da je svrha standardnih ugovornih klauzula o zaštiti podataka koje je Komisija donijela na temelju članka 46. stavka 2. točke (c) navedene uredbe isključivo pružiti voditeljima obrade ili njihovim izvršiteljima s poslovnim nastanom u Uniji ugovorne zaštitne mjere koje se ujednačeno primjenjuju u svim trećim zemljama i stoga neovisno o razini zaštite zajamčenoj u svakoj od tih zemalja. Budući da te standardne klauzule o zaštiti podataka zbog svoje naravi ne mogu pružiti jamstva koja bi prelazila ugovornu obvezu nadziranja poštovanja razine zaštite koja se zahtijeva pravom Unije, može se pokazati potrebnim da voditelj obrade, ovisno o situaciji u određenoj trećoj zemlji, donese dodatne mjere kako bi osigurao poštovanje te razine zaštite.

134 U tom pogledu, kao što je nezavisni odvjetnik naveo u točki 126. svojeg mišljenja, ugovorni mehanizam predviđen u članku 46. stavku 2. točki (c) GDPR-a, temelji se na davanju odgovornosti voditelju obrade ili njegovu izvršitelju s poslovnim nastanom u Uniji te, podredno, nadležnom nadzornom tijelu. Stoga je prije svega na tom voditelju obrade ili njegovu izvršitelju da u svakom slučaju zasebno i, ako je potrebno, u suradnji s primateljem podataka, provjere osigurava li pravo treće zemlje odredišta primjerenu zaštitu, s obzirom na pravo Unije, osobnih podataka prenesenih na temelju standardnih klauzula o zaštiti podataka, tako da prema potrebi osigura dodatne zaštitne mjere uz one ponuđene tim klauzulama.

135 Ako voditelj obrade ili njegov izvršitelj s poslovnim nastanom u Uniji ne može donijeti dodatne mjere koje bi bile dostatne da se osigura takva zaštita, oni ili, podredno, nadležno nadzorno tijelo moraju obustaviti ili okončati prijenos osobnih podataka predmetnoj trećoj zemlji. Tako je osobito kad pravo te treće zemlje primatelju osobnih podataka iz Unije nalaže obveze koje su suprotne navedenim klauzulama i stoga mogu dovesti u pitanje ugovorno jamstvo primjerene razine zaštite od pristupa javnih tijela navedene treće zemlje tim podacima.

136 Stoga sama činjenica da standardne ugovorne klauzule o zaštiti podataka koje se nalaze u Komisijinoj odluci donesenoj na temelju članka 46. stavka 2. točke (c) GDPR-a, poput onih iz priloga Odluci o standardnim ugovornim klauzulama, ne obvezuju tijela treće zemlje u koju osobni podaci mogu biti preneseni ne može utjecati na valjanost te odluke.

137 S druge strane, ta valjanost ovisi o tome sadržava li, u skladu sa zahtjevom iz članka 46. stavka 1. i članka 46. stavka 2. točke (c) GDPR-a, tumačenih u vezi s člancima 7., 8. i 47. Povelje, takva odluka učinkovite mehanizme koji u praksi omogućuju osiguranje razine zaštite koja se zahtijeva pravom Unije i obustavu ili zabranu prijenosa osobnih podataka temeljenih na takvim klauzulama u slučaju povrede tih klauzula ili nemogućnosti njihova poštovanja.

138 Što se tiče zaštitnih mjera sadržanih u standardnim klauzulama o zaštiti podataka iz Priloga Odluci o standardnim ugovornim klauzulama, iz njezine klauzule 4. točaka (a) i (b), klauzule 5. točke (a), klauzule 9. i klauzule 11. stavka 1. proizlazi da se voditelj obrade s poslovnim nastanom u Uniji, primatelj osobnih podataka i njegov eventualni izvršitelj obrade međusobno obvezuju da se obrada tih podataka, uključujući njihov prijenos, provodila te će se nastaviti provoditi u skladu s „pravom koje se primjenjuje na zaštitu podataka”, odnosno, prema definiciji u članku 3. točki (f) navedene odluke, „zakonodavstvo[m] koje štiti temeljna prava i slobode pojedinaca i posebno njihovo pravo na privatnost u pogledu obrade osobnih podataka koje primjenjuje nadzornik podataka u državi članici u kojoj izvoznik podataka ima poslovni nastan”. Odredbe GDPR-a, tumačene u vezi s Poveljom, dio su tog zakonodavstva.

139 Nadalje, primatelj osobnih podataka s poslovnim nastanom u trećoj zemlji obvezuje se na temelju te klauzule 5. točke (a) odmah obavijestiti voditelja obrade s poslovnim nastanom u Uniji u slučaju da eventualno ne može postupiti u skladu s obvezama koje ima na temelju sklopljenog ugovora. Konkretno, prema navedenoj klauzuli 5. točki (b), taj primatelj jamči da nema razloga za vjerovanje da ga zakonodavstvo koje se na njega primjenjuje onemogućava u ispunjavanju njegovih obveza prema ugovoru te da će u slučaju promjene u zakonodavstvu koja bi mogla imati bitan negativan učinak na jamstva i obveze iz klauzula o zaštiti podataka koje se nalaze u prilogu Odluci o standardnim ugovornim klauzulama, o promjeni odmah obavijestiti voditelja obrade podataka čim toga postane svjestan. Nadalje, iako ta klauzula 5. u točkama (d) podtočki (i) omogućuje primatelju osobnih podataka da voditelja obrade s poslovnim nastanom u Uniji ne obavijesti o pravno obvezujućem zahtjevu tijela kaznenog progona za otkrivanje osobnih podataka ako postoji propis koji brani takvo primateljevo postupanje poput zabrane prema kaznenom pravu radi očuvanja povjerljivosti kaznene istrage, primatelj je ipak dužan, u skladu s klauzulom 5. točkom (a) priloga Odluci o standradnim ugovornim klauzulama, obavijestiti voditelja obrade o svojoj nemogućnosti da postupi u skladu sa standardnim klauzulama o zaštiti podataka.

140 U obama slučajevima na koje se odnosi, ta klauzula 5. u točkama (a) i (b) voditelju obrade s poslovnim nastanom u Uniji dodjeljuje pravo da obustavi prijenos podataka i/ili raskine ugovor. S obzirom na zahtjeve iz članka 46. stavka 1. i članka 46. stavka 2. točke (c) GDPR-a, u vezi s člancima 7. i 8. Povelje, voditelj obrade obvezan je obustaviti prijenos podataka i/ili raskinuti ugovor kad primatelj podataka ne može ili više ne može poštovati standardne klauzule o zaštiti podataka. U suprotnom bi voditelj obrade povrijedio zahtjeve koje mu nalaže klauzula 4. točka (a) priloga Odluci o standardnim ugovornim klauzulama, tumačena u vezi s odredbama GDPR-a i Povelje.

141 Tako proizlazi da klauzula 4. točka (a) i klauzula 5. točke (a) i (b) tog priloga obvezuju voditelja obrade s poslovnim nastanom u Uniji i primatelja osobnih podataka da prije provođenja prijenosa osobnih podataka u treću zemlju odredišta provjere omogućuje li zakonodavstvo te zemlje navedenom primatelju da postupi u skladu sa standardnim klauzulama o zaštiti podataka koje se nalaze u prilogu Odluci o standardnim ugovornim klauzulama. Kad je riječ o toj provjeri, bilješka koja se odnosi na navedenu klauzulu 5. pojašnjava da obvezni zahtjevi tog zakonodavstva koji ne nadilaze ono što je neophodno u demokratskom društvu za očuvanje nacionalne sigurnosti, obrane i javne sigurnosti nisu protivni tim standardnim klauzulama za zaštitu podataka. Nasuprot tomu, kao što je istaknuo nezavisni odvjetnik u točki 131. svojeg mišljenja, činjenica ispunjavanja obveze koja se temelji na pravu treće zemlje odredišta koja prekoračuje ono što je nužno za takvu svrhu mora se smatrati povredom navedenih klauzula. Ocjena tih subjekata o nužnosti takve obveze mora, ovisno o slučaju, uzeti u obzir da je u Komisijinoj odluci o primjerenosti donesenoj na temelju članka 45. stavka 3. GDPR-a utvrđeno da predmetna treća zemlja osigurava primjerenu razinu zaštite.

142 Iz toga proizlazi da su voditelj obrade s poslovnim nastanom u Uniji i primatelj osobnih podataka dužni prethodno provjeriti poštuje li predmetna treća zemlja razinu zaštite koja se zahtijeva pravom Unije. Primatelj tih podataka je, u slučaju potrebe, na temelju te klauzule 5. točke (b) obvezan obavijestiti voditelja obrade o svojoj eventualnoj nemogućnosti da postupi u skladu tim klauzulama, te je na potonjem da obustavi prijenos podataka i/ili raskine ugovor.

143 Ako primatelj osobnih podataka koji se prenose trećoj zemlji obavijesti voditelja obrade, na temelju klauzule 5. točke (b) priloga Odluci o standardnim ugovornim klauzulama, da mu zakonodavstvo predmetne treće zemlje ne omogućuje postupanje u skladu sa standardnim klauzulama o zaštiti podataka iz tog priloga, iz klauzule 12. navedenog priloga proizlazi da podaci koji su već preneseni u tu treću zemlju i njihove kopije moraju u cijelosti biti vraćeni ili uništeni. U svakom slučaju, klauzula 6. tog priloga sankcionira nepoštovanje tih standardnih klauzula dodjeljujući zainteresiranoj osobi pravo na naknadu pretrpljene štete.

144 Valja dodati da se, u skladu s klauzulom 4. točkom (f) priloga Odluci o standardnim ugovornim klauzulama, voditelj obrade s poslovnim nastanom u Uniji obvezuje, kada se posebne kategorije podataka mogu prenijeti trećoj zemlji koja ne pruža odgovarajuću razinu zaštite, o tome obavijestiti osobu na koju se odnose podaci prije prijenosa ili što je prije moguće nakon tog prijenosa. Ta informacija može toj osobi omogućiti da protiv voditelja obrade upotrijebi pravo na pravni lijek koje joj priznaje klauzula 3. stavak 1. tog priloga kako bi taj voditelj odgodio predviđeni prijenos, raskinuo ugovor sklopljen s primateljem osobnih podataka ili, ovisno o slučaju, od potonjeg zatražio povrat ili uništavanje prenesenih podataka.

145 Naposljetku, na temelju klauzule 4. točke (g) navedenog priloga, voditelj obrade s poslovnim nastanom u Uniji dužan je, kada ga primatelj osobnih podataka na temelju klauzule 5. točke (b) tog priloga obavijesti da je došlo do promjene u zakonodavstvu koje se na njega odnosi, a koja bi mogla imati bitan negativan učinak na jamstva i obveze iz klauzula, proslijediti tu obavijest nadležnom nadzornom tijelu ako unatoč navedenoj obavijesti odluči nastaviti s prijenosom ili ukinuti njegovu obustavu. Prenošenje takve obavijesti tom nadzornom tijelu i pravo tog tijela da izvrši reviziju primatelja osobnih podataka na temelju klauzule 8. stavka 2. tog priloga omogućuju navedenom nadzornom tijelu da provjeri treba li izvršiti obustavu ili zabranu predviđenog prijenosa kako bi se osigurala primjerena razina zaštite.

146 U tom kontekstu članak 4. Odluke o standardnim ugovornim klauzulama, tumačen u vezi s uvodnom izjavom 5. Provedbene odluke 2016/2297, potvrđuje da se Odlukom o standardnim ugovornim klauzulama ni na koji način ne sprečava nadležno nadzorno tijelo da obustavi ili zabrani, ovisno o slučaju, prijenos osobnih podataka trećoj zemlji koji se temelji na standardnim ugovornim klauzulama o zaštiti podataka koje se nalaze u prilogu toj odluci. U tom pogledu, kao što to proizlazi iz odgovora na osmo pitanje, osim ako je Komisija valjano donijela odluku o primjerenosti, nadležno nadzorno tijelo dužno je, na temelju članka 58. stavka 2. točaka (f) i (j) GDPR-a, obustaviti ili zabraniti takav prijenos ako smatra, s obzirom na sve okolnosti svojstvene tom prijenosu, da se te klauzule ne poštuju ili se ne mogu poštovati u toj trećoj zemlji i da zaštita prenesenih podataka koja se zahtijeva pravom Unije ne može biti osigurana drugim sredstvima, u slučaju da voditelj obrade ili njegov izvršitelj s poslovnim nastanom u Uniji sam nije obustavio ili okončao prijenos.

147 Kad je riječ o okolnosti, koju je istaknuo povjerenik, prema kojoj bi nadzorna tijela različitih država članica mogla donositi neujednačene odluke u vezi s prijenosima osobnih podataka takvoj trećoj zemlji, valja dodati da iz članka 55. stavka 1. i članka 57. stavka 1. točke (a) GDPR-a proizlazi da je zadaća praćenja primjene te uredbe dodijeljena, u načelu, svakom nadzornom tijelu na državnom području države članice u kojoj se nalazi. Nadalje, kako bi se izbjegle neujednačene odluke, članak 64. stavak 2. navedene uredbe predviđa mogućnost da nadzorno tijelo koje ocijeni da se prijenosi podataka trećoj zemlji općenito moraju zabraniti zatraži mišljenje Europskog odbora za zaštitu podataka (EOZP), koji, pak, na temelju članka 65. stavka 1. točke (c) te uredbe može donijeti obvezujuću odluku, među ostalim kad nadzorno tijelo ne uzme u obzir izdano mišljenje.

148 Iz stoga slijedi da odluka o standardnim ugovornim klauzulama predviđa učinkovite mehanizme na temelju kojih se u praksi može osigurati da prijenos osobnih podataka trećoj zemlji primjenom standardnih klauzula o zaštiti podataka koje se nalaze u prilogu toj odluci bude obustavljen ili zabranjen kad primatelj osobnih podataka ne poštuje navedene klauzule ili ih nije u mogućnosti poštovati.

149 S obzirom na sva prethodna razmatranja, na sedmo i jedanaesto pitanje valja odgovoriti tako da analizom Odluke o standardnim ugovornim klauzulama s obzirom na članke 7., 8. i 47. Povelje nije utvrđen nijedan element koji bi mogao utjecati na valjanost te odluke.

Četvrto, peto, deveto i deseto pitanje

150 Svojim devetim pitanjem sud koji je uputio zahtjev želi u biti znati je li i u kojoj mjeri nadzorno tijelo države članice obvezano utvrđenjima koja se nalaze u Odluci o sustavu zaštite privatnosti prema kojima Sjedinjene Američke Države osiguravaju primjerenu razinu zaštite. Svojim četvrtim, petim i desetim pitanjem taj sud želi u biti znati krše li se, s obzirom na njegova utvrđenja u pogledu prava Sjedinjenih Američkih Država, prijenosom osobnih podataka toj trećoj zemlji na temelju standardnih klauzula o zaštiti podataka koje se nalaze u prilogu Odluci o standardnim ugovornim klauzulama prava zajamčena člancima 7., 8. i 47. Povelje te u biti pita Sud osobito je li uspostavljanje pravobranitelja spomenutog u Prilogu III. Odluci o sustavu zaštite podataka u skladu s tim člankom 47.

151 Najprije valja navesti da iako povjerenikova tužba iz glavnog postupka osporava samo valjanost Odluke o standardnim ugovornim klauzulama, ta je tužba sudu koji je uputio zahtjev podnesena prije donošenja Odluke o sustavu zaštite privatnosti. Budući da svojim četvrtim i petim pitanjem taj sud općenito pita Sud o zaštiti koja se na temelju članaka 7., 8. i 47. Povelje mora osigurati u kontekstu takvog prijenosa, Sud prilikom izvršavanja svoje ocjene mora uzeti u obzir okolnosti koje proizlaze iz naknadnog donošenja Odluke o sustavu zaštite podataka. To vrijedi tim više što navedeni sud svojim desetim pitanjem izričito pita je li zaštita koja se zahtijeva tim člankom 47. osigurana posredstvom pravobranitelja spomenutog u potonjoj odluci.

152 Osim toga, iz navoda koji se nalaze u zahtjevu za prethodnu odluku proizlazi da je u glavnom postupku Facebook Ireland naveo da je Odluka o sustavu zaštite privatnosti obvezivala povjerenika u pogledu utvrđenja o primjerenosti razine zaštite koju osiguravaju Sjedinjene Američke Države i stoga o zakonitosti prijenosa osobnih podataka trećoj zemlji na temelju standardnih ugovornih klauzula koje se nalaze u Odluci o standardnim ugovornim klauzulama.

153 Međutim, kao što proizlazi iz točke 59. ove presude, u svojoj presudi od 3. listopada 2017. priloženoj zahtjevu za prethodnu odluku sud koji je uputio zahtjev istaknuo je da je bio dužan uzeti u obzir izmjene prava do kojih je došlo u razdoblju između podnošenja tužbe i pred njime održane rasprave. Tako se čini da je taj sud obvezan, kako bi riješio spor u glavnom postupku, uzeti u obzir promijenjene okolnosti koje proizlaze iz donošenja Odluke o sustavu zaštite privatnosti te njezine eventualne obvezujuće učinke.

154 Konkretno, pitanje obvezatnosti utvrđenja u Odluci o sustavu zaštite privatnosti da Sjedinjene Američke Države osiguravaju primjerenu razinu zaštite relevantno je u svrhu ocjene kako obveza, spomenutih u točkama 141. i 142. ove presude, voditelja obrade i primatelja osobnih podataka trećoj zemlji na temelju standardnih klauzula o zaštiti podataka koje se nalaze u prilogu Odluci o standardnim ugovornim klauzulama, tako i obveza nadzornog tijela da, u slučaju potrebe, obustavi ili zabrani takav prijenos.

155 Kad je riječ, naime, o obvezujućim učincima Odluke o sustavu zaštite privatnosti, članak 1. stavak 1. te odluke određuje da u svrhu članka 45. stavka 1. GDPR-a „Sjedinjene Američke Države osiguravaju odgovarajuću razinu zaštite osobnih podataka koji se prenose iz Unije organizacijama u Sjedinjenim Američkim Državama u okviru europsko-američkog sustava zaštite privatnosti”. U skladu s člankom 1. stavkom 3. navedene odluke, osobni podaci smatraju se prenesenima u okviru tog sustava kad se iz Unije prenose organizacijama u Sjedinjenim Američkim Državama koje se nalaze na popisu organizacija u sustavu zaštite privatnosti, koji vodi i objavljuje američko Ministarstvo trgovine u skladu s odjeljcima I. i III. načela navedenih u Prilogu II. toj odluci.

156 Kao što proizlazi iz sudske prakse spomenute u točkama 117. i 118. ove presude, Odluka o sustavu zaštite privatnosti obvezujuća je za nadzorna tijela jer se njome utvrđuje da Sjedinjene Američke Države jamče primjerenu razinu zaštite te je stoga njezin učinak odobravanje prijenosa osobnih podataka izvršenih u okviru europsko-američkog sustava zaštite podataka. Stoga, sve dok tu odluku Sud ne proglasi nevaljanom, nadležno nadzorno tijelo ne može obustaviti ili zabraniti prijenos osobnih podataka organizaciji u tom sustavu ako smatra, za razliku od Komisijine ocjene u navedenoj odluci, da zakonodavstvo Sjedinjenih Američkih Država kojim se uređuje pristup osobnim podacima prenesenima u okviru navedenog sustava i uporaba tih podataka od strane javnih tijela te treće zemlje za potrebe nacionalne sigurnosti, kaznenog progona ili javnog interesa ne osigurava primjerenu razinu zaštite.

157 Ipak, u skladu sa sudskom praksom navedenom u točkama 119. i 120. ove presude, nadležno nadzorno tijelo kojem osoba podnese pritužbu mora posve samostalno ispitati poštuje li predmetni prijenos osobnih podataka zahtjeve utvrđene GDPR-om i, u slučaju da prigovore koje je ta osoba istaknula kako bi osporila valjanost odluke o primjerenosti smatra utemeljenima, podnijeti tužbu nacionalnim sudovima kako bi oni uputili Sudu zahtjev za prethodnu odluku u svrhu ispitivanja valjanosti te odluke.

158 Naime, pritužbu u smislu članka 77. stavka 1. GDPR-a u kojoj osoba čiji su osobni podaci preneseni ili bi mogli biti preneseni trećoj zemlji navodi da važeće pravo i praksa u toj zemlji ne osiguravaju odgovarajuću razinu zaštite, neovisno o Komisijinu utvrđenju u odluci donesenoj na temelju članka 45. stavka 3. te uredbe, valja tumačiti na način da se ona u biti odnosi na usklađenost te odluke sa zaštitom privatnosti i temeljnih prava i sloboda pojedinaca (vidjeti analogijom, kad je riječ o članku 25. stavku 6. i članku 28. stavku 4. Direktive 95/46, presudu od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 59.).

159 U predmetnom slučaju M. Schrems u biti je od povjerenika zatražio da zabrani ili obustavi prijenos njegovih osobnih podataka s društva Facebook Ireland na Facebook Inc., koji ima poslovni nastan u Sjedinjenim Američkim Državama, zbog toga što ta treća zemlja ne osigurava primjerenu razinu zaštite. Budući da je povjerenik, po završetku istrage o navodima M. Schremsa, pokrenuo postupak pred sudom koji je uputio zahtjev, čini se da se potonji, s obzirom na podnesene dokaze i pred njime održanu kontradiktornu raspravu, pita o osnovanosti sumnji M. Schremsa u primjerenost zaštite koju osigurava navedena treća zemlja, unatoč Komisijinim naknadnim utvrđenjima u Odluci o sustavu zaštite privatnosti, što je taj sud navelo da Sudu postavi četvrto, peto i deseto prethodno pitanje.

160 Kao što je nezavisni odvjetnik naveo u točki 175. svojeg mišljenja, ta prethodna pitanja treba dakle razumjeti na način da u biti dovode u pitanje Komisijino utvrđenje u Odluci o sustavu zaštite privatnosti prema kojem Sjedinjene Američke Države osiguravaju primjerenu razinu zaštite osobnih podataka koji se iz Unije prenose toj trećoj zemlji te da stoga dovode u pitanje i valjanost te odluke.

161 S obzirom na utvrđenja navedena u točkama 121. i 157. do 160. ove presude te kako bi se sudu koji je uputio zahtjev pružio potpun odgovor valja razmotriti je li Odluka o sustavu zaštite privatnosti u skladu sa zahtjevima koji proizlaze iz GDPR-a, tumačenog u vezi s Poveljom (vidjeti analogijom presudu od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 67.).

162 Kako bi donijela odluku o primjerenosti na temelju članka 45. stavka 3. GDPR-a, Komisija mora utvrditi, pružajući valjano obrazloženje, da dotična treća zemlja doista osigurava, zbog svojeg domaćeg zakonodavstva ili međunarodnih obveza koje je preuzela, razinu zaštite temeljnih prava koja je bitno ekvivalentna onoj koja se jamči u pravnom poretku Unije (vidjeti analogijom, kad je riječ o članku 25. stavku 6. Direktive 95/46, presudu od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 96.).

Sadržaj Odluke o sustavu zaštite privatnosti

163 Komisija je u članku 1. stavku 1. Odluke o sustavu zaštite privatnosti utvrdila da Sjedinjene Američke Države osiguravaju primjerenu razinu zaštite osobnih podataka koji se prenose iz Unije organizacijama u Sjedinjenim Američkim Državama u okviru europsko-američkog sustava zaštite privatnosti, koji se sastoji, među ostalim, na temelju članka 1. stavka 2. te odluke, od načela koja je 7. srpnja 2016. izdalo američko Ministarstvo trgovine, kako je navedeno u Prilogu II. navedenoj odluci te u službenim izjavama i obvezama iz dokumenata navedenih u Prilogu I. i prilozima III. do VII. toj odluci.

164 Međutim, u točki I.5 naslovljenoj „Načela okvira europsko-američkog sustava zaštite” koja se nalazi u Prilogu II. Odluci o sustavu zaštite privatnosti također je navedeno da pridržavanje tih načela može biti ograničeno, osobito „u mjeri potrebnoj da se ispune zahtjevi u pogledu nacionalne sigurnosti, javnog interesa ili kaznenog progona”. Tako ta odluka propisuje, poput Odluke 2000/520, nadređenost tih zahtjeva nad navedenim načelima na temelju koje su samocertificirane organizacije iz SAD-a koje primaju osobne podatke iz Unije dužne u potpunosti odbaciti ta načela ako su ona u sukobu s tim zahtjevima te se, dakle, pokažu s njima nespojiva (vidjeti analogijom, kad je riječ o Odluci 2000/520, presudu od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 86.).

165 S obzirom na svoju općenitost, izuzeće iz točke I.5 Priloga II. Odluci o sustavu zaštite privatnosti na taj način omogućuje zadiranje, na temelju zahtjeva nacionalne sigurnosti, javnog interesa, ili domaćeg zakonodavstva Sjedinjenih Američkih Država, u temeljna prava osoba čiji se osobni podaci prenose ili bi se mogli prenositi iz Unije u Sjedinjene Američke Države (vidjeti analogijom, kad je riječ o Odluci 2000/520, presudu od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 87.). Konkretnije, i kako je utvrđeno u Odluci o sustavu zaštite privatnosti, takvo zadiranje može biti rezultat pristupa osobnim podacima prenesenima iz Unije u Sjedinjene Američke Države i uporabe tih podataka od strane američkih javnih tijela u okviru nadzornih programa PRISM i UPSTREAM koji se temelje na članku 702. FISA-e te na Izvršnom nalogu br. 12333.

166 U tom kontekstu Komisija je u uvodnim izjavama 67. do 135. Odluke o sustavu zaštite privatnosti ocijenila ograničenja i zaštitne mjere predviđene u zakonodavstvu Sjedinjenih Američkih Država, osobito u članku 702. FISA-e, Izvršnom nalogu br. 12333 i PPD-28, u vezi s pristupom američkih javnih tijela osobnim podacima prenesenima u okviru europsko-američkog sustava zaštite privatnosti i uporabom tih podataka za potrebe nacionalne sigurnosti, kaznenog progona i u druge svrhe u općem interesu.

167 Slijedom te ocjene, Komisija je u uvodnoj izjavi 136. te odluke utvrdila da „Sjedinjene Američke Države osiguravaju odgovarajuću razinu zaštite osobnih podataka koji se prenose iz Unije samocertificiranim organizacijama u SAD-u" te je u uvodnoj izjavi 140. navedene odluke ocijenila da će „na temelju dostupnih informacija o pravnom poretku SAD-a […] svako zadiranje američkih javnih tijela u temeljna prava osoba čiji se podaci prenose iz Unije u Sjedinjene Američke Države u okviru europsko-američkog sustava zaštite privatnosti radi nacionalne sigurnosti, kaznenog progona ili drugih javnih interesa i povezana ograničenja koja se određuju samocertificiranim organizacijama u pogledu njihovog pridržavanja Načela biti ograničena na ono što je nužno za postizanje predmetnog legitimnog cilja te da postoji djelotvorna pravna zaštita od takvog zadiranja".

Utvrđivanje primjerene razine zaštite

168 S obzirom na elemente koje Komisija navodi u Odluci o sustavu zaštite privatnosti te one koje je sud koji je uputio zahtjev utvrdio u glavnom postupku, taj sud dvoji o tome osigurava li pravo Sjedinjenih Američkih Država doista primjerenu razinu zaštite koja se zahtijeva člankom 45. GDPR-a, u vezi s temeljnim pravima zajamčenima člancima 7., 8. i 47. Povelje. Konkretno, navedeni sud smatra da pravo te treće zemlje ne predviđa ograničenja i zaštitne mjere koji su potrebni u pogledu zadiranja dopuštenog njezinim domaćim zakonodavstvom niti osigurava djelotvornu sudsku zaštitu protiv takvog zadiranja. U potonjem smislu taj sud dodaje da uspostavljanje pravobranitelja za sustav zaštite privatnosti ne može nadomjestiti te praznine jer se taj pravobranitelj ne može izjednačiti sa sudom, u smislu članka 47. Povelje.

169 Kad je riječ, kao prvo, o člancima 7. i 8. Povelje, koji doprinose razini zaštite koja se zahtijeva u Uniji, a čije poštovanje Komisija mora utvrditi prije nego što donese odluku o primjerenosti na temelju članka 45. stavka 1. GDPR-a, valja podsjetiti da članak 7. Povelje svakoj osobi jamči poštovanje njezina privatnog i obiteljskog života, doma i komuniciranja. Kad je riječ o članku 8. stavku 1. Povelje, on svima daje pravo na zaštitu osobnih podataka koji se na njega ili nju odnose.

170 Tako pristup osobnim podacima fizičke osobe radi njihova čuvanja ili uporabe utječe na temeljno pravo te osobe na poštovanje njezina privatnog života, zajamčeno člankom 7. Povelje, pri čemu se to pravo odnosi na svaku informaciju u vezi s određenom ili odredivom fizičkom osobom. Navedene obrade podataka obuhvaćene su i člankom 8. Povelje jer predstavljaju obradu osobnih podataka u smislu tog članka i stoga nužno moraju ispunjavati zahtjeve za zaštitu podataka predviđene navedenim člankom (vidjeti u tom smislu presude od 9. studenoga 2010., Volker und Markus Schecke i Eifert, C-92/09 i C-93/09, EU:C:2010:662, t. 49. i 52. i od 8. travnja 2014., Digital Rights Ireland i dr., C-293/12 i C-594/12, EU:C:2014:238, t. 29. i mišljenje 1/15 (Sporazum PNR EU-Kanada) od 26. srpnja 2017., EU:C:2017:592, t. 122. i 123.).

171 Sud je već ranije presudio da dostavljanje osobnih podataka trećoj osobi, primjerice javnom tijelu, predstavlja zadiranje u temeljno pravo predviđeno člankom 7. i 8. Povelje, neovisno o tome na koji se način dostavljene informacije kasnije rabe. Isto vrijedi i za čuvanje osobnih podataka te za pristup tim podacima kako bi se njima koristila javna tijela, te je u tom pogledu nevažno imaju li dotične informacije o privatnom životu osjetljiv karakter, odnosno jesu li zainteresirane osobe zbog tog zadiranja pretrpjele eventualne neugodnosti (vidjeti, u tom smislu, presude od 20. svibnja 2003.,

Österreichischer Rundfunk i dr., C-465/00, C-138/01 i C-139/01, EU:C:2003:294, t. 74. i 75.; od 8. travnja 2014., Digital Rights Ireland i dr., C-293/12 i C-594/12, EU:C:2014:238, t. 33. do 36., i mišljenje 1/15 (Sporazum PNR EU-Kanada) od 26. srpnja 2017., EU:C:2017:592, t. 124. i 126.).

172 Međutim, prava priznata člancima 7. i 8. Povelje nisu apsolutna prava, nego ih treba uzeti u obzir s obzirom na njihovu funkciju u društvu (vidjeti u tom smislu presude od 9. studenoga 2010., Volker und Markus Schecke i Eifert, C-92/09 i C-93/09, EU:C:2010:662, t. 48. i navedenu sudsku praksu i od 17. listopada 2013., Schwarz, C-291/12, EU:C:2013:670, t. 33. i navedenu sudsku praksu i mišljenje 1/15 (Sporazum PNR EU-Kanada) od 26. srpnja 2017., EU:C:2017:592, t. 136.).

173 U tom smislu treba također reći da se u skladu s člankom 8. stavkom 2. Povelje osobni podaci moraju obrađivati, među ostalim, „u utvrđene svrhe i na temelju suglasnosti osobe o kojoj je riječ, ili na nekoj drugoj legitimnoj osnovi utvrđenoj zakonom”.

174 Nadalje, u skladu s prvom rečenicom članka 52. stavka 1. Povelje, svako ograničavanje pri ostvarivanju prava i sloboda priznatih Poveljom mora biti predviđeno zakonom i mora poštovati bit tih prava i sloboda. Prema drugoj rečenici članka 52. stavka 1. Povelje, u skladu s načelom proporcionalnosti, ograničenja tih prava i sloboda moguća su samo ako su potrebna i ako zaista odgovaraju ciljevima u općem interesu koje priznaje Unija ili potrebi zaštite prava i sloboda drugih osoba.

175 U tom smislu valja dodati da zahtjev da svako ograničenje ostvarivanja temeljnih prava mora biti predviđeno zakonom znači da se u samoj pravnoj osnovi kojom se dopušta zadiranje u ta prava mora definirati doseg ograničenja ostvarivanja dotičnog prava (vidjeti mišljenje 1/15 (Sporazum PNR EU-Kanada) od 26. srpnja 2017., EU:C:2017:592, t. 139. i navedenu sudsku praksu).

176 Naposljetku, kako bi se ispunio zahtjev proporcionalnosti prema kojem odstupanja od zaštite osobnih podataka i njezina ograničenja moraju biti u granicama onog što je strogo nužno, predmetni propis kojim se zadire u prava mora predvidjeti jasna i precizna pravila kojima se uređuju doseg i primjena predmetne mjere i nalažu minimalni zahtjevi, tako da osobe čiji su podaci preneseni raspolažu dostatnim jamstvima koja omogućuju djelotvornu zaštitu njihovu osobnih podataka od rizika zlouporabe. On mora osobito navesti u kojim se okolnostima i pod kojim uvjetima može donijeti mjera kojom se predviđa obrada takvih podataka, na taj način osiguravajući da zadiranje bude ograničeno na ono što je strogo nužno. Nužnost posjedovanja takvih jamstava još je značajnija kad su osobni podaci podvrgnuti automatskoj obradi (vidjeti u tom smislu mišljenje 1/15 (Sporazum PNR EU-Kanada) od 26. srpnja 2017., EU:C:2017:592, t. 140. i 141. i navedenu sudsku praksu).

177 U tu svrhu članak 45. stavak 2. točka (a) GDPR-a pojašnjava da u okviru svoje ocjene primjerenosti razine zaštite koju osigurava treća zemlja Komisija osobito vodi računa o „postojanju djelotvornih i provedivih prava ispitanika” čiji se osobni podaci prenose.

178 U predmetnom slučaju Komisijino utvrđenje u Odluci o sustavu zaštite privatnosti prema kojem Sjedinjene Američke Države osiguravaju razinu zaštite koja je bitno ekvivalentna onoj koju u okviru Unije jamči GDPR, tumačen u vezi s člancima 7. i 8. Povelje, dovedeno je u pitanje, među ostalim, zbog toga što zadiranje koje proizlazi iz nadzornih programa utemeljenih na članku 702. FISA-e i Izvršnom nalogu br. 12333 nije podvrgnuto zahtjevima kojima se, na temelju načela proporcionalnosti, osigurava razina zaštite bitno ekvivalentna onoj zajamčenoj člankom 52. stavkom 1. drugom rečenicom Povelje. Stoga valja ispitati provode li se ti nadzorni programi u skladu s takvim zahtjevima a da pritom nije potrebno prethodno provjeriti poštuje li ta treća zemlja zahtjeve koji su bitno ekvivalentni onima predviđenima prvom rečenicom članka 52. stavka 1. Povelje.

179 U tom pogledu, kad je riječ o nadzornim programima koji se temelje na članku 702. FISA-e, Komisija je u uvodnoj izjavi 109. Odluke o sustavu zaštite privatnosti utvrdila da, prema navedenom članku, „FISC ne odobrava pojedinačne mjere nadzora, već odobrava programe nadzora (npr. PRISM, UPSTREAM) na temelju godišnjih certifikacija koje pripremaju Glavni državni odvjetnik i direktor

Nacionalne obavještajne službe". Kao što to proizlazi iz iste uvodne izjave, cilj kontrole koju provodi FISC je dakle provjeriti odgovaraju li ti nadzorni programi cilju prikupljanja stranih obavještajnih informacija, ali se ne odnosi na pitanje „jesu li osobe čiji se podaci prikupljaju radi pribavljanja stranih obavještajnih podataka ispravno odabrane".

180 Stoga proizlazi da u članku 702. FISA-e uopće nisu propisana ograničenja u njemu sadržanih ovlasti za provođenje programa nadzora radi prikupljanja stranih obavještajnih informacija kao ni zaštitne mjere za osobe koje nisu američki državljani, a na koje bi se ti programi mogli odnositi. U tim okolnostima i kako je nezavisni odvjetnik u biti naveo u točkama 291., 292. i 297. svojeg mišljenja, taj članak ne može osigurati razinu zaštite koja je bitno ekvivalentna onoj zajamčenoj Poveljom, kako je tumači sudska praksa navedena u točkama 175. i 176. ove presude, prema kojoj sama pravna osnova kojom se dopušta zadiranje u temeljna prava mora, u skladu s načelom proporcionalnosti, definirati doseg ograničenja ostvarivanja dotičnog prava i predvidjeti jasna i precizna pravila kojima se uređuju doseg i primjena predmetne mjere i nalažu minimalni zahtjevi.

181 U skladu s utvrđenjima koja se nalaze u Odluci o sustavu zaštite privatnosti, točno je da se nadzorni programi koji se temelje na članku 702. FISA-e moraju provoditi uz poštovanje zahtjeva koji rezultiraju iz PPD-28. Međutim, iako je Komisija u uvodnim izjavama 69. i 77. Odluke o sustavu zaštite privatnosti istaknula da su zahtjevi iz PPD-28 obvezujući za američke obavještajne službe, američka vlada je u odgovoru na pitanje Suda odgovorila da PPD-28 osobama na koje se odnose podaci ne dodjeljuje prava na koja se u postupku pred sudovima mogu pozivati protiv američkih tijela. Stoga ta odluka ne može osigurati razinu zaštite koja je bitno ekvivalentna onoj koja proizlazi iz Povelje, što je u suprotnosti s onime što se zahtijeva člankom 45. stavkom 2. točkom (a) GDPR-a, a prema kojem utvrđivanje te razine ovisi, među ostalim, o postojanju učinkovitih i provedivih prava osoba čiji su podaci preneseni predmetnoj trećoj zemlji.

182 Kad je riječ o nadzornim programima koji se temelje na Izvršnom nalogu br. 12333, iz spisa kojim raspolaže Sud proizlazi da tim nalogom ni američkim tijelima nisu dodijeljena prava na koja se mogu pozivati pred sudovima.

183 Valja dodati da PPD-28, s kojim mora biti usklađena primjena programa obuhvaćenih dvjema prethodnim točkama, omogućuje provođenje „‚skupno[g....]' prikupljanj[a...] relativno velike količine elektronički prikupljenih obavještajnih informacija ili podataka u okolnostima u kojima se obavještajna zajednica ne može koristiti identifikatorom povezanim s određenom ciljanom osobom […]", kao što je precizirano u dopisu od 21. lipnja 2016. Ureda direktora nacionalne obavještajne službe (Office of the Director of National Intelligence) američkom ministarstvu trgovine i upravi za međunarodnu trgovinu, koji se nalazi u Prilogu VI. Odluci o sustavu zaštite privatnosti. Međutim, ta mogućnost na temelju koje se može, u okviru nadzornih programa temeljenih na Izvršnom nalogu br. 12333, pristupiti podacima koji su „u prijelazu" prema Sjedinjenim Američkim Državama – a da taj pristup pritom nije podložan nikakvom sudskom nadzoru – ni u kojem slučaju ne određuje na dovoljno jasan i precizan način doseg takvog skupnog prikupljanja osobnih podataka.

184 Stoga proizlazi da ni članak 702. FISA-e ni Izvršni nalog br. 12333, tumačeni u vezi s PPD-om 28, ne odgovaraju minimalnim zahtjevima koji su u pravu Unije povezani s načelom proporcionalnosti, tako da nije moguće utvrditi da su nadzorni programi koji se temelje na tim odredbama ograničeni na ono što je strogo nužno.

185 U tim okolnostima ograničenja zaštite osobnih podataka koja proizlaze iz domaćih propisa Sjedinjenih Američkih Država u vezi s pristupom takvim podacima prenesenima iz Unije u Sjedinjene Američke Države i njihovom uporabom od strane američkih tijela te koja je Komisija ocijenila u Odluci o sustavu zaštite privatnosti nisu uređena tako da bi ispunjavala zahtjeve koji su bitno ekvivalentni onima koji se na temelju prava Unije zahtijevaju člankom 52. stavkom 1. drugom rečenicom Povelje.

186 Kad je riječ, kao drugo, o članku 47. Povelje, koji također pridonosi razini zaštite koja se zahtijeva u okviru Unije, a čije poštovanje mora utvrditi Komisija prije nego što donese odluku o primjerenosti na temelju članka 45. stavka 1. GDPR-a, valja podsjetiti da prvi stavak tog članka 47. nalaže da svaka osoba čija su prava i slobode zajamčeni pravom Unije povrijeđeni ima pravo na djelotvoran pravni lijek pred sudom uz poštovanje uvjeta predviđenih u tom članku. U skladu s drugim stavkom navedenog članka, svatko ima pravo da neovisni i nepristrani sud ispita njegov slučaj.

187 Prema ustaljenoj sudskoj praksi, sâmo postojanje djelotvornog sudskog nadzora radi osiguranja poštovanja Unijinih pravnih odredaba svojstveno je postojanju pravne države. Tako propis koji pojedincima ne pruža nikakvu mogućnost korištenja pravnim sredstvima radi pristupa osobnim podacima koji se na njih odnose, ili radi ispravka ili brisanja takvih podataka, ne poštuje bitan sadržaj temeljnog prava na djelotvornu sudsku zaštitu, kao što je to propisano u članku 47. Povelje (presuda od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650, t. 95. i navedena sudska praksa).

188 U tom smislu članak 45. stavak 2. točka (a) GDPR-a zahtijeva da u okviru svoje ocjene primjerenosti razine zaštite koju pruža treća zemlja Komisija vodi računa među ostalim o postojanju „učinkovite upravne i sudske zaštite ispitanika čiji se osobni podaci prenose”. Uvodna izjava 104. GDPR-a u tom pogledu ističe da bi treća zemlja „trebala […] osigurati učinkovit neovisan nadzor zaštite podataka te mehanizme suradnje s tijelima država članica za zaštitu podataka” i precizira da bi „ispitanici trebali imati učinkovita i ostvariva prava te učinkovitu upravnu i sudsku zaštitu”.

189 Postojanje takvih mogućnosti djelotvorne pravne zaštite u predmetnoj trećoj zemlji osobito je važno u kontekstu prijenosa osobnih podataka toj trećoj zemlji jer se, kao što to proizlazi iz uvodne izjave 116. GDPR-a, osobe na koje se odnose podaci mogu suočiti s činjenicom da upravna i sudska tijela država članica nemaju na raspolaganju dovoljne ovlasti i sredstva da bi učinkovito postupala po pritužbama tih osoba u vezi s navodno nezakonitom obradom njihovih tako prenesenih podataka u toj trećoj zemlji, što te osobe može primorati da se obrate nacionalnim tijelima i sudovima te treće zemlje.

190 Komisijino utvrđenje u Odluci o sustavu zaštite privatnosti da Sjedinjene Američke Države osiguravaju razinu zaštite koja je bitno ekvivalentna onoj zajamčenoj člankom 47. Povelje, u predmetnom je slučaju dovedeno u pitanje među ostalim zbog toga što uspostavljanje pravobranitelja za sustav zaštite privatnosti ne može nadomjestiti praznine koje je sama Komisija utvrdila kad je riječ o sudskoj zaštiti osoba čiji su osobni podaci preneseni toj trećoj zemlji.

191 U tom pogledu Komisija je u uvodnoj izjavi 115. Odluke o sustavu zaštite privatnosti navela da „iako prema tome pojedinci, uključujući osobe iz [Unije] čiji se podaci obrađuju, imaju na raspolaganju različite oblike pravne zaštite ako su bili predmetom nezakonitog (elektroničkog) nadzora za potrebe nacionalne sigurnosti, očito je i da nisu obuhvaćene barem neke pravne osnove koje američka obavještajna tijela (npr. Izvršni nalog br. 12333) mogu upotrijebiti”. Tako je u pogledu Izvršnog naloga br. 12333 Komisija u navedenoj uvodnoj izjavi 115. istaknula nepostojanje bilo kakvih pravnih sredstava. Prema sudskoj praksi navedenoj u točki 187. ove presude, takva praznina u sudskoj zaštiti u pogledu zadiranja povezanih s obavještajnim programima koji se temelje na tom predsjedničkom nalogu protivi se zaključku, poput onog Komisijinog u Odluci o sustavu zaštite privatnosti, da pravo Sjedinjenih Američkih Država osigurava razinu zaštite koja je bitno ekvivalentna onoj zajamčenoj člankom 47. Povelje.

192 Nadalje, kad je riječ kako o nadzornim programima koji se temelje na članku 702. FISA-e tako i onima koji se temelje na Izvršnom nalogu br. 12333, u točkama 181. i 182. ove presude navedeno je da ni PPD-28 ni Izvršni nalog br. 12333 dotičnim osobama ne dodjeljuju prava koja bi se protiv američkih tijela mogla ostvarivati pred sudovima, tako da te osobe na raspolažu pravom na djelotvoran pravni lijek.

193 Komisija je ipak u uvodnim izjavama 115. i 116. Odluke o sustavu zaštite privatnosti utvrdila da se može smatrati da Sjedinjene Američke Države osiguravaju razinu zaštite bitno ekvivalentnu onoj zajamčenoj člankom 47. Povelje zbog postojanja mehanizma pravobranitelja koji su uspostavila američka tijela, kako je opisano u dopisu koji je 7. srpnja 2016. američki ministar vanjskih poslova uputio povjerenici Europske unije za pravosuđe, zaštitu potrošača i ravnopravnost spolova, koji se nalazi u Prilogu III. toj odluci, te zbog prirode zadaće povjerene pravobranitelju, u predmetnom slučaju „višem koordinatoru međunarodne diplomacije u području informacijske tehnologije".

194 Razmatranje pitanja može li mehanizam pravobranitelja koji je predviđen Odlukom o sustavu zaštite privatnosti nadoknaditi ograničenja prava na sudsku zaštitu koja je utvrdila Komisija mora, u skladu sa zahtjevima iz članka 47. Povelje i sudske prakse iz točke 187. ove presude, polaziti od načela da pojedinci moraju imati mogućnost korištenja pravnim sredstvima pred neovisnim i nepristranim sudom radi pristupa osobnim podacima koji se na njih odnose ili ispravka ili brisanja takvih podataka.

195 Međutim, u dopisu navedenom u točki 193. ove presude pravobranitelj za sustav zaštite privatnosti, iako opisan na način da je „neovisan o obavještajnoj zajednici", predstavljen je tako da „izravno izvješćuje ministra vanjskih poslova koji će pravobranitelju osigurati objektivno obavljanje dužnosti, neovisno o bilo kakvom neprimjerenom utjecaju koji bi mogao imati učinka na odgovor koji treba pružiti". Nadalje, osim činjenice da, kao što je Komisija utvrdila u uvodnoj izjavi 116. te odluke, pravobranitelja imenuje ministar vanjskih poslova te je on sastavni dio američkog ministarstva vanjskih poslova, navedena odluka ne sadržava, kao što je nezavisni odvjetnik naveo u točki 337. svojeg mišljenja, nikakav navod prema kojem se na razrješenje pravobranitelja s njegove dužnosti ili opoziv njegova imenovanja primjenjuju posebna jamstva, što može dovesti u pitanje njegovu neovisnost u odnosu na izvršnu vlast (vidjeti u tom smislu presudu od 21. siječnja 2020., Banco de Santander, C-274/14, EU:C:2020:17, t. 60. i 63. i navedenu sudsku praksu).

196 Isto tako, kao što je nezavisni odvjetnik istaknuo u točki 338. svojeg mišljenja, iako je u uvodnoj izjavi 120. Odluke o sustavu zaštite privatnosti navedeno da se američka vlada obvezala da će predmetna sastavnica obavještajnih službi biti dužna ispraviti svaku povredu primjenjivih pravnih pravila koju utvrdi pravobranitelj za sustav zaštite privatnosti, navedena odluka ne sadržava nikakav navod da će pravobranitelj biti ovlašten donositi obvezujuće odluke u vezi s tim službama niti se u njoj navode zakonske zaštitne mjere kojima je popraćena ta obveza američke vlade, a na koje se mogu pozvati osobe na koje se odnose podaci.

197 Mehanizam pravobranitelja predviđen Odlukom o sustavu zaštite privatnosti stoga ne pruža pravno sredstvo pred tijelom koje osobama čiji se podaci prenose u Sjedinjene Američke Države pruža zaštitne mjere bitno ekvivalentne onima koje se zahtijevaju člankom 47. Povelje.

198 Stoga je Komisija, utvrdivši u članku 1. stavku 1. Odluke o sustavu zaštite privatnosti da Sjedinjene Američke Države osiguravaju primjerenu razinu zaštite osobnih podataka prenesenih iz Unije organizacijama u toj trećoj zemlji u okviru europsko-američkog sustava zaštite privatnosti, povrijedila zahtjeve iz članka 45. stavka 1. GDPR-a, u vezi s člancima 7., 8. i 47. Povelje.

199 Iz toga slijedi da članak 1. Odluke o sustavu zaštite privatnosti nije u skladu s člankom 45. stavkom 1. GDPR-a, tumačenim u vezi s člancima 7., 8. i 47. Povelje, te je zbog toga nevaljan.

200 Budući da je članak 1. Odluke o sustavu zaštite privatnosti neodvojiv od njezinih članaka 2. do 6. te od njezinih priloga, njegova nevaljanost utječe na valjanost te odluke u cjelini.

201 S obzirom na sva prethodna razmatranja, valja zaključiti da je Odluka o sustavu zaštite privatnosti nevaljana.

202 Kad je riječ o tome treba li održati na snazi učinke te odluke kako bi se izbjegao nastanak pravne praznine (vidjeti u tom smislu presudu od 28. travnja 2016., Borealis Polyolefine i dr., C-191/14, C-192/14, C-295/14, C-389/14 i C-391/14 do C-393/14, EU:C:2016:311, t. 106.), valja u svakom slučaju primijetiti da, s obzirom na članak 49. GDPR-a, poništenje odluke o primjerenosti poput Odluke o sustavu zaštite privatnosti ne može dovesti do takve pravne praznine. Naime, tim se člankom precizno utvrđuju uvjeti u kojima može doći do prijenosa osobnih podataka trećoj zemlji kad ne postoji odluka o primjerenosti na temelju članka 45. stavka 3. navedene uredbe ili odgovarajuće zaštitne mjere na temelju članka 46. te uredbe.

Troškovi

203 Budući da ovaj postupak ima značaj prethodnog pitanja za stranke glavnog postupka pred sudom koji je uputio zahtjev, na tom je sudu da odluči o troškovima postupka. Troškovi podnošenja očitovanja Sudu, koji nisu troškovi spomenutih stranaka, ne nadoknađuju se.

Slijedom navedenoga, Sud (veliko vijeće) odlučuje:

1. **Članak 2. stavke 1. i 2. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) treba tumačiti na način da je područjem primjene te uredbe obuhvaćen prijenos osobnih podataka izvršen u komercijalne svrhe s gospodarskog subjekta s poslovnim nastanom u državi članici drugom gospodarskom subjektu s poslovnim nastanom u trećoj zemlji, bez obzira na to što tijekom ili nakon tog prijenosa te podatke mogu obrađivati tijela predmetne treće zemlje u svrhu javne sigurnosti, obrane ili nacionalne sigurnosti.**

2. **Članak 46. stavak 1. i članak 46. stavak 2. točku (c) Uredbe 2016/679 valja tumačiti tako da odgovarajuće zaštitne mjere, provediva prava i djelotvorni pravni lijekovi koji se zahtijevaju tim odredbama moraju osigurati da prava osoba čiji se osobni podaci prenose trećoj zemlji na temelju standardnih klauzula o zaštiti podataka uživaju razinu zaštite koja je bitno ekvivalentna onoj zajamčenoj u okviru Europske unije tom uredbom, tumačenom u vezi s Poveljom Europske unije o temeljnim pravima. U tom smislu ocjena razine zaštite koja se osigurava u kontekstu takvog prijenosa mora osobito uzeti u obzir kako ugovorne odredbe koje su ugovorili voditelj obrade ili izvršitelj obrade s poslovnim nastanom u Europskoj uniji i primatelj podataka s poslovnim nastanom u predmetnoj trećoj zemlji tako i, kad je riječ o eventualnom pristupu javnih tijela te treće zemlje tako prenesenim osobnim podacima, relevantne elemente njezina pravnog sustava, osobito one navedene u članku 45. stavku 2. navedene uredbe.**

3. **Članak 58. stavak 2. točke (f) i (j) Uredbe 2016/679 treba tumačiti na način da je nadležno nadzorno tijelo, osim ako postoji odluka o primjerenosti koju je Europska komisija valjano donijela, dužno obustaviti ili zabraniti prijenos podataka trećoj zemlji na temelju standardnih klauzula o zaštiti podataka koje je donijela Komisija kada to nadzorno tijelo smatra, u vezi sa svim okolnostima tog prijenosa, da te klauzule nisu ili ne mogu biti poštovane u toj trećoj zemlji i da zaštita prenesenih podataka koja se zahtijeva pravom Unije, osobito člancima 45. i 46. te uredbe i Poveljom o temeljnim pravima, ne može biti osigurana drugim sredstvima, ako voditelj obrade ili izvršitelj obrade s poslovnim nastanom u Uniji sam nije obustavio prijenos ili ga okončao.**

4. **Analizom Odluke Komisije 2010/87/EU od 5. veljače 2010. o standardnim ugovornim klauzulama za prijenos osobnih podataka obrađivačima u trećim zemljama u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća, kako je izmijenjena Provedbenom**

odlukom Komisije (EU) 2016/2297 od 16. prosinca 2016., s obzirom na članke 7., 8. i 47. Povelje o temeljnim pravima, nije utvrđen nijedan element koji bi mogao utjecati na valjanost te odluke.

5. **Provedbena odluka Komisije (EU) 2016/1250 od 12. srpnja 2016. o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća nevaljana je.**

Potpisi