Zbirka odločb sodne prakse

SODBA SODIŠČA (veliki senat)

z dne 16. julija 2020 *

„Predhodno odločanje – Varstvo posameznikov pri obdelavi osebnih podatkov – Listina Evropske unije o temeljnih pravicah – Členi 7, 8 in 47 – Uredba (EU) 2016/679 – Člen 2(2) – Področje uporabe – Prenosi osebnih podatkov v tretjo državo v komercialne namene – Člen 45 – Sklep Komisije o ustreznosti – Člen 46 – Prenosi, za katere se uporabljajo ustrezni zaščitni ukrepi – Člen 58 – Pooblastila nadzornih organov – Obdelava prenesenih podatkov, ki jo javni organi tretje države izvajajo zaradi nacionalne varnosti – Presoja ustreznosti ravni varstva, ki se zagotavlja v tretji državi – Sklep 2010/87/EU – Standardna določila o varstvu za prenos osebnih podatkov v tretje države – Ustrezni zaščitni ukrepi, ki jih zagotovi upravljavec – Veljavnost – Izvedbeni sklep (EU) 2016/1250 – Ustreznost varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA – Veljavnost – Pritožba fizične osebe, katere podatki so bili iz Evropske unije preneseni v Združene države“

V zadevi C-311/18,

katere predmet je predlog za sprejetje predhodne odločbe na podlagi člena 267 PDEU, ki ga je vložilo High Court (višje sodišče, Irska) z odločbo z dne 4. maja 2018, ki je na Sodišče prispela 9. maja 2018, v postopku

Data Protection Commissioner

proti

Facebook Ireland Ltd,

Maximillian Schrems,

ob udeležbi

The United States of America,

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

SODIŠČE (veliki senat),

v sestavi K. Lenaerts, predsednik, R. Silva de Lapuerta, podpredsednica, A. Arabadjiev, predsednik senata, A. Prechal, predsednica senata, M. Vilaras, M. Safjan, S. Rodin, P. G. Xuereb, predsedniki senata, L. S. Rossi, predsednica senata, I. Jarukaitis, predsednik senata, M. Ilešič, T. von Danwitz (poročevalec) in D. Šváby, sodniki,

* Jezik postopka: angleščina.

generalni pravobranilec: H. Saugmandsgaard Øe,

sodna tajnica: C. Strömholm, administratorka,

na podlagi pisnega postopka in obravnave z dne 9. julija 2019,

ob upoštevanju stališč, ki so jih predložili:

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

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

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

– za The United States of America E. Barrington, SC, S. Kingston, BL, ter S. Barton in B. Walsh, solicitors,

– za Electronic Privacy Information Centre S. Lucey, solicitor, G. Gilmore in A. Butler, BL, ter C. O'Dwyer, SC,

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

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

– za Irsko A. Joyce in M. Browne, agenta, skupaj z D. Fennellyjem, BL,

– za belgijsko vlado J.-C. Halleux in P. Cottin, agenta,

– za češko vlado M. Smolek, J. Vláčil, O. Serdula in A. Kasalická, agenti,

– za nemško vlado J. Möller, D. Klebs in T. Henze, agenti,

– za francosko vlado A.-L. Desjonquères, agentka,

– za nizozemsko vlado C. S. Schillemans, K. Bulterman in M. Noort, agenti,

– za avstrijsko vlado J. Schmoll in G. Kunnert, agenta,

– za poljsko vlado B. Majczyna, agent,

– za portugalsko vlado L. Inez Fernandes, A. Pimenta in C. Vieira Guerra, agenti,

– za vlado Združenega kraljestva S. Brandon in D. Guðmundsdóttir, agenta, skupaj z J. Holmesom, QC, in C. Knightom, barrister,

– za Evropski parlament M. J. Martínez Iglesias in A. Caiola, agenta,

– za Evropsko komisijo D. Nardi, H. Krämer in H. Kranenborg, agenti,

– za Evropski odbor za varstvo podatkov (EOVP) A. Jelinek in K. Behn, agenta,

po predstavitvi sklepnih predlogov generalnega pravobranilca na obravnavi 19. decembra 2019

izreka naslednjo

Sodbo

1 Predlog za sprejetje predhodne odločbe se v bistvu nanaša na

– razlago člena 3(2), prva alinea, členov 25 in 26 ter člena 28(3) Direktive Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 15, str. 355) v povezavi s členom 4(2) PEU ter členi 7, 8 in 47 Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina),

– razlago in veljavnost Sklepa Komisije z dne 5. februarja 2010 o standardnih pogodbenih klavzulah za prenos osebnih podatkov obdelovalcem s sedežem v tretjih državah v skladu z Direktivo 95/46 (2010/87/EU) (UL 2010, L 39, str. 5), kakor je bil spremenjen z Izvedbenim sklepom Komisije (EU) 2016/2297 z dne 16. decembra 2016 (UL 2016, L 344, str. 100, v nadaljevanju: Sklep SPK), ter

– razlago in veljavnost Izvedbenega sklepa Komisije (EU) 2016/1250 z dne 12. julija 2016 na podlagi Direktive 95/46 o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA (UL 2016, L 207, str. 1, v nadaljevanju: Sklep o zasebnostnem ščitu).

2 Ta predlog je bil vložen v okviru spora med Data Protection Commissioner (pooblaščenec za varstvo podatkov, Irska, v nadaljevanju: pooblaščenec) ter družbo Facebook Ireland Ltd in Maximillianom Schremsom glede pritožbe, ki jo je ta vložil v zvezi s tem, da je družba Facebook Ireland njegove osebne podatke prenesla na družbo Facebook Inc. v Združenih državah.

Pravni okvir

Direktiva 95/46

3 Člen 3(2) Direktive 95/46, naslovljen „Področje uporabe“, je določal:

„Ta direktiva se ne uporablja za obdelavo osebnih podatkov:

– med dejavnostjo, ki ne sodi na področje uporabe zakonodaje Skupnosti, kot so tiste, opredeljene v naslovih V in VI Pogodbe o Evropski uniji, in v vsakem primeru v postopkih obdelave v zvezi z javno varnostjo, obrambo, državno varnostjo (vključno z gospodarsko blaginjo države, kadar se postopek obdelave nanaša na zadeve državne varnosti) in pri dejavnostih države na področju kazenskega prava,

[…]“

4 Člen 25 te direktive je določal:

„1. Države članice predvidijo, da se lahko prenos osebnih podatkov […] v tretjo državo izvede le, če brez poseganja v skladnost z nacionalnimi določbami, ki so sprejete v skladu z drugimi določbami te direktive, ta tretja država zagotovi ustrezno raven varstva.

2. Ustreznost ravni varstva, ki jo nudi tretja država, se oceni glede na vse okoliščine, ki so povezane s postopkom prenosa ali z nizom postopkov prenosa podatkov; […]

[…]

6. Komisija lahko v skladu s postopkom iz člena 31(2) ugotovi, da tretja država zagotavlja ustrezno raven varstva v smislu odstavka 2 tega člena zaradi svoje domače zakonodaje ali mednarodnih obveznosti, ki jih je prevzela, predvsem na podlagi zaključka pogajanj iz odstavka 5, za zaščito zasebnega življenja in temeljnih svoboščin in pravic posameznikov.

Države članice sprejmejo ukrepe, potrebne za uskladitev s sklepom Komisije.“

5 Člen 26(2) in (4) navedene direktive je določal:

„2. Brez poseganja v odstavek 1 lahko država članica dovoli prenos ali niz prenosov osebnih podatkov v tretjo državo, ki ne zagotavlja ustrezne ravni varstva v smislu člena 25(2), kadar upravljavec navede ustrezne zaščitne ukrepe glede varstva zasebnosti ter temeljnih pravic in svoboščin posameznikov in glede uresničevanja ustreznih pravic; takšni zaščitni ukrepi lahko predvsem izhajajo iz ustreznih pogodbenih klavzul.

[…]

4. Kadar Komisija v skladu s postopkom iz člena 31(2) odloči, da nekatera standardna pogodbena določila nudijo zadostno zaščito iz odstavka 2, države članice sprejmejo potrebne ukrepe za uskladitev z odločitvijo Komisije.“

6 Člen 28(3) te direktive je določal:

„Vsakemu organu se podeli predvsem:

– preiskovalna pooblastila, kakršna so pooblastila za dostop do podatkov, ki sestavljajo vsebino postopkov obdelave, in pooblastila za zbiranje vseh informacij, ki so potrebne za izvajanje njegovih nadzornih nalog,

– učinkovita pooblastila za posredovanje, kakšna so npr. dajanje mnenj pred izvajanjem postopkov obdelave v skladu s členom 20 in zagotavljanje ustrezne objave takih mnenj, odrejanje blokiranja, izbrisa ali uničenja podatkov, naložitev začasne ali dokončne prepovedi obdelave, opozarjanje ali opominjanje upravljavca ali napotitev zadeve v nacionalne parlamente ali druge politične institucije,

– pooblastila za sodelovanje v sodnih postopkih, kadar so kršene nacionalne določbe, sprejete v skladu s to direktivo, ali za seznanitev sodnih organov s temi kršitvami.

[…]“

Splošna uredba o varstvu podatkov

7 Direktiva 95/46 je bila razveljavljena in nadomeščena z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46 (Splošna uredba o varstvu podatkov) (UL 2016, L 119, str. 1, v nadaljevanju: Splošna uredba o varstvu podatkov).

8 V uvodnih izjavah 6, 10, 101, 103, 104, od 107 do 109, 114, 116 in 141 Splošne uredbe o varstvu podatkov je navedeno:

„(6) Hiter tehnološki razvoj in globalizacija sta prinesla nove izzive za varstvo osebnih podatkov. Obseg zbiranja in izmenjave osebnih podatkov se je bistveno povečal. Tehnologija zasebnim podjetjem in javnim organom omogoča, da osebne podatke uporabljajo za dosego svojih ciljev v obsegu, kakršnega še ni bilo. Posamezniki vedno bolj dajejo osebne podatke na razpolago tako javno kot globalno. Tehnologija je spremenila tako gospodarstvo kot družbeno življenje ter bi morala še naprej omogočati lažje izvajanje prostega pretoka osebnih podatkov v Uniji ter prenosa v tretje države in mednarodne organizacije, pri čemer je treba zagotoviti visoko raven varstva osebnih podatkov.

[…]

(10) Za zagotovitev dosledne in visoke ravni varstva posameznikov ter odstranitev ovir za prenos osebnih podatkov v Uniji bi morala biti raven varstva pravic in svoboščin posameznikov pri obdelavi osebnih podatkov enaka v vseh državah članicah. V vsej Uniji bi bilo treba zagotoviti dosledno in enotno uporabo pravil za varstvo temeljnih pravic in svoboščin posameznikov pri obdelavi osebnih podatkov. Kar zadeva obdelavo osebnih podatkov z namenom izpolnjevanja pravne obveznosti, za opravljanje naloge, ki se izvaja v javnem interesu, ali pri izvajanju javne oblasti, dodeljene upravljavcu, bi moralo biti državam članicam dovoljeno ohraniti ali uvesti nacionalne določbe za podrobnejšo opredelitev uporabe pravil iz te uredbe. Države članice so v povezavi s splošnim in horizontalnim pravom o varstvu podatkov, s katerim se izvaja Direktiva 95/46/ES, sprejele več področnih zakonov na področjih, kjer so potrebne podrobnejše določbe. Tudi ta uredba državam članicam daje manevrski prostor za podrobnejšo opredelitev njenih pravil, tudi glede obdelave posebnih vrst osebnih podatkov (‚občutljivi podatki‘). V tem obsegu ta uredba ne izključuje prava držav članic, s katerim so opredeljene okoliščine posebnih primerov obdelave, vključno s podrobnejšo določitvijo pogojev, pod katerimi je obdelava osebnih podatkov zakonita.

[…]

(101) Prenosi osebnih podatkov v države zunaj Unije in mednarodne organizacije ter iz njih so potrebni za razvoj mednarodne trgovine in mednarodnega sodelovanja. Povečanje takih prenosov je prineslo nove izzive in skrbi glede varstva osebnih podatkov. Vendar kadar se osebni podatki prenašajo iz Unije upravljavcem, obdelovalcem ali drugim prejemnikom v tretjih državah ali mednarodnim organizacijam, raven varstva posameznikov, ki jo v Uniji zagotavlja ta uredba, ne bi smela biti ogrožena, vključno v primeru nadaljnjih prenosov osebnih podatkov iz tretje države ali mednarodne organizacije upravljavcem, obdelovalcem v isti ali drugi tretji državi ali mednarodni organizaciji. V vsakem primeru se lahko prenosi v tretje države in mednarodne organizacije izvajajo samo v popolni skladnosti s to uredbo. Prenos bi se lahko izvedel le, če upravljavec ali obdelovalec v skladu z drugimi določbami te uredbe izpolnjuje pogoje iz določb te uredbe v zvezi s prenosom podatkov v tretje države ali mednarodne organizacije.

[…]

(103) Komisija lahko sklene – z učinkom za celotno Unijo – da tretja država. ozemlje ali določeni sektor v tretji državi ali mednarodna organizacija nudi ustrezno raven varstva podatkov, s čimer zagotavlja pravno varnost in enotnost po vsej Uniji v zvezi s tretjo državo ali mednarodno organizacijo, za katero velja, da zagotavlja takšno raven varstva. V takih primerih se lahko prenosi osebnih podatkov v to tretjo državo ali mednarodno organizacijo opravijo brez potrebe

po pridobitvi dodatnega dovoljenja. Komisija lahko, potem ko tretjo državo ali mednarodno organizacijo obvesti in ji predloži celotno izjavo z navedbo razlogov, takšno odločitev tudi prekliče.

(104) Komisija bi morala v skladu s temeljnimi vrednotami, na katerih temelji Unija, zlasti z varstvom človekovih pravic, v svoji oceni tretje države ali ozemlja ali določenega sektorja v tretji državi upoštevati, v kolikšni meri posamezna tretja država spoštuje načelo pravne države, dostop do pravnega varstva, pa tudi mednarodna pravila in standarde na področju človekovih pravic ter svojo splošno in področno zakonodajo, med drugim zakonodajo na področju javne varnosti, obrambe, nacionalne varnosti ter javnega reda in kazenskega prava. Pri sprejetju sklepa o ustreznosti glede ozemlja ali določenega sektorja v tretji državi bi bilo treba upoštevati jasna in objektivna merila, kot so posebne dejavnosti obdelave ter področje uporabe veljavnih pravnih standardov in veljavne zakonodaje v tretji državi. Tretja država bi morala nuditi jamstva, ki zagotavljajo ustrezno raven varstva, ki je v osnovi enakovredna tisti, zagotovljeni v Uniji, zlasti kadar se osebni podatki obdelujejo v enem ali več določenih sektorjih. Zlasti bi morala zagotavljati učinkovit neodvisen nadzor varstva podatkov ter mehanizme sodelovanja z organi za varstvo podatkov držav članic, posamezniki, na katere se nanašajo osebni podatki, pa bi morali imeti učinkovite in izvršljive pravice ter dostop do učinkovitega upravnega in sodnega varstva.

[…]

(107) Komisija lahko ugotovi, da tretja država, ozemlje ali določen sektor v tretji državi ali mednarodna organizacija ne zagotavlja več ustrezne ravni varstva podatkov. Posledično bi se moral prenos osebnih podatkov v to tretjo državo ali mednarodno organizacijo prepovedati, razen če so izpolnjene zahteve iz te uredbe v zvezi s prenosi ob upoštevanju ustreznih zaščitnih ukrepov, vključno z zavezujočimi poslovnimi pravili in odstopanji za posebne primere. V takem primeru bi moralo biti predvideno posvetovanje med Komisijo in takimi tretjimi državami ali mednarodnimi organizacijami. Komisija bi morala tretjo državo ali mednarodno organizacijo pravočasno obvestiti o zadevnih razlogih in z njo začeti posvetovanja za izboljšanje stanja.

(108) Če sklep o ustreznosti ni sprejet, bi moral upravljavec ali obdelovalec sprejeti ukrepe, na podlagi katerih pomanjkanje varstva podatkov v tretji državi nadomestijo z ustreznimi zaščitnimi ukrepi za posameznika, na katerega se nanašajo osebni podatki. Taki ustrezni zaščitni ukrepi so lahko sestavljeni iz uporabe zavezujočih poslovnih pravil, standardnih določil Komisije o varstvu podatkov, standardnih določil nadzornega organa o varstvu podatkov ali pogodbenih določil, ki jih je odobril nadzorni organ. S temi zaščitnimi ukrepi bi bilo treba zagotoviti skladnost z zahtevami glede varstva podatkov in pravicami posameznikov, na katere se nanašajo osebni podatki, ki ustrezajo obdelavi znotraj Unije, vključno z razpoložljivostjo izvršljivih pravic posameznikov, na katere se nanašajo osebni podatki, in učinkovitih pravnih sredstev, tudi pravico do učinkovitega upravnega ali sodnega varstva ali odškodnine, v Uniji ali tretji državi. Nanašati bi se morali zlasti na skladnost s splošnimi načeli v zvezi z obdelavo osebnih podatkov ter načeli vgrajenega in prevzetega varstva podatkov. […]

(109) Možnost, ki jo ima upravljavec ali obdelovalec glede uporabe standardnih določil Komisije ali nadzornega organa o varstvu podatkov, upravljavcem ali obdelovalcem ne bi smela preprečiti niti, da standardna določila o varstvu podatkov vključijo v obsežnejšo pogodbo, kot je pogodba med obdelovalcem in drugim obdelovalcem, niti da dodajo druga določila ali dodatne zaščitne ukrepe, če ti neposredno ali posredno ne nasprotujejo standardnim pogodbenim določilom Komisije ali nadzornega organa ali posegajo v temeljne pravice ali svoboščine posameznikov, na katere se nanašajo osebni podatki. Upravljavce in obdelovalce bi bilo treba spodbujati, da vzpostavijo dodatne zaščitne ukrepe s pomočjo pogodbenih obveznosti, ki bi dopolnjevale standardna zaščitna določila.

[…]

(114) V vsakem primeru bi moral upravljavec ali obdelovalec, če Komisija ni sprejela sklepa o ustrezni ravni varstva podatkov v tretji državi, uporabiti rešitve, ki posameznikom, na katere se nanašajo osebni podatki, zagotavljajo izvršljive in učinkovite pravice glede obdelave njihovih podatkov v Uniji po prenosu teh podatkov, tako da lahko še vedno uresničujejo temeljne pravice in zaščitne ukrepe.

[…]

(116) Pri čezmejnem prenosu osebnih podatkov zunaj Unije se lahko poveča tveganje v zvezi z zmožnostjo posameznikov za uresničevanje pravic do varstva podatkov, zlasti da se zaščitijo pred nezakonito uporabo ali razkritjem navedenih podatkov. Hkrati lahko nadzorni organi ugotovijo, da ne morejo obravnavati pritožb ali izvesti preiskav v zvezi z dejavnostmi zunaj svojih meja. Njihova prizadevanja za čezmejno sodelovanje lahko ovirajo tudi nezadostna pooblastila za preprečevanje kršitev ali njihovo odpravo, neskladne pravne ureditve in praktične ovire, na primer omejitev virov. […]

[…]

(141) Vsak posameznik, na katerega se nanašajo osebni podatki, bi moral imeti pravico, da vloži pritožbo pri enem nadzornem organu, zlasti v državi članici svojega običajnega prebivališča, in pravico do učinkovitega pravnega sredstva v skladu s členom 47 Listine, kadar meni, da so njegove pravice iz te uredbe kršene, ali če nadzorni organ ne obravnava pritožbe, jo v celoti ali deloma zavrže ali zavrne ali ne ukrepa, kadar je tak ukrep potreben za zaščito pravic posameznika, na katerega se nanašajo osebni podatki. […]“

9 Člen 2(1) in (2) te uredbe določa:

„1. Ta uredba se uporablja za obdelavo osebnih podatkov, ki se v celoti ali delno izvaja z avtomatiziranimi sredstvi, in za obdelavo osebnih podatkov, ki so del zbirke ali so namenjeni oblikovanju dela zbirke, ki se ne izvaja z avtomatiziranimi sredstvi.

2. Ta uredba se ne uporablja za obdelavo osebnih podatkov:

(a) v okviru dejavnosti zunaj področja uporabe prava Unije;

(b) s strani držav članic, kadar izvajajo dejavnosti, ki spadajo na področje uporabe poglavja 2 naslova V PEU;

(c) s strani fizične osebe med potekom popolnoma osebne ali domače dejavnosti;

(d) s strani pristojnih organov za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem.“

10 Člen 4 navedene uredbe določa:

„V tej uredbi:

[…]

(2) ‚obdelava‘ pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje;

[…]

(7) ‚upravljavec‘ pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo Unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Unije ali pravom države članice;

(8) ‚obdelovalec‘ pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;

(9) ‚uporabnik‘ pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Vendar pa se javni organi, ki lahko prejmejo osebne podatke v okviru posamezne poizvedbe v skladu s pravom Unije ali pravom države članice, ne štejejo za uporabnike; obdelava teh podatkov s strani teh javnih organov poteka v skladu z veljavnimi pravili o varstvu podatkov glede na namene obdelave;

[…]“

11 Člen 23 iste uredbe določa:

„1. Pravo Unije ali pravo države članice, ki velja za upravljavca ali obdelovalca podatkov, lahko z zakonodajnim ukrepom omeji obseg obveznosti in pravic iz členov 12 do 22 in člena 34, pa tudi člena 5, kolikor njegove določbe ustrezajo pravicam in obveznostim iz členov 12 do 22, če taka omejitev spoštuje bistvo temeljnih pravic in svoboščin ter je potreben in sorazmeren ukrep v demokratični družbi za zagotavljanje:

(a) državne varnosti;

(b) obrambe;

(c) javne varnosti;

(d) preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem;

[…]

2. Zlasti vsak zakonodajni ukrep iz odstavka 1 vsebuje posebne določbe vsaj, kjer je ustrezno, glede:

(a) namenov obdelave ali vrst obdelave;

(b) vrst osebnih podatkov;

(c) obsega uvedenih omejitev;

(d) zaščitnih ukrepov za preprečitev zlorab ali nezakonitega dostopa ali prenosa;

(e) natančnejše ureditve upravljavca ali vrst upravljavcev;

(f) obdobij hrambe in veljavnih zaščitnih ukrepov, pri čemer se upoštevajo narava, obseg in nameni obdelave ali vrste obdelave;

(g) tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, ter

(h) pravice posameznikov, na katere se nanašajo osebni podatki, da so obveščeni o omejitvi, razen če bi to posegalo v namen omejitve.“

12 Poglavje V Splošne uredbe o varstvu podatkov, naslovljeno „Prenos osebnih podatkov v tretje države ali mednarodne organizacije“, vsebuje člene od 44 do 50 te uredbe. Člen 44 te uredbe, naslovljen „Splošno načelo za prenose“, določa:

„Vsak prenos osebnih podatkov, ki se obdelujejo ali so namenjeni obdelavi po prenosu v tretjo državo ali mednarodno organizacijo, se ob upoštevanju drugih določb te uredbe izvede le, če upravljavec in obdelovalec ravnata v skladu s pogoji iz tega poglavja, kar velja tudi za nadaljnje prenose osebnih podatkov iz tretje države ali mednarodne organizacije v drugo tretjo državo ali drugo mednarodno organizacijo. Vse določbe tega poglavja se uporabljajo za zagotovitev, da ni ogrožena raven varstva posameznikov, ki jo zagotavlja ta uredba.“

13 Člen 45 te uredbe, naslovljen „Prenosi na podlagi sklepa o ustreznosti“, v odstavkih od 1 do 3 določa:

„1. Prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo se lahko izvede, če Komisija odloči, da zadevna tretja država, ozemlje, eden ali več določenih sektorjev v tej tretji državi ali mednarodna organizacija zagotavlja ustrezno raven varstva podatkov. Za tak prenos ni potrebno posebno dovoljenje.

2. Komisija pri ocenjevanju ustreznosti ravni varstva upošteva zlasti naslednje elemente:

(a) načelo pravne države, spoštovanje človekovih pravic in temeljnih svoboščin, ustrezno splošno in področno zakonodajo, tudi na področju javne varnosti, obrambe, nacionalne varnosti in kazenskega prava ter dostopa javnih organov do osebnih podatkov, pa tudi izvajanje take zakonodaje, pravila o varstvu podatkov, strokovna pravila ter varnostne ukrepe, vključno s pravili za nadaljnji prenos osebnih podatkov v drugo tretjo državo ali mednarodno organizacijo, ki se spoštujejo v navedeni tretji državi ali mednarodni organizaciji, sodno prakso, pa tudi dejanske in izvršljive pravice ter učinkovito upravno in sodno varstvo posameznikov, na katere se nanašajo osebni podatki, ki se prenašajo;

(b) obstoj enega ali več učinkovito delujočih neodvisnih nadzornih organov v tretji državi članici ali pristojnih za mednarodno organizacijo, ki so odgovorni za zagotavljanje in izvrševanje predpisov o varstvu podatkov, kar vključuje tudi ustrezna pooblastila za izvrševanje, za pomoč in svetovanje posameznikom, na katere se nanašajo osebni podatki, pri uresničevanju njihovih pravic ter za sodelovanje z nadzornimi organi držav članic, in

(c) mednarodne zaveze, ki jih je sprejela zadevna tretja država ali mednarodna organizacija, ali druge obveznosti, ki izhajajo iz pravno zavezujočih konvencij ali instrumentov, pa tudi iz sodelovanja tretje države ali mednarodne organizacije v večstranskih ali regionalnih sistemih, zlasti glede varstva osebnih podatkov.

3. Komisija lahko po oceni ustreznosti ravni varstva z izvedbenim aktom odloči, da tretja država, ozemlje ali en ali več določenih sektorjev v zadevni tretji državi ali mednarodna organizacija zagotavlja ustrezno raven varstva v smislu odstavka 2 tega člena. V izvedbenem aktu se določi mehanizem za redni pregled, vsaj vsaka štiri leta, ki v celoti upošteva razvoj dogodkov na zadevnem področju v tretji

državi ali mednarodni organizaciji. V izvedbenem aktu se določi njegova ozemeljska veljavnost in sektorska uporaba ter, kadar je ustrezno, opredeli nadzorni organ ali organi iz točke (b) odstavka 2 tega člena. Izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 93(2).“

14 Člen 46 navedene uredbe, naslovljen „Prenosi, za katere se uporabljajo ustrezni zaščitni ukrepi“, v odstavkih od 1 do 3 določa:

„1. Kadar sklep v skladu s členom 45(3) ni sprejet, lahko upravljavec ali obdelovalec osebne podatke prenese v tretjo državo ali mednarodno organizacijo le, če je upravljavec ali obdelovalec predvidel ustrezne zaščitne ukrepe, in pod pogojem, da imajo posamezniki, na katere se nanašajo osebni podatki, na voljo izvršljive pravice in učinkovita pravna sredstva.

2. Ustrezni zaščitni ukrepi iz odstavka 1 se lahko, ne da bi bilo potrebno posebno dovoljenje nadzornih organov, zagotovijo s:

(a) pravno zavezujočim in izvršljivim instrumentom, ki ga sprejmejo javni organi ali telesa;

(b) zavezujočimi poslovnimi pravili v skladu s členom 47;

(c) standardnimi določili o varstvu podatkov, ki jih sprejme Komisija v skladu s postopkom pregleda iz člena 93(2);

(d) standardnimi določili o varstvu podatkov, ki jih sprejme nadzorni organ in odobri Komisija v skladu s postopkom pregleda iz člena 93(2);

(e) odobrenim kodeksom ravnanja v skladu s členom 40, skupaj z zavezujočimi in izvršljivimi zavezami upravljavca ali obdelovalca v tretji državi, da bo uporabljal ustrezne zaščitne ukrepe, tudi glede pravic posameznikov, na katere se nanašajo osebni podatki, ali

(f) odobrenim mehanizmom certificiranja v skladu s členom 42, skupaj z zavezujočimi in izvršljivimi zavezami upravljavca ali obdelovalca v tretji državi, da bo uporabljal ustrezne zaščitne ukrepe, tudi glede pravic posameznikov, na katere se nanašajo osebni podatki.

3. Ustrezni zaščitni ukrepi iz odstavka 1 se lahko z dovoljenjem ustreznega nadzornega organa zagotovijo tudi zlasti s:

(a) pogodbenimi določili med upravljavcem ali obdelovalcem in upravljavcem, obdelovalcem ali uporabnikom osebnih podatkov v tretji državi ali mednarodni organizaciji, ali

(b) določbami, ki se vstavijo v upravne dogovore med javnimi organi ali telesi in v katere so vključene izvršljive in učinkovite pravice za posameznike, na katere se nanašajo osebni podatki.“

15 Člen 49 iste uredbe, naslovljen „Odstopanja v posebnih primerih“, določa:

„1. Če sklep o ustreznosti v skladu s členom 45(3) ni sprejet ali pa niso sprejeti ustrezni zaščitni ukrepi v skladu s členom 46, vključno z zavezujočimi poslovnimi pravili, se lahko prenos ali niz prenosov osebnih podatkov v tretjo državo ali mednarodno organizacijo izvede le pod enim izmed naslednjih pogojev:

(a) posameznik, na katerega se nanašajo osebni podatki, je izrecno privolil v predlagani prenos, potem ko je bil obveščen o morebitnih tveganjih, ki jih zaradi nesprejetja sklepa o ustreznosti in ustreznih zaščitnih ukrepov takšni prenosi pomenijo zanj;

(b) prenos je potreben za izvajanje pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem ali za izvajanje predpogodbenih ukrepov, sprejetih na zahtevo posameznika, na katerega se nanašajo osebni podatki;

(c) prenos je potreben za sklenitev ali izvajanje pogodbe med upravljavcem in drugo fizično ali pravno osebo, ki je v interesu posameznika, na katerega se nanašajo osebni podatki;

(d) prenos je potreben zaradi pomembnih razlogov javnega interesa;

(e) prenos je potreben za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov;

(f) prenos je potreben za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali drugih oseb, kadar posameznik, na katerega se nanašajo osebni podatki, fizično ali poslovno ni sposoben dati privolitve,

(g) prenos se opravi iz registra, ki je po pravu Unije ali pravu države članice namenjen zagotavljanju informacij javnosti in je na voljo za vpogled bodisi javnosti na splošno bodisi kateri koli osebi, ki lahko izkaže zakonit interes, vendar le, če so v posameznem primeru izpolnjeni pogoji za tak vpogled, določeni s pravom Unije ali pravom države članice.

Kadar podlaga za prenos ne morejo biti določbe iz člena 45 ali 46, vključno z določbami zavezujočih poslovnih pravil, in ne velja nobeno od odstopanj v posebnih primerih iz prvega pododstavka tega odstavka, se lahko prenos v tretjo državo ali mednarodno organizacijo izvede samo, če prenos ni ponovljiv, zadeva le omejeno število posameznikov, na katere se nanašajo osebni podatki, je potreben zaradi nujnih zakonitih interesov, za katere si prizadeva upravljavec in nad katerimi ne prevladajo interesi ali pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, in pod pogojem, da je upravljavec ocenil vse okoliščine v zvezi s prenosom podatkov in na podlagi te ocene predvidel ustrezne zaščitne ukrepe v zvezi z varstvom osebnih podatkov. Upravljavec o prenosu obvesti nadzorni organ. Poleg informacij iz členov 13 in 14 upravljavec posreduje posamezniku, na katerega se nanašajo osebni podatki, tudi informacije o zadevnem prenosu in nujnih zakonitih interesih, za katere si prizadeva upravljavec.

2. Prenos v skladu s točko (g) prvega pododstavka odstavka 1 ne vključuje vseh osebnih podatkov ali celih vrst osebnih podatkov, ki jih vsebuje register. Kadar je register namenjen vpogledu oseb, ki imajo zakoniti interes, se prenos opravi samo, če to zahtevajo te osebe ali če bodo te osebe uporabniki.

3. Točke (a), (b) in (c) prvega pododstavka odstavka 1 ter drugi pododstavek navedenega odstavka se ne uporabljajo za dejavnosti, ki jih opravljajo javni organi pri izvajanju svojih javnih pooblastil.

4. Javni interes iz točke (d) prvega pododstavka odstavka 1 je priznan v pravu Unije ali pravu države članice, ki velja za upravljavca.

5. Če sklepa o ustreznosti ni, se lahko v pravu Unije ali pravu države članice zaradi pomembnih razlogov javnega interesa izrecno določijo omejitve prenosa posebnih vrst osebnih podatkov v tretjo državo ali mednarodno organizacijo. Države članice o takšnih določbah uradno obvestijo Komisijo.

6. Upravljavec ali obdelovalec dokumentira oceno in ustrezne zaščitne ukrepe iz drugega pododstavka odstavka 1 tega člena v evidenci iz člena 30.“

16 Člen 51(1) Splošne uredbe o varstvu podatkov določa:

„Vsaka država članica zagotovi enega ali več neodvisnih javnih organov, ki so pristojni za spremljanje uporabe te uredbe, da se zaščitijo temeljne pravice in svoboščine posameznikov v zvezi z obdelavo ter olajša prost pretok osebnih podatkov v Uniji (v nadaljnjem besedilu: nadzorni organ).“

17 V skladu s členom 55(1) te uredbe je „[v]sak nadzorni organ […] na ozemlju svoje države članice pristojen za opravljanje dodeljenih nalog in izvajanje prenesenih pooblastil v skladu s to uredbo“.

18 Člen 57(1) navedene uredbe določa:

„Brez poseganja v druge naloge, določene v tej uredbi, vsak nadzorni organ na svojem ozemlju:

(a) spremlja in zagotavlja uporabo te uredbe;

[…]

(f) obravnava pritožbe, ki jih vloži posameznik, na katerega se nanašajo osebni podatki, oziroma v skladu s členom 80 telo, organizacija ali združenje, v ustreznem obsegu preuči vsebino pritožbe in v razumnem roku obvesti pritožnika o poteku in rezultatu preiskave, zlasti če je potrebna nadaljnja preiskava ali usklajevanje z drugim nadzornim organom;

[…]“

19 Člen 58(2) in (4) iste uredbe določa:

„2. Vsak nadzorni organ ima vsa naslednja popravljalna pooblastila:

[…]

(f) da uvede začasno ali dokončno omejitev obdelave, vključno s prepovedjo obdelave;

[…]

(j) da odredi prekinitev prenosov podatkov uporabniku v tretji državi ali mednarodni organizaciji.

[…]

4. Nadzorni organ izvaja pooblastila, ki so mu dodeljena v skladu s tem členom, na podlagi [ob upoštevanju] ustreznih zaščitnih ukrepov, vključno z učinkovitim pravnim sredstvom in ustreznim pravnim postopkom, kot je določeno v pravu Unije in pravu države članice v skladu z Listino.“

20 Člen 64(2) Splošne uredbe o varstvu podatkov določa:

„Kateri koli nadzorni organ, predsednik [Evropskega odbora za varstvo podatkov (EOVP)] ali Komisija lahko zahteva, da katero koli zadevo splošne uporabe ali z učinkom v več kot eni državi članici preuči odbor, ki da mnenje, zlasti kadar pristojni nadzorni organ ne izpolni obveznosti glede medsebojne pomoči v skladu s členom 61 ali glede skupnega ukrepanja v skladu s členom 62.“

21 Člen 65(1) te uredbe določa:

„Da se zagotovi pravilna in dosledna uporaba te uredbe v posameznih primerih, odbor sprejme zavezujočo odločitev v naslednjih primerih:

[…]

(c) kadar pristojni nadzorni organ ne zaprosi za mnenje odbora v primerih iz člena 64(1) ali ne upošteva mnenja odbora, izdanega na podlagi člena 64. V tem primeru lahko kateri koli zadevni nadzorni organ ali Komisija zadevo posreduje odboru.“

22 Člen 77 navedene uredbe, naslovljen „Pravica do vložitve pritožbe pri nadzornem organu“, določa:

„1. Brez poseganja v katero koli drugo upravno ali pravno sredstvo ima vsak posameznik, na katerega se nanašajo osebni podatki, pravico, da vloži pritožbo pri nadzornem organu, zlasti v državi članici, v kateri ima običajno prebivališče, v kateri je njegov kraj dela ali v kateri je domnevno prišlo do kršitve, če meni, da obdelava osebnih podatkov v zvezi z njim krši to uredbo.

2. Nadzorni organ, pri katerem je vložena pritožba, obvesti pritožnika o stanju zadeve in odločitvi o pritožbi, vključno z možnostjo pravnega sredstva na podlagi člena 78.“

23 Člen 78 iste uredbe, naslovljen „Pravica do učinkovitega pravnega sredstva zoper nadzorni organ“, v odstavkih 1 in 2 določa:

„1. Brez poseganja v katero koli drugo upravno ali izvensodno sredstvo ima vsaka fizična ali pravna oseba pravico do učinkovitega pravnega sredstva zoper pravno zavezujočo odločitev nadzornega organa v zvezi z njo.

2. Brez poseganja v katero koli drugo upravno ali izvensodno sredstvo ima vsak posameznik, na katerega se nanašajo osebni podatki, pravico do učinkovitega pravnega sredstva, kadar nadzorni organ, ki je pristojen na podlagi členov 55 in 56, ne obravnava pritožbe ali če posameznika, na katerega se nanašajo osebni podatki, v treh mesecih ne obvesti o stanju zadeve ali odločitvi o pritožbi, vloženi na podlagi člena 77.“

24 Člen 94 Splošne uredbe o varstvu podatkov določa:

„1. Direktiva [95/46] se razveljavi z učinkom od 25. maja 2018.

2. Sklicevanja na razveljavljeno direktivo se štejejo kot sklicevanja na to uredbo. Sklicevanja na Delovno skupino za varstvo posameznikov pri obdelavi osebnih podatkov, ustanovljeno s členom 29 Direktive [95/46], se štejejo kot sklicevanja na Evropski odbor za varstvo podatkov, ustanovljen s to uredbo.“

25 Člen 99 te uredbe določa:

„1. Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

2. Uporablja se od 25. maja 2018.“

Sklep SPK

26 V uvodni izjavi 11 Sklepa SPK je navedeno:

„Nadzorni organi držav članic imajo v tem pogodbenem mehanizmu ključno vlogo pri zagotavljanju primernega varstva osebnih podatkov po prenosu. V izjemnih primerih, kadar izvozniki podatkov odklonijo dajanje primernih navodil uvozniku podatkov ali pa so jih nesposobni dati, ter kadar obstaja neizbežna nevarnost resne škode za posameznike, na katere se nanašajo osebni podatki, naj standardne pogodbene klavzule dovolijo nadzornim organom pregled uvoznikov podatkov in podobdelovalcev ter, kjer je to primerno, sprejemanje odločitev, zavezujočih za uvoznike in podobdelovalce. Nadzorni organi naj bi imeli pooblastilo za prepoved ali začasno ustavitev prenosa podatkov ali niza prenosov, ki temelji na standardnih pogodbenih klavzulah v tistih izjemnih primerih, kjer se ugotovi verjetnost, da ima lahko prenos na pogodbeni podlagi precej škodljivih posledic za jamstva in obveznosti, ki zagotavljajo primerno varstvo posameznika, na katerega se nanašajo osebni podatki.“

27 Člen 1 tega sklepa določa:

„Standardne pogodbene klavzule iz Priloge veljajo za takšne, ki zagotavljajo ustrezne zaščitne ukrepe glede varstva zasebnosti ter temeljnih pravic in svoboščin posameznikov in glede uresničevanja ustreznih pravic, kakor zahteva člen 26(2) Direktive [95/46]."

28 Ta sklep se v skladu s svojim členom 2, drugi odstavek, „uporablja za prenos osebnih podatkov s strani upravljavcev s sedežem v Evropski uniji prejemnikom s sedežem zunaj ozemlja Evropske unije, ki delujejo samo kot obdelovalci".

29 Člen 3 navedenega sklepa določa:

„V tem sklepu se uporabljajo naslednje opredelitve pojmov:

[…]

(c) ‚izvoznik podatkov' pomeni upravljavca, ki prenaša osebne podatke;

(d) ‚uvoznik podatkov' pomeni obdelovalca s sedežem v tretji državi, ki soglaša, da od izvoznika podatkov prejema osebne podatke, namenjene za obdelavo v imenu izvoznika podatkov po prenosu v skladu z njegovimi navodili in pogoji tega sklepa, ter ki ni podvržen sistemu tretje države za zagotovitev primernega varstva v smislu člena 25(1) Direktive [95/46];

[…]

(f) ‚veljavno pravo o varstvu podatkov' pomeni zakonodajo, ki varuje temeljne pravice in svoboščine posameznikov ter zlasti njihovo pravico do zasebnosti glede obdelave osebnih podatkov, ki jo uporablja upravljavec podatkov v državi članici, v kateri je sedež izvoznika podatkov;

[…]"

30 Člen 4 Sklepa 2010/87 je v prvotni različici, ki je veljala pred začetkom veljavnosti Izvedbenega sklepa 2016/2297, določal:

„1. Pristojni organi v državah članicah lahko ne glede na svoja pooblastila za sprejetje ukrepov za zagotovitev skladnosti z nacionalnimi predpisi, sprejetimi v skladu s poglavji II, III, V in VI Direktive [95/46], izvajajo svoja obstoječa pooblastila, da prepovejo ali začasno ustavijo pretok podatkov v tretje države zaradi varstva posameznikov pri obdelavi njihovih osebnih podatkov v primerih, če:

(a) je ugotovljeno, da zakonodaja, ki velja za uvoznika podatkov ali podobdelovalca, temu nalaga zahteve po odstopanju od veljavnega prava o varstvu podatkov, ki presegajo omejitve, potrebne v demokratični družbi, kakor jih predvideva člen 13 Direktive 95/46/ES, če zaradi teh zahtev obstaja verjetnost precejšnjih škodljivih posledic za jamstva, zagotovljena z veljavnim pravom o varstvu podatkov in standardnimi pogodbenimi klavzulami;

(b) pristojni organ ugotovi, da uvoznik podatkov ali podobdelovalec ni spoštoval standardnih pogodbenih klavzul iz Priloge, ali

(c) obstaja precejšnja verjetnost, da standardne pogodbene klavzule iz Priloge niso ali ne bodo izpolnjene ter da bi nadaljnji prenos povzročil neposredno tveganje z resno škodo za posameznike, na katere se nanašajo osebni podatki.

2. Prepoved ali začasna ustavitev v skladu z odstavkom 1 preneha veljati takoj, ko nehajo obstajati razlogi za prepoved ali začasno ustavitev.

3. Ko države članice sprejmejo ukrepe v skladu z odstavkoma 1 in 2, takoj obvestijo Komisijo, ki bo posredovala informacije drugim državam članicam.“

31 V točki 5 obrazložitve Izvedbenega sklepa 2016/2297, ki je bil sprejet po razglasitvi sodbe z dne 6. oktobra 2015, Schrems (C-362/14, EU:C:2015:650), je navedeno:

„Sklep Komisije, sprejet v skladu s členom 26(4) Direktive [95/46], je s potrebnimi spremembami zavezujoč za vse organe držav članic, na katere je naslovljen, vključno z njihovimi neodvisnimi nadzornimi organi, v delu, v katerem priznava, da prenosi, ki se izvedejo na podlagi standardnih pogodbenih klavzul iz Sklepa, nudijo zadostno zaščito v skladu s členom 26(2) navedene direktive. To nacionalnim nadzornim organom ne preprečuje izvrševanja njihovih pristojnosti za nadzor pretoka podatkov, vključno s pooblastilom za začasno ustavitev ali prepoved prenosa osebnih podatkov, če se ugotovi, da izvajanje prenosa krši zakonodajo EU ali nacionalno zakonodajo o varstvu podatkov, kot v primeru, da uvoznik podatkov ne spoštuje standardnih pogodbenih klavzul.“

32 Člen 4 Sklepa SPK v sedanji različici, ki izhaja iz Izvedbenega sklepa 2016/2297, določa:

„Kadar pristojni organi v državah članicah izvajajo svoja pooblastila v skladu s členom 28(3) Direktive [95/46], na podlagi česar pride do začasne ustavitve ali dokončne prepovedi prenosa podatkov v tretje države, da se zaščitijo posamezniki pri obdelavi njihovih osebnih podatkov, zadevna država članica nemudoma obvesti Komisijo, ta pa informacije posreduje drugim državam članicam.“

33 Priloga k Sklepu SPK, naslovljena „Standardne pogodbene klavzule (obdelovalci)“, vsebuje 12 standardnih klavzul. Klavzula 3 te priloge, naslovljena „Klavzula v korist tretjega“, določa:

„1. Posameznik, na katerega se nanašajo osebni podatki, lahko kot upravičena tretja stranka proti izvozniku podatkov uveljavlja to klavzulo, klavzulo 4(b) do (i), klavzulo 5(a) do (e) in (g) do (j), klavzulo 6(1) in (2), klavzulo 7, klavzulo 8(2) ter klavzule 9 do 12.

2. Posameznik, na katerega se nanašajo osebni podatki, lahko proti uvozniku podatkov uveljavlja to klavzulo, klavzulo 5(a) do (e) in (g), klavzulo 6, klavzulo 7, klavzulo 8(2) ter klavzule 9 do 12, če izvoznik podatkov dejansko izgine ali pravno preneha obstajati, razen če je pravni naslednik s pogodbo ali po zakonu prevzel vse pravice in obveznosti izvoznika podatkov; v tem primeru lahko posameznik, na katerega se nanašajo osebni podatki, navedene klavzule uveljavlja proti pravnemu nasledniku.

[…]“

34 Klavzula 4 te priloge, naslovljena „Obveznosti izvoznika podatkov“, določa:

„Izvoznik podatkov soglaša z naslednjim in zagotavlja:

(a) da se je obdelava osebnih podatkov vključno s prenosom izvajala in se bo še naprej izvajala v skladu z ustreznimi določbami veljavnega prava o varstvu podatkov (ter so bili po potrebi o tem obveščeni pristojni organi v državi članici, v kateri je sedež izvoznika podatkov) in da ne krši ustreznih predpisov te države;

(b) da je uvoznika podatkov poučil in mu bo med trajanjem obdelave osebnih podatkov še naprej dajal navodila, da naj obdeluje prenesene osebne podatke samo v imenu izvoznika podatkov ter v skladu z veljavnim pravom o varstvu podatkov in klavzulami;

[…]

(f) da je bil oziroma bo posameznik, na katerega se nanašajo osebni podatki, v primeru prenosa posebnih vrst podatkov pred prenosom ali čim prej po njem obveščen o tem, da bi se njegovi podatki lahko prenesli v tretjo državo, ki ne zagotavlja primernega varstva v smislu Direktive [95/46];

(g) da v skladu s klavzulo 5(b) in klavzulo 8(3) vsako obvestilo, prejeto od uvoznika podatkov ali katerega koli podobdelovalca, posreduje nadzornemu organu za varstvo osebnih podatkov, če se odloči nadaljevati prenos ali odpraviti začasno ustavitev;

[…]“

35 Klavzula 5 te priloge, naslovljena „Obveznosti uvoznika podatkov […]“, določa:

„Uvoznik podatkov soglaša z naslednjim in zagotavlja:

(a) da obdeluje osebne podatke samo v imenu izvoznika podatkov ter v skladu z njegovimi navodili in klavzulami; če jih iz kakršnih koli razlogov ne more upoštevati, soglaša, da o tem nemudoma obvesti izvoznika podatkov, ki je v tem primeru upravičen začasno ustaviti prenos podatkov in/ali odstopiti od pogodbe;

(b) da nima razloga za domnevo, da mu zakonodaja, ki velja zanj, preprečuje izpolnjevanje navodil izvoznika podatkov in obveznosti iz pogodbe, ter da bo v primeru spremembe te zakonodaje, ki bo verjetno imela znaten negativen učinek na jamstva in obveznosti iz klavzul, to spremembo sporočil izvozniku podatkov takoj, ko bo zanjo izvedel, izvoznik podatkov pa je v tem primeru upravičen začasno ustaviti prenos podatkov in/ali odstopiti od pogodbe;

[…]

(d) da bo izvoznika podatkov nemudoma obvestil o:
   (i) vseh pravno zavezujočih zahtevah organa kazenskega pregona za posredovanje osebnih podatkov, razen če je to kako drugače prepovedano, na primer s prepovedjo po kazenski zakonodaji zaradi ohranjanja zaupnosti kazenske preiskave;
   (ii) vsakem naključnem ali nepooblaščenem dostopu; ter
   (iii) vseh zahtevah, prejetih neposredno od posameznikov, na katere se nanašajo osebni podatki, ne da bi nanje odgovoril, razen če dobi za to pooblastilo;

[…]“

36 V opombi k naslovu te klavzule 5 je navedeno:

„Obvezne zahteve nacionalne zakonodaje, veljavne za uvoznika podatkov, ki ne presegajo tega, kar je potrebno v demokratični družbi na podlagi enega od interesov iz člena 13(1) Direktive [95/46], to je, če predstavljajo ukrep, potreben za zaščito nacionalne varnosti, obrambe, javne varnosti, preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj ali etičnih kršitev za zakonsko urejene poklice, pomembnega gospodarskega ali finančnega interesa države, varstva posameznika, na katerega se nanašajo osebni podatki, ali pravic in svoboščin drugih, niso v nasprotju s standardnimi pogodbenimi klavzulami. […]“

37 Klavzula 6 Priloge k Sklepu SPK, naslovljena „Odgovornost“, določa:

„1. Stranki soglašata, da je vsak posameznik, na katerega se nanašajo osebni podatki, ki je zaradi kršitve obveznosti iz klavzule 3 ali klavzule 11 s strani stranke ali podobdelovalca utrpel škodo, upravičen od izvoznika podatkov prejeti odškodnino za utrpelo škodo.

2. Če posameznik, na katerega se nanašajo osebni podatki, zaradi kršitve katere koli obveznosti iz klavzule 3 ali klavzule 11 s strani uvoznika podatkov ali njegovega podobdelovalca ne more uveljavljati odškodninskega zahtevka v skladu z odstavkom 1 zoper izvoznika podatkov, ker je izvoznik podatkov dejansko izginil, pravno prenehal obstajati ali pa postal insolventen, uvoznik podatkov soglaša, da lahko posameznik zahtevek uveljavlja zoper njega namesto zoper izvoznika podatkov […].

[…]“

38 Klavzula 8 te priloge, naslovljena „Sodelovanje z nadzornimi organi“, v odstavku 2 določa:

„Stranki soglašata, da ima nadzorni organ pravico izvesti pregled uvoznika podatkov in vseh podobdelovalcev, ki ima enak obseg in zanj veljajo enaki pogoji, ki bi veljali za pregled izvoznika podatkov v skladu z veljavnim pravom o varstvu podatkov.“

39 Klavzula 9 te priloge, naslovljena „Pravo, ki se uporablja“, določa, da za klavzule velja pravo države članice, v kateri je sedež izvoznika podatkov.

40 Klavzula 11 iste priloge, naslovljena „Podobdelava“, določa:

„1. Uvoznik podatkov brez predhodnega pisnega soglasja izvoznika podatkov podobdelovalcu ne sme oddati izvajanja postopkov obdelave, ki jih izvaja v imenu izvoznika podatkov na podlagi klavzul. Uvoznik podatkov lahko s soglasjem izvoznika podatkov odda izvajanje svojih obveznosti iz klavzul samo s pisnim sporazumom s podobdelovalcem, ki podobdelovalcu nalaga iste obveznosti, kot jih ima uvoznik podatkov po klavzulah. […]

2. Predhodni pisni sporazum med uvoznikom podatkov in podobdelovalcem vsebuje tudi klavzulo v korist tretjega, kot je določena v klavzuli 3, za primere, ko posameznik, na katerega se nanašajo osebni podatki, ne more uveljavljati odškodninskega zahtevka iz odstavka 1 klavzule 6 zoper izvoznika podatkov ali uvoznika podatkov, ker sta dejansko izginila, pravno prenehala obstajati ali pa postala insolventna in noben pravni naslednik ni s pogodbo ali po zakonu prevzel pravnih obveznosti izvoznika ali uvoznika podatkov. Takšna odgovornost podobdelovalca je omejena na njegove postopke obdelave iz klavzul.

[…]“

41 Klavzula 12 Priloge k Sklepu SPK, naslovljena „Obveznosti po prenehanju opravljanja storitev obdelave osebnih podatkov“, v odstavku 1 določa:

„Stranki soglašata, da uvoznik podatkov in podobdelovalec po prenehanju opravljanja storitev obdelave podatkov glede na izbiro izvoznika podatkov vrneta vse prenesene osebne podatke in njihove kopije izvozniku podatkov ali vse osebne podatke uničita in izvozniku podatkov potrdita, da sta to storila, razen če zakonodaja, veljavna za uvoznika podatkov, temu preprečuje vračanje ali uničenje vseh ali dela prenesenih osebnih podatkov. […]“

Sklep o zasebnostnem ščitu

42 Sodišče je s sodbo z dne 6. oktobra 2015, Schrems (C-362/14, EU:C:2015:650), razglasilo za neveljavno Odločbo Komisije 2000/520/ES z dne 26. julija 2000 po Direktivi 95/46 o primernosti zaščite, ki jo zagotavljajo načela zasebnosti varnega pristana in s tem povezana najpogosteje zastavljena vprašanja, ki jih je izdalo Ministrstvo za trgovino ZDA (UL, posebna izdaja v slovenščini, poglavje 16, zvezek 1, str. 119), v kateri je Komisija ugotovila, da ta tretja država zagotavlja ustrezno raven varstva.

43 Komisija je po razglasitvi te sodbe sprejela Sklep o zasebnostnem ščitu, potem ko je za njegovo sprejetje opravila oceno ureditve Združenih držav, kot je pojasnjeno v točki 65 obrazložitve navedenega sklepa:

„Komisija je ocenila omejitve in zaščitne ukrepe, ki so na voljo v zakonodaji ZDA, kar zadeva dostop in uporabo osebnih podatkov, ki jih javni organi v ZDA prenašajo v okviru zasebnostnega ščita EU-ZDA za namene nacionalne varnosti, kazenskega pregona in drugih javnih interesov. Poleg tega je vlada ZDA prek urada direktorja nacionalne obveščevalne službe (Office of the Director of National Intelligence, v nadaljnjem besedilu: ODNI) […] Komisiji predložila podrobna zagotovila in zaveze, vsebovane v Prilogi VI k temu sklepu. Z dopisom, ki ga je podpisal državni sekretar [minister za zunanje zadeve] in ki je priložen kot Priloga III k temu sklepu, se je vlada ZDA tudi zavezala, da bo ustvarila nov nadzorni mehanizem za posege na področju nacionalne varnosti, varuha človekovih pravic na področju zasebnostnega ščita, ki bo neodvisen od obveščevalne skupnosti. Zagotovilo Ministrstva za obrambo ZDA, vsebovano v Prilogi VII k temu sklepu, opisuje omejitve in zaščitne ukrepe, ki se uporabljajo za dostop do podatkov in njihovo uporabo s strani javnih organov pregona in za druge namene javnega interesa. Za povečanje preglednosti in izražanje pravne narave teh zavez bo vsak od dokumentov, navedenih v in priloženih temu sklepu, objavljen v zveznem registru ZDA [(*U.S. Federal Register*)].“

44 Analiza, ki jo je Komisija opravila v zvezi s temi omejitvami in zaščitnimi ukrepi, je povzeta v točkah od 67 do 135 obrazložitve Sklepa o zasebnostnem ščitu, medtem ko so ugotovitve te institucije, ki se nanašajo na ustrezno raven varstva v okviru zasebnostnega ščita EU-ZDA, navedene v točkah od 136 do 141 obrazložitve tega sklepa.

45 Natančneje, v točkah 68, 69, 76, 77, 109, od 112 do 116, 120, 136 in 140 obrazložitve tega sklepa je navedeno:

„(68) Po zakonodaji ZDA je zagotavljanje nacionalne varnosti v pristojnosti predsednika kot glavnega poveljnika, glavnega upravitelja in, kar zadeva tuje obveščevalne službe, kot pristojnega za zunanje zadev[e] ZDA […]. Ker ima kongres pristojnosti za uvedbo omejitev in je to storil v različnih primerih, lahko v okviru teh omejitev usmerja dejavnosti obveščevalne skupnosti ZDA, zlasti z odredbami ali predsedniškimi direktivami. […] Trenutno sta glavna pravna instrumenta v zvezi s tem Odredba št. 12333 […] in Predsedniška politična direktiva št. 28 (Presidential Policy Directive 28, v nadaljnjem besedilu: PPD-28).

(69) [PPD-28], objavljena 17. januarja 2014, uvaja številne omejitve za ‚obveščevalne operacije SIGINT [(signals intelligence, prestrezanje signalov)]‘ […]. Ta predsedniška direktiva je zavezujoča za obveščevalne organe ZDA […] in ostane veljavna po spremembi v administraciji ZDA […]. PPD-28 je zlasti pomembna za nedržavljane ZDA, vključno s posamezniki iz EU, na katere se nanašajo osebni podatki. […]

[…]

(76) Čeprav ta načela [iz PPD-28] niso navedena v zadevnih pravnih izrazih, zajemajo bistvo načel nujnosti in sorazmernosti. […]

(77) Tako kot direktiva, ki jo izda predsednik kot glavni upravitelj, so te zahteve zavezujoče za celotno obveščevalno skupnost in se še naprej izvajajo prek pravil in postopkov agencij[…], ki prenašajo splošna načela v posebna navodila za vsakodnevne dejavnosti. […]

[…]

(109) V nasprotju s tem pa [United States Foreign Intelligence Surveillance Court (FISC) (sodišče ZDA za nadzor nad tujimi obveščevalnimi službami)] v skladu s členom 702 [Foreign Intelligence Surveillance Act (FISA)] ne dovoljuje posameznih nadzornih ukrepov, temveč dovoljuje nadzorne programe (kot sta programa PRISM in UPSTREAM) na podlagi letnih potrdil, ki jih pripravita [United States Attorney General (generalni državni tožilec)] in [Director of National Intelligence (DNI) (direktor nacionalne obveščevalne službe)]. […] Kot je navedeno, potrdila, ki ji odobri FISC, ne vsebujejo nobenih informacij o ciljnih posameznikih, temveč so v njih opredeljene kategorije tujih obveščevalnih podatkov […]. Čeprav FISC ne presoja – na podlagi verjetnega vzroka ali katerega koli drugega standarda – ustreznosti ciljnega osredotočanja na posameznike za pridobivanje tujih obveščevalnih podatkov […], njegov nadzor zajema tudi nadzor nad izpolnjevanjem pogoja, da ‚je pomemben namen pridobivanja zbrati tuje obveščevalne podatke'. […]

[…]

(112) Prvič, zakon o nadzoru tujih obveščevalnih podatkov določa več pravnih sredstev za izpodbijanje nezakonitega elektronskega nadzora, ki so na voljo tudi nedržavljanom ZDA […]. To vključuje možnost, da posamezniki vložijo civilni zahtevek za denarno odškodnino proti ZDA, če so bile informacije o njih nezakonito in namerno uporabljene ali razkrite […], da osebno tožijo uslužbence vlade ZDA (ki so ravnali ‚pod pretvezo zakona') za denarno odškodnino […] in da izpodbijajo zakonitost nadzora (ter zahtevajo omejitev informacij), če namerava vlada ZDA uporabiti ali razkriti kakršne koli informacije, ki so pridobljene ali izhajajo iz elektronskega nadzora, proti posamezniku v sodnem ali upravnem postopku v ZDA […].

(113) Drugič, vlada ZDA je opozorila Komisijo na številne dodatne možnosti, ki bi jih posamezniki iz EU, na katere se nanašajo osebni podatki, lahko uporabili za pritožbo proti vladnim uslužbencem zaradi nezakonitega vladnega dostopa do osebnih podatkov ali njihove uporabe, tudi za domnevne namene nacionalne varnosti […].

(114) Nenazadnje je vlada ZDA opozorila, da je [Freedom of Information Act (FOIA) (zakon o dostopu do informacij javnega značaja)] sredstvo, s pomočjo katerega lahko nedržavljani ZDA zahtevajo dostop do obstoječih evidenc zvezne agencije, tudi če te evidence vsebujejo osebne podatke posameznika […]. Zakon o dostopu do informacij javnega značaja se ne osredotoča na določanje možnosti uporabe individualnih pravnih sredstev proti posegom v osebne podatke kot take, čeprav bi lahko posameznikom načeloma omogočal, da pridobijo dostop do ustreznih informacij, ki jih hranijo nacionalne obveščevalne agencije. […]

(115) Čeprav imajo zato posamezniki, vključno s posamezniki iz EU, na katere se nanašajo osebni podatki, na voljo različne možnosti pravnega varstva, če so predmet nezakonitega (elektronskega) nadzora za namene nacionalne varnosti, je prav tako jasno, da vsaj nekatere pravne podlage, ki jih lahko uporabijo obveščevalni organi ZDA (npr. Odredba št. 12333), niso zajete. Poleg tega so tudi kadar za nedržavljane ZDA načeloma obstajajo možnosti pravnega varstva, kot na primer pri nadzoru v skladu s FISA, razpoložljive možnosti za ukrepanje omejene […] in zahtevki posameznikov (vključno z državljani ZDA) se razglasijo za nedopustne, če ne morejo dokazati pravnega interesa […], kar omejuje dostop do rednih sodišč […].

(116) Da bi zagotovila dodatne možnosti pravnega varstva, ki bi bile na voljo vsem posameznikom iz EU, na katere se nanašajo osebni podatki, se je vlada ZDA odločila, da bo ustvarila nov mehanizem varuha človekovih pravic, kot je določen v dopisu državnega sekretarja [ministra za zunanje zadeve] ZDA Komisiji, ki je priložen v Prilogi III k temu sklepu. Ta mehanizem temelji na imenovanju visokega koordinatorja (na ravni podsekretarja) na zunanjem ministrstvu v skladu s PPD-28 kot kontaktne točke za tuje vlade, na katero lahko naslovijo vprašanja v zvezi z obveščevalnimi dejavnostmi SIGINT ZDA, vendar bistveno presega prvotni koncept.

[…]

(120) Vlada ZDA se zavezuje, da bo zagotovila, da si bo varuh človekovih pravic na področju zasebnostnega ščita pri opravljanju svojih nalog lahko zagotovil sodelovanje drugih mehanizmov za nadzor in pregled skladnosti, ki jih določa pravo ZDA. […] Če kateri koli od teh nadzornih organov odkrije neskladnost, bo moral zadevni organ obveščevalne skupnosti (npr. obveščevalna agencija) odpraviti neskladnosti, saj bo varuh človekovih pravic le tako lahko predložil ‚pozitiven' odgovor posamezniku (tj. da je bila morebitna neskladnost odpravljena), h kateremu se je vlada ZDA zavezala. […]

[…]

(136) Ob upoštevanju navedenih ugotovitev Komisija meni, da ZDA zagotavljajo ustrezno stopnjo varstva osebnih podatkov, ki se v okviru zasebnostnega ščita EU-ZDA prenašajo iz Unije samocertificiranim organizacijam.

[…]

(140) Nenazadnje, Komisija na podlagi razpoložljivih informacij o pravnem redu ZDA, vključno z zavezami vlade ZDA, meni, da bodo kakršni koli posegi javnih organov ZDA v temeljne pravice oseb, katerih podatki se v okviru zasebnostnega ščita prenašajo iz Unije v ZDA za namene nacionalne varnosti, kazenskega pregona ali drugih javnih interesov, in iz tega izhajajoče omejitve, uvedene za samocertificirane organizacije v zvezi z njihovim spoštovanjem načel, omejeni na tisto, kar je nujno potrebno za doseganje zadevnega zakonitega cilja, in da obstaja učinkovito pravno varstvo pred takim posegom."

46 Člen 1 Sklepa o zasebnostnem ščitu določa:

„1. Za namene člena 25(2) Direktive [95/46] ZDA zagotavljajo ustrezno raven varstva osebnih podatkov, ki se v okviru zasebnostnega ščita EU-ZDA prenašajo iz Unije organizacijam v ZDA.

2. Zasebnostni ščit EU-ZDA sestavljajo načela, ki jih je 7. julija 2016 izdalo Ministrstvo za trgovino ZDA, kakor so navedena v Prilogi II, ter uradna zagotovila in zaveze iz dokumentov, navedenih v prilogah I in III–VII.

3. Za namene odstavka 1 se osebni podatki prenašajo v okviru zasebnostnega ščita EU-ZDA, kadar se prenašajo iz Unije organizacijam v ZDA, ki so vključene na ‚seznam zasebnostnega ščita', ki ga vodi in objavlja Ministrstvo za trgovino ZDA, v skladu s členoma I in III načel iz Priloge II."

47 V Prilogi II k Sklepu o zasebnostnem ščitu, naslovljeni „Načela okvira zasebnostnega ščita EU-ZDA izdalo Ministrstvo za trgovino ZDA", je v točki I.5 navedeno, da je zavezanost k tem načelom lahko omejena, če je to potrebno, med drugim za izpolnjevanje „zahtev nacionalne varnosti, javnega interesa ali kazenskega pregona".

48 Priloga III k temu sklepu vsebuje dopis Johna Kerryja, takratnega Secretary of State (minister za zunanje zadeve, Združene države), komisarki za pravosodje, potrošnike in enakost spolov z dne 7. julija 2016, ki mu je v prilogi A priložen memorandum z naslovom „Mehanizem varuha človekovih pravic na področju zasebnostnega ščita EU-ZDA v zvezi z obveščevalno dejavnostjo SIGINT", ki vsebuje ta odlomek:

„Ob priznanju pomembnosti okvira zasebnostnega ščita EU-ZDA ta memorandum določa proces za izvedbo novega mehanizma, skladno s [PPD-28], v zvezi z obveščevalno dejavnostjo SIGINT.

[…] Predsednik Obama je objavil, da bo izdal novo predsedniško direktivo – PPD-28 – s katero bo ‚jasno predpisal, kaj počnemo in česa ne počnemo pri našem čezmorskem nadzoru‘.

Člen 4(d) PPD-28 določa, da mora zunanji minister imenovati ‚višjega koordinatorja za mednarodno diplomacijo v informacijski tehnologiji‘ (višji koordinator), ‚ki bo … služil kot oseba za stike s tujimi vladami, ki želijo sprožiti vprašanja v zvezi z obveščevalnimi dejavnostmi SIGINT, ki jih izvajajo Združene države‘.

[…]

1. […] Višji koordinator bo deloval kot varuh človekovih pravic na področju zasebnostnega ščita in […] bo tesno sodeloval z ustreznimi uradniki iz drugih Ministrstev in agencij, ki so odgovorni za obdelavo zahtevkov v skladu z veljavno zakonodajo in politiko Združenih držav. Varuh človekovih pravic je neodvisen od obveščevalnih skupnosti. Varuh človekovih pravic poroča neposredno zunanjemu ministru, ki zagotovi, da varuh človekovih pravic opravlja svoje funkcije objektivno in neodvisno od neprimernega vpliva, ki bi lahko imel učinek na odgovor.

[…]“

49 Priloga VI k Sklepu o zasebnostnem ščitu vsebuje dopis urada direktorja nacionalne obveščevalne službe (Office of the Director of National Intelligence) ameriškemu ministrstvu za trgovino in upravi za mednarodno trgovino z dne 21. junija 2016, v katerem je pojasnjeno, da PPD-28 omogoča „‚množično‘ zbiranje […] relativno velikega obsega obveščevalnih informacij ali podatkov SIGINT v okoliščinah, v katerih obveščevalna skupnost ne more uporabiti identifikatorja, povezanega z določeno ciljno osebo […], da bi osredotočila zbiranje“.

Spor o glavni stvari in vprašanja za predhodno odločanje

50 M. Schrems, avstrijski državljan, ki prebiva v Avstriji, od leta 2008 uporablja družbeno omrežje Facebook (v nadaljevanju: Facebook).

51 Vse osebe, ki prebivajo na ozemlju Unije in želijo uporabljati Facebook, morajo ob registraciji podpisati pogodbo z družbo Facebook Ireland, ki je hčerinska družba Facebook Inc. s sedežem v Združenih državah. Osebni podatki uporabnikov Facebooka, ki prebivajo na ozemlju Unije, se v celoti ali delno prenesejo na strežnike družbe Facebook Inc., ki so na ozemlju Združenih držav in na katerih se obdelujejo.

52 M. Schrems je 25. junija 2013 pri pooblaščencu vložil pritožbo, v kateri je v bistvu predlagal, naj se družbi Facebook Ireland prepove prenos njegovih osebnih podatkov v Združene države, pri čemer je trdil, da veljavna zakonodaja in praksa v tej državi ne zagotavljata zadostnega varstva osebnih podatkov, ki se hranijo na njenem ozemlju, pred dejavnostmi nadzora, ki jih tam izvajajo javni organi. Ta pritožba je bila zavrnjena med drugim zato, ker je Komisija v Odločbi 2000/520 ugotovila, da Združene države zagotavljajo ustrezno raven varstva.

53 High Court (višje sodišče, Irska), pri katerem je M. Schrems vložil tožbo zoper zavrnitev njegove pritožbe, je pri Sodišču vložilo predlog za sprejetje predhodne odločbe, ki se je nanašal na razlago in veljavnost Odločbe 2000/520. Sodišče je s sodbo z dne 6. oktobra 2015, Schrems (C-362/14, EU:C:2015:650), to odločbo razglasilo za neveljavno.

54 Predložitveno sodišče je na podlagi te sodbe razveljavilo odločbo, s katero je bila pritožba M. Schremsa zavrnjena, in zadevo vrnilo v odločanje pooblaščencu. V okviru preiskave, ki jo je začel pooblaščenec, je družba Facebook Ireland pojasnila, da je bil velik del osebnih podatkov prenesen na družbo Facebook Inc. na podlagi standardnih določil o varstvu podatkov iz Priloge k Sklepu SPK. Glede na ta dejstva je pooblaščenec M. Schremsa pozval, naj pritožbo spremeni.

55 V tako spremenjeni pritožbi, ki je bila vložena 1. decembra 2015, je M. Schrems med drugim trdil, da ameriško pravo družbi Facebook Inc. nalaga, da osebne podatke, ki so bili posredovani tej družbi, da na voljo ameriškim organom, kot sta National Security Agency (NSA) in Federal Bureau of Investigation (FBI). Trdil je, da so bili ti podatki v okviru različnih programov nadzora uporabljeni na način, ki ni združljiv s členi 7, 8 in 47 Listine, zato prenosa navedenih podatkov v Združene države ni mogoče upravičiti s Sklepom SPK. V teh okoliščinah je M. Schrems pooblaščencu predlagal, naj prepove ali začasno ustavi prenos njegovih osebnih podatkov na družbo Facebook Inc.

56 Pooblaščenec je 24. maja 2016 objavil „osnutek odločbe“, v katerem je povzel začasne ugotovitve svoje preiskave. V tem osnutku je začasno ugotovil, da obstaja nevarnost, da bi se ameriški organi z osebnimi podatki državljanov Unije, ki so bili preneseni v Združene države, seznanili in jih obdelovali na način, ki ni skladen s členoma 7 in 8 Listine, in da pravo Združenih držav tem državljanom ne zagotavlja pravnih sredstev, ki bi bila skladna s členom 47 Listine. Pooblaščenec je ugotovil, da te pomanjkljivosti ni mogoče odpraviti s standardnimi določili o varstvu podatkov iz Priloge k Sklepu SPK, saj ta določila posameznikom, na katere se osebni podatki nanašajo, zagotavljajo le pogodbene pravice v razmerju do izvoznika in uvoznika podatkov, ne zavezujejo pa ameriških organov.

57 Ker je pooblaščenec menil, da se v teh okoliščinah v zvezi s spremenjeno pritožbo M. Schremsa postavlja vprašanje veljavnosti Sklepa SPK, se je 31. maja 2016 obrnil na High Court (višje sodišče) – pri čemer se je oprl na sodno prakso, ki izhaja iz sodbe z dne 6. oktobra 2015, Schrems (C-362/14, EU:C:2015:650, točka 65) – da bi omenjeno sodišče Sodišču postavilo to vprašanje. High Court (višje sodišče) je z odločbo z dne 4. maja 2018 pri Sodišču vložilo ta predlog za sprejetje predhodne odločbe.

58 High Court (višje sodišče) je temu predlogu za sprejetje predhodne odločbe priložilo sodbo z dne 3. oktobra 2017, v kateri je opisalo rezultat presoje dokazov, ki so mu bili predloženi v okviru nacionalnega postopka, v katerem je sodelovala ameriška vlada.

59 V tej sodbi, na katero se v predlogu za sprejetje predhodne odločbe večkrat sklicuje, je predložitveno sodišče poudarilo, da načeloma nima le pravice, ampak tudi obveznost, da preuči vsa navajana dejstva in trditve, ki so mu predloženi, da bi se lahko na njihovi podlagi odločilo, ali je treba predlog za sprejetje predhodne odločbe vložiti. Vsekakor bi moralo upoštevati morebitne spremembe zakonodaje, do katerih je prišlo med vložitvijo tožbe in obravnavo na tem sodišču. Predložitveno sodišče je pojasnilo, da v okviru postopka v glavni stvari njegova presoja ni omejena na razloge za neveljavnost, ki jih je navedel pooblaščenec, tako da lahko po uradni dolžnosti upošteva tudi druge razloge za neveljavnost in na njihovi podlagi vloži predlog za sprejetje predhodne odločbe.

60 Iz ugotovitev v navedeni sodbi izhaja, da obveščevalne dejavnosti ameriških organov v zvezi z osebnimi podatki, prenesenimi v Združene države, urejata zlasti člen 702 FISA in Odredba št. 12333.

61 V zvezi s členom 702 FISA predložitveno sodišče v isti sodbi pojasnjuje, da ta člen generalnemu državnemu tožilcu in direktorju nacionalne obveščevalne službe omogoča, da na podlagi odobritve FISC za pridobitev „tujih obveščevalnih podatkov“ skupaj dovolita nadzor neameriških državljanov, ki so zunaj ozemlja Združenih držav, poleg tega pa je ta člen med drugim podlaga za programe nadzora PRISM in UPSTREAM. Po ugotovitvah tega sodišča morajo ponudniki spletnih storitev v okviru programa PRISM NSA posredovati vsa sporočila, ki jih pošlje in prejme „izbirnik“, pri čemer se nekatera od teh sporočil posredujejo tudi FBI in Central Intelligence Agency (CIA, centralna obveščevalna agencija).

62 V zvezi s programom UPSTREAM je navedeno sodišče ugotovilo, da so v okviru tega programa telekomunikacijska podjetja, ki upravljajo „hrbtenico“ spleta – to je omrežje kablov, stikal in usmerjevalnikov – prisiljena NSA omogočiti kopiranje in filtriranje tokov spletnega prometa za zbiranje komunikacij, ki jih pošlje ali prejme neameriški državljan, na katerega se nanaša „izbirnik“, ali ki so v zvezi s tem državljanom. V okviru navedenega programa ima NSA po ugotovitvah tega sodišča dostop tako do metapodatkov kot do vsebine zadevnih komunikacij.

63 Predložitveno sodišče je v zvezi z Odredbo št. 12333 ugotovilo, da ta odredba NSA omogoča dostop do podatkov „v tranzitu“ proti Združenim državam, tako da omogoča dostop do podmorskih kablov, nameščenih na dnu Atlantika, ter zbiranje in hrambo podatkov, še preden ti prispejo v Združene države in se zanje uporabijo določbe FISA. Pojasnilo je, da dejavnosti, ki se izvajajo na podlagi Odredbe št. 12333, niso urejene z zakonom.

64 Glede omejitev obveščevalnih dejavnosti predložitveno sodišče poudarja dejstvo, da se za neameriške osebe uporablja zgolj PPD-28 in da ta vsebuje zgolj navedbo, da bi morale biti obveščevalne dejavnosti „čim bolj usmerjene“ (*as tailored as feasible*). Navedeno sodišče na podlagi svojih ugotovitev meni, da Združene države izvajajo množično obdelavo podatkov, ne da bi zagotavljale v bistvu enakovredno varstvo, kot ga zagotavljata člena 7 in 8 Listine.

65 V zvezi s sodnim varstvom to sodišče navaja, da državljani Unije nimajo na voljo enakih pravnih sredstev zoper obdelavo osebnih podatkov s strani ameriških organov kot ameriški državljani, ker se četrti amandma Constitution of the United States (ustava Združenih držav), ki v ameriškem pravu pomeni največje varstvo pred nezakonitim nadzorom, ne uporablja za državljane Unije. V zvezi s tem predložitveno sodišče pojasnjuje, da pravna sredstva, ki so zadnjenavedenim na voljo, vsebujejo velike ovire, zlasti obveznost – ki jo je po mnenju tega sodišča pretirano težko izpolniti – da izkažejo svoje procesno upravičenje. Poleg tega to sodišče navaja, da dejavnosti, ki jih NSA opravlja na podlagi Odredbe št. 12333, niso predmet sodnega nadzora in zoper njih ni mogoče vložiti pravnega sredstva pred sodišči. Nazadnje, navedeno sodišče meni, da varuh človekovih pravic na področju zasebnostnega ščita ni sodišče v smislu člena 47 Listine, zaradi česar ameriško pravo državljanom Unije ne zagotavlja ravni varstva, ki bi bila v bistvu enakovredna ravni varstva, ki se zagotavlja s temeljno pravico iz tega člena.

66 Predložitveno sodišče v predlogu za sprejetje predhodne odločbe še pojasnjuje, da se stranki iz postopka v glavni stvari ne strinjata zlasti glede vprašanja uporabe prava Unije v primerih, v katerih se v tretjo državo prenašajo osebni podatki, ki jih lahko organi te države obdelujejo med drugim za namene nacionalne varnosti, in glede elementov, ki jih je treba upoštevati pri presoji ustrezne ravni varstva, ki jo zagotavlja navedena država. To sodišče zlasti navaja, da po mnenju družbe Facebook Ireland ugotovitve Komisije v zvezi z ustreznostjo ravni varstva, ki jo zagotavlja tretja država, kot so navedene v Sklepu o zasebnostnem ščitu, zavezujejo nadzorne organe tudi v okviru prenosa osebnih podatkov, ki temelji na standardnih določilih o varstvu podatkov iz Priloge k Sklepu SPK.

67 V zvezi s temi standardnimi določili o varstvu podatkov se omenjeno sodišče sprašuje, ali je Sklep SPK mogoče šteti za veljaven kljub temu, da – kot navaja to sodišče – ta določila za državne organe zadevne tretje države niso zavezujoča in zato z njimi ni mogoče odpraviti morebitnega neobstoja ustrezne ravni varstva v tej državi. V zvezi s tem predložitveno sodišče meni, da možnost, ki jo imajo pristojni organi držav članic na podlagi člena 4(1)(a) Sklepa 2010/87 v različici, ki je veljala pred začetkom veljavnosti Izvedbenega sklepa 2016/2297, in sicer da prepovejo prenos osebnih podatkov v tretjo državo, ki uvozniku podatkov nalaga obveznosti, ki niso združljive z jamstvi, vsebovanimi v teh standardnih določilih, kaže na to, da je zaradi stanja prava v tretji državi prepoved prenosa podatkov lahko upravičena tudi v primeru, če se ta prenos opravi na podlagi standardnih določil o varstvu podatkov iz Priloge k Sklepu SPK, iz česar je razvidna možnost, da ta določila ne zadostujejo, da bi se zagotovilo ustrezno varstvo. Ob tem se predložitveno sodišče sprašuje o obsegu pooblastila pooblaščenca, da prepove prenos podatkov, ki temelji na teh določilih, pri čemer meni, da diskrecijska pravica ne zadostuje za zagotovitev ustreznega varstva.

68 V teh okoliščinah je High Court (višje sodišče) prekinilo odločanje in Sodišču v predhodno odločanje predložilo ta vprašanja:

„1. Ali v okoliščinah, kadar zasebno podjetje iz države članice [Unije] prenese osebne podatke zasebnemu podjetju v tretji državi v komercialne namene v skladu s Sklepom [SPK] in jih lahko v tretji državi nadalje obdelujejo njeni organi zaradi nacionalne varnosti, pa tudi zaradi kazenskega pregona in vodenja zunanjih zadev tretje države, pravo [Unije,] vključno z Listino […][,] velja za prenos podatkov ne glede na določbe člena 4(2) PEU v zvezi z nacionalno varnostjo in določbe prve alinee člena 3(2) Direktive [95/46] v zvezi z javno varnostjo, obrambo in varnostjo države?

2. (a) Ali so pri odločanju o tem, ali obstaja kršitev pravic posameznika zaradi prenosa podatkov iz [Unije] v tretjo državo v skladu s Sklepom [SPK], pri čemer se v tej tretji državi lahko dalje obdelujejo zaradi nacionalne varnosti, pomembno merilo primerjave v smislu Direktive [95/46]:
   (i) Listina, PEU, PDEU, Direktiva [95/46], [Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin, podpisana v Rimu 4. novembra 1950] (ali katera koli druga določba prava [Unije],) ali
   (ii) nacionalni zakoni ene ali več držav članic?
   (b) Ali je treba v primeru, v katerem so pomembno merilo primerjave [(zakoni iz točke ii)], vanje vključiti tudi prakse v okviru nacionalne varnosti v eni ali več državah članicah?

3. Ali je treba pri ocenjevanju, ali tretja država zagotavlja raven varnosti, ki jo zahteva pravo [Unije] za osebne podatke, ki se prenesejo v to državo v smislu člena 26 Direktive [95/46], raven varstva v tretji državi ocenjevati s sklicevanjem na:
   (a) veljavna pravila v tretji državi, ki izhajajo iz domačega prava ali mednarodnih zavez, in prakso, oblikovano za zagotavljanje skladnosti s temi pravili, vključno s strokovnimi pravili in varnostnimi ukrepi, upoštevanimi v tretji državi,

   ali
   (b) pravila iz točke (a), skupaj s takimi upravnimi in regulativnimi praksami in praksami za zagotavljanje skladnosti, zaščitnimi političnimi ukrepi, postopki, protokoli, mehanizmi nadzora in izvensodnimi sredstvi, ki veljajo v tretji državi?

4. Ali so glede na dejstva, ki jih je ugotovilo High Court (višje sodišče) v zvezi s pravom [Združenih držav], če se osebni podatki prenesejo iz [Unije v Združene države] v skladu s Sklepom [SPK], s tem kršene pravice posameznikov v skladu s členoma 7 in/ali 8 Listine?

5. Glede na dejstva, ki jih je ugotovilo High Court (višje sodišče) v zvezi s pravom [Združenih držav], če se osebni podatki prenesejo iz [Unije v Združene države] v skladu s Sklepom [SPK]:
   (a) Ali raven varstva, ki jo nudijo [Združene države], spoštuje bistveno vsebino pravice posameznika do pravnega sredstva v primeru kršitve njegovih pravic do varstva podatkov, ki jih zagotavlja člen 47 Listine?

   Če je odgovor na vprašanje (a) pritrdilen:
   (b) Ali so omejitve, ki jih pravo [Združenih držav] nalaga v zvezi s pravico posameznika do pravnega sredstva v okviru nacionalne varnosti [Združenih držav], sorazmerne v smislu člena 52 Listine in ne presegajo tistega, kar je potrebno v demokratični družbi za namene nacionalne varnosti?

6. (a) Kakšna je raven varstva, ki jo je treba zagotoviti za prenos osebnih podatkov v tretjo državo v skladu s [standardnimi pogodbenimi določili], sprejetimi v skladu s sklepom Komisije [iz] člena 26(4) [Direktive 95/46], glede na določbe [te d]irektive ter zlasti [njenih] členov 25 in 26 ob upoštevanju Listine?

(b) Katere dejavnike je treba upoštevati pri ocenjevanju, ali raven varstva, ki se zagotavlja za prenos podatkov v tretjo državo v skladu s Sklepom [SPK], izpolnjuje zahteve Direktive [95/46] in Listine?

7. Ali dejstvo, da se [standardna določila o varstvu podatkov] uporabljajo med izvoznikom podatkov in uvoznikom podatkov ter ne zavezujejo nacionalnih organov tretje države, ki lahko od uvoznika podatkov zahtevajo, naj osebne podatke, prenesene v skladu s klavzulami iz Sklepa [SPK], da na voljo varnostnim službam te države za nadaljnjo obdelavo, izključuje, da te klavzule zagotavljajo ustrezne zaščitne ukrepe, kakor to določa člen 26(2) Direktive [95/46]?

8. Če za uvoznika podatkov iz tretje države velja zakonodaja o nadzoru, ki je glede na [organ, pristojen za varstvo podatkov,] v navzkrižju s [standardnimi pogodbenimi določili] […] ali s členoma 25 in 26 Direktive [95/46] in/ali Listino, ali mora [organ, pristojen za varstvo podatkov,] uporabiti svoja izvršilna pooblastila v skladu s členom 28(3) Direktive [95/46] za prekinitev pretoka podatkov ali je izvajanje takih pooblastil omejeno le na izjemne primere glede na [uvodno izjavo 11 Sklepa SPK] ali pa lahko [organ, pristojen za varstvo podatkov,] uporabi svojo diskrecijsko pravico, da ne prekine pretoka podatkov?

9. (a) Ali Sklep [o zasebnostnem ščitu] v smislu člena 25(6) Direktive [95/46] predstavlja ugotovitev o splošni uporabi, ki [organe, pristojne za varstvo podatkov,] in sodišča držav članic zavezuje tako, da se šteje, da [Združene države] zagotavljajo ustrezno raven varstva v smislu člena 25(2) Direktive [95/46] zaradi njihovega domačega prava ali mednarodnih zavez, ki so jih sklenile?
(b) Če to ni tako, kakšen pomen, če sploh kakšen, ima Sklep [o zasebnostnem ščitu] pri ocenjevanju glede ustreznosti zaščitnih ukrepov, zagotovljenih za prenesene podatke v [Združene države], ki se prenašajo v skladu s Sklepom [SPK]?

10. Ali glede na ugotovitve High Court (višje sodišče) v zvezi s pravom [Združenih držav] določba o varuhu človekovih pravic na področju zasebnostnega ščita v skladu s [Prilogo A k Prilogi III] k Sklepu [o zasebnostnem ščitu] v zvezi z obstoječim režimom v [Združenih državah] zagotavlja pravno sredstvo za posameznike, na katere se nanašajo osebni podatki, ki se prenesejo v [Združene države] v skladu s Sklepom [SPK], ki je skladno s členom 47 Listine?

11. Ali Sklep [SPK] krši člene 7, 8 in/ali 47 Listine?“

Dopustnost predloga za sprejetje predhodne odločbe

69 Družba Facebook Ireland ter nemška vlada in vlada Združenega kraljestva trdijo, da predlog za sprejetje predhodne odločbe ni dopusten.

70 Družba Facebook Ireland navaja, da so bile določbe Direktive 95/46, na katerih temeljijo vprašanja za predhodno odločanje, razveljavljene s Splošno uredbo o varstvu podatkov.

71 Čeprav je v zvezi s tem res, da je bila Direktiva 95/46 na podlagi člena 94(1) Splošne uredbe o varstvu podatkov razveljavljena z učinkom od 25. maja 2018, je ta direktiva 4. maja 2018, ko je bil oblikovan ta predlog za sprejetje predhodne odločbe, ki je na Sodišče prispel 9. maja 2018, še veljala. Poleg tega so bili člen 3(2), prva alinea, člena 25 in 26 ter člen 28(3) Direktive 95/46, na katere se nanašajo vprašanja za predhodno odločanje, v bistvu povzeti v členu 2(2) ter členih 45, 46 in 58 Splošne uredbe o varstvu podatkov. Poleg tega je treba opozoriti, da je naloga Sodišča, da razloži vse določbe prava Unije, ki jih nacionalna sodišča potrebujejo za odločanje v sporih, ki so jim predloženi, tudi če te določbe niso izrecno navedene v vprašanjih, ki jih ta sodišča postavijo (sodba z dne 2. aprila 2020, Ruska Federacija, C-897/19 PPU, EU:C:2020:262, točka 43 in navedena sodna praksa). Iz teh različnih razlogov

okoliščina, da je predložitveno sodišče vprašanja za predhodno odločanje oblikovalo tako, da se je sklicevalo le na določbe Direktive 95/46, ne more povzročiti nedopustnosti tega predloga za sprejetje predhodne odločbe.

72 Nemška vlada ugovor nedopustnosti opira na okoliščino, prvič, da je pooblaščenec izrazil le dvome, in ne dokončnega mnenja v zvezi z vprašanjem veljavnosti Sklepa SPK, in drugič, da predložitveno sodišče ni preverilo, ali je M. Schrems nedvomno dal soglasje za prenos podatkov iz postopka v glavni stvari, zaradi česar bi bil odgovor na to vprašanje, če bi bilo to tako, brezpredmeten. Nazadnje, vlada Združenega kraljestva meni, da so vprašanja za predhodno odločanje hipotetična, ker omenjeno sodišče ni ugotovilo, da so bili ti podatki na podlagi navedenega sklepa dejansko preneseni.

73 Iz ustaljene sodne prakse Sodišča izhaja, da izključno nacionalno sodišče, ki odloča o sporu in mora prevzeti odgovornost za izdano sodno odločbo, glede na značilnosti zadeve presodi nujnost pridobitve predhodne odločbe, da bi lahko izdalo sodbo, in upoštevnost vprašanj, ki jih zastavi Sodišču. Zato Sodišče, kadar se postavljena vprašanja nanašajo na razlago ali veljavnost pravnega pravila iz prava Unije, načeloma mora odločiti. Iz tega sledi, da za vprašanja, ki jih postavijo nacionalna sodišča, velja domneva upoštevnosti. Sodišče lahko odgovor na vprašanje za predhodno odločanje, ki ga je postavilo nacionalno sodišče, zavrne le, če je očitno, da zahtevana razlaga ni v nikakršni zvezi z dejanskim stanjem ali predmetom spora o glavni stvari, če je problem hipotetičen ali če Sodišče nima na voljo pravnih in dejanskih okoliščin, ki jih potrebuje, da bi lahko na postavljena vprašanja dalo koristne odgovore (sodbe z dne 16. junija 2015, Gauweiler in drugi, C-62/14, EU:C:2015:400, točki 24 in 25; z dne 2. oktobra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, točka 45, in z dne 19. decembra 2019, Dobersberger, C-16/18, EU:C:2019:1110, točki 18 in 19).

74 V obravnavanem primeru predlog za sprejetje predhodne odločbe vsebuje dejanske in pravne elemente, ki zadostujejo za razumevanje obsega vprašanj za predhodno odločanje. Poleg tega in predvsem na podlagi nobenega elementa iz spisa, ki ga ima na voljo Sodišče, ni mogoče šteti, da zahtevana razlaga prava Unije nima zveze z dejanskim stanjem ali predmetom spora o glavni stvari ali da je hipotetična, med drugim zato, ker naj bi prenos osebnih podatkov iz postopka v glavni stvari temeljil na izrecni privolitvi osebe, ki jo ta prenos zadeva, in ne na Sklepu SPK. Iz navedb v tem predlogu za sprejetje predhodne odločbe je namreč razvidno, da je družba Facebook Ireland priznala, da družbi Facebook Inc. prenaša osebne podatke svojih naročnikov, ki prebivajo v Uniji, in da se velik del teh prenosov, katerih zakonitost M. Schrems izpodbija, opravi na podlagi standardnih določil o varstvu podatkov iz Priloge k Sklepu SPK.

75 Poleg tega na dopustnost tega predloga za sprejetje predhodne odločbe ne vpliva dejstvo, da pooblaščenec ni izrazil dokončnega mnenja o veljavnosti tega sklepa, saj predložitveno sodišče meni, da je odgovor na vprašanja za predhodno odločanje, ki se nanašajo na razlago in veljavnost pravnih pravil prava Unije, potreben za rešitev spora o glavni stvari.

76 Iz tega sledi, da je predlog za sprejetje predhodne odločbe dopusten.

Vprašanja za predhodno odločanje

77 Uvodoma je treba spomniti, da ta predlog za sprejetje predhodne odločbe izhaja iz pritožbe, s katero je M. Schrems pooblaščencu predlagal, naj odredi, da se za naprej začasno ustavi ali prepove, da družba Facebook Ireland opravi prenos njegovih osebnih podatkov družbi Facebook Inc. Čeprav se vprašanja za predhodno odločanje nanašajo na določbe Direktive 95/46, pa ni sporno, da pooblaščenec v času, ko je bila ta direktiva z učinkom od 25. maja 2018 razveljavljena in nadomeščena s Splošno uredbo o varstvu podatkov, še ni sprejel končne odločitve v zvezi s to pritožbo.

78 Zaradi dejstva, da ni bila sprejeta nacionalna odločba, se položaj iz postopka v glavni stvari razlikuje od položajev, na podlagi katerih sta bili izdani sodbi z dne 24. septembra 2019, Google (Ozemeljski obseg odstranitve povezav) (C-507/17, EU:C:2019:772), in z dne 1. oktobra 2019, Planet49 (C-673/17, EU:C:2019:801), katerih predmet so bile odločbe, ki so bile sprejete pred razveljavitvijo navedene direktive.

79 Zato je treba na vprašanja za predhodno odločanje odgovoriti ob upoštevanju določb Splošne uredbe o varstvu podatkov, in ne določb Direktive 95/46.

Prvo vprašanje

80 Predložitveno sodišče želi s prvim vprašanjem v bistvu izvedeti, ali je treba člen 2(1) in člen 2(2)(a), (b) in (d) Splošne uredbe o varstvu podatkov v povezavi s členom 4(2) PEU razlagati tako, da prenos osebnih podatkov, ki ga gospodarski subjekt s sedežem v državi članici opravi drugemu gospodarskemu subjektu s sedežem v tretji državi, če lahko organi te tretje države te podatke med tem prenosom ali po njem obdelujejo za namene javne varnosti, obrambe in državne varnosti, spada na področje uporabe te uredbe.

81 V zvezi s tem je treba najprej poudariti, da se določba iz člena 4(2) PEU, v skladu s katero znotraj Unije nacionalna varnost ostaja v izključni pristojnosti vsake države članice, nanaša izključno na države članice Unije. Zato ta določba v obravnavanem primeru ni upoštevna za razlago člena 2(1) in člena 2(2)(a), (b) in (d) Splošne uredbe o varstvu podatkov.

82 Člen 2(1) Splošne uredbe o varstvu podatkov določa, da se ta uredba uporablja za obdelavo osebnih podatkov, ki se v celoti ali delno izvaja z avtomatiziranimi sredstvi, in za obdelavo osebnih podatkov, ki so del zbirke ali so namenjeni oblikovanju dela zbirke, ki se ne izvaja z avtomatiziranimi sredstvi. Člen 4, točka 2, te uredbe pojem „obdelava“ opredeljuje kot „vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih“, pri čemer so kot primer navedeni „razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa“, brez razlikovanja glede na to, ali se ta dejanja izvajajo v Uniji ali so povezana s tretjo državo. Sicer navedena uredba za prenos osebnih podatkov v tretje države določa posebna pravila, ki so v poglavju V te uredbe z naslovom „Prenos osebnih podatkov v tretje države ali mednarodne organizacije“, poleg tega pa nadzornim organom v zvezi s tem podeljuje posebna pooblastila iz člena 58(2)(j) iste uredbe.

83 Iz tega izhaja, da dejanje, s katerim se osebni podatki iz ene države članice prenesejo v tretjo državo, pomeni obdelavo osebnih podatkov v smislu člena 4, točka 2, Splošne uredbe o varstvu podatkov, ki se opravi na ozemlju države članice, pri čemer se za to obdelavo ta uredba uporablja na podlagi svojega člena 2(1) (v zvezi s členom 2(b) in členom 3(1) Direktive 95/46 glej po analogiji sodbo z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 45 in navedena sodna praksa).

84 V zvezi z vprašanjem, ali je mogoče šteti, da je tako dejanje na podlagi člena 2(2) Splošne uredbe o varstvu podatkov izključeno iz področja uporabe te uredbe, je treba spomniti, da ta določba vsebuje izjeme, za katere se ne uporablja, kot je opredeljeno v členu 2(1) te uredbe, in da je treba te izjeme razlagati ozko (v zvezi s členom 3(2) Direktive 95/46 glej po analogiji sodbo z dne 10. julija 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, točka 37 in navedena sodna praksa).

85 Ker je bil v obravnavanem primeru prenos osebnih podatkov iz postopka v glavni stvari opravljen med družbama Facebook Ireland in Facebook Inc., to je med dvema pravnima osebama, ta prenos ne spada na področje uporabe člena 2(2)(c) Splošne uredbe o varstvu podatkov, ki se nanaša na obdelavo podatkov, ki jo opravi fizična oseba v okviru popolnoma osebne ali domače dejavnosti. Ta prenos prav tako ne spada na področje uporabe izjem iz člena 2(2)(a), (b) in (d) te uredbe, ker so dejavnosti, ki so v tem členu navedene primeroma, vedno dejavnosti držav ali drugih državnih organov, ki niso

povezane s področji dejavnosti posameznikov (v zvezi s členom 3(2) Direktive 95/46 glej po analogiji sodbo z dne 10. julija 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, točka 38 in navedena sodna praksa).

86 Zaradi dejstva, da obstaja možnost, da organi tretje države osebne podatke, ki se med dvema gospodarskima subjektoma prenesejo v komercialne namene, med prenosom ali po prenosu obdelujejo za namene javne varnosti, obrambe in državne varnosti, pa ta prenos ne more biti izključen iz področja uporabe Splošne uredbe o varstvu podatkov.

87 Poleg tega je iz besedila člena 45(2)(a) te uredbe, iz katerega izhaja obveznost, da Komisija pri ocenjevanju ustreznosti ravni varstva v tretji državi upošteva, med drugim, „ustrezno splošno in področno zakonodajo, tudi na področju javne varnosti, obrambe, nacionalne varnosti in kazenskega prava ter dostopa javnih organov do osebnih podatkov, pa tudi izvajanje take zakonodaje“, razvidno, da to, da tretja država za namene javne varnosti, obrambe in državne varnosti morda obdeluje zadevne podatke, ne vpliva na uporabo te uredbe za zadevni prenos.

88 Iz tega sledi, da zaradi dejstva, da lahko zadevne podatke organi zadevne tretje države med prenosom ali po njem obdelujejo za namene javne varnosti, obrambe in državne varnosti, takega prenosa ni mogoče izvzeti iz področja uporabe Splošne uredbe o varstvu podatkov.

89 Zato je treba na prvo vprašanje odgovoriti, da je treba člen 2(1) in (2) Splošne uredbe o varstvu podatkov razlagati tako, da prenos osebnih podatkov, ki ga gospodarski subjekt s sedežem v državi članici v komercialne namene opravi drugemu gospodarskemu subjektu s sedežem v tretji državi, spada na področje uporabe te uredbe, ne glede na to, da lahko organi te tretje države te podatke med tem prenosom ali po njem obdelujejo za namene javne varnosti, obrambe in državne varnosti.

Drugo, tretje in šesto vprašanje

90 Predložitveno sodišče z drugim, tretjim in šestim vprašanjem Sodišče v bistvu sprašuje o ravni varstva, ki se s členom 46(1) in členom 46(2)(c) Splošne uredbe o varstvu podatkov zahteva v okviru prenosa osebnih podatkov v tretjo državo, ki temelji na standardnih določilih o varstvu podatkov. To sodišče zlasti prosi Sodišče, naj pojasni elemente, ki jih je treba upoštevati pri ugotavljanju, ali je ta raven varstva pri takem prenosu zagotovljena.

91 Glede zahtevane ravni varstva iz povezane razlage teh določb izhaja, da lahko upravljavec ali obdelovalec, če ni sprejet sklep o ustreznosti na podlagi člena 45(3) te uredbe, osebne podatke v tretjo državo prenese le, če je predvidel „ustrezne zaščitne ukrepe“ in če imajo posamezniki, na katere se osebni podatki nanašajo, na voljo „izvršljive pravice in učinkovita pravna sredstva“, pri čemer se lahko ti „ustrezni zaščitni ukrepi“ zagotovijo med drugim s standardnimi določili o varstvu podatkov, ki jih sprejme Komisija.

92 Čeprav v členu 46 Splošne uredbe o varstvu podatkov ni pojasnjena narava zahtev, ki izhajajo iz tega sklicevanja na „ustrezne zaščitne ukrepe“, „izvršljive pravice“ in „učinkovita pravna sredstva“, je treba ugotoviti, da je ta člen vključen v poglavje V te uredbe, zato ga je treba razlagati ob upoštevanju člena 44 te uredbe, ki je naslovljen „Splošno načelo za prenose“ in ki določa, da se „vse določbe tega poglavja […] uporabljajo za zagotovitev, da ni ogrožena raven varstva posameznikov, ki jo zagotavlja ta uredba“. To raven varstva je zato treba zagotoviti ne glede na določbo navedenega poglavja, na podlagi katere se osebni podatki prenašajo v tretjo državo.

93 Kot je namreč generalni pravobranilec navedel v točki 117 sklepnih predlogov, je namen določb poglavja V Splošne uredbe o varstvu podatkov v skladu s ciljem, navedenim v uvodni izjavi 6 te uredbe, zagotoviti kontinuiteto visoke ravni tega varstva v primeru prenosa osebnih podatkov v tretjo državo.

94 Člen 45(1), prvi stavek, Splošne uredbe o varstvu podatkov določa, da se lahko prenos osebnih podatkov v tretjo državo dovoli na podlagi sklepa, s katerim Komisija ugotovi, da ta tretja država, ozemlje ali eden oziroma več določenih sektorjev v tej tretji državi zagotavljajo ustrezno raven varstva podatkov. V zvezi s tem se ne zahteva, da tretja država zagotavlja enako raven varstva, kot je zagotovljena v pravnem redu Unije, ampak je treba izraz „ustrezna raven varstva“, kot izhaja tudi iz uvodne izjave 104 te uredbe, razumeti tako, da zahteva, da ta tretja država na podlagi svoje nacionalne zakonodaje ali mednarodnih obveznosti, ki jih je sprejela, dejansko zagotavlja raven varstva svoboščin in temeljnih pravic, ki je v bistvu enakovredna tisti, ki se v Uniji zagotavlja s to uredbo v povezavi z Listino. Če take zahteve ne bi bilo, namen, ki je omenjen v prejšnji točki, namreč ne bi bil dosežen (v zvezi s členom 25(6) Direktive 95/46 glej po analogiji sodbo z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 73).

95 V zvezi s tem je v uvodni izjavi 107 Splošne uredbe o varstvu podatkov navedeno, da če „tretja država, ozemlje ali določen sektor v tretji državi […] ne zagotavlja več ustrezne ravni varstva podatkov […], bi se moral prenos osebnih podatkov v to tretjo državo […] prepovedati, razen če so izpolnjene zahteve iz te uredbe v zvezi s prenosi ob upoštevanju ustreznih zaščitnih ukrepov“. Glede tega je v uvodni izjavi 108 navedene uredbe pojasnjeno, da morajo ustrezni zaščitni ukrepi, ki jih mora v primeru, da sklep o ustreznosti ni sprejet, na podlagi člena 46(1) te uredbe sprejeti upravljavec ali obdelovalec, „[nadomestiti] pomanjkanje varstva podatkov v tretji državi“, da bi se „zagotovila skladnost z zahtevami glede varstva podatkov in pravicami posameznikov, na katere se nanašajo osebni podatki, ki ustrezajo obdelavi znotraj Unije“.

96 Iz tega izhaja, kot je generalni pravobranilec navedel v točki 115 sklepnih predlogov, da morajo ustrezni zaščitni ukrepi zagotavljati, da je osebam, katerih podatki se v tretjo državo prenašajo na podlagi standardnih določil o varstvu podatkov – enako kot pri prenosu na podlagi sklepa o ustreznosti – zagotovljena raven varstva, ki je v osnovi enakovredna tisti, ki je zagotovljena v Uniji.

97 Predložitveno sodišče se sprašuje tudi, ali je treba to raven varstva, ki je v bistvu enakovredna tisti, ki je zagotovljena v Uniji, določiti glede na pravo Unije, zlasti glede na pravice, zagotovljene z Listino, in/ali glede na temeljne pravice, določene z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin (v nadaljevanju: EKČP), ali glede na nacionalno pravo držav članic.

98 V zvezi s tem je treba spomniti, da čeprav so, kot potrjuje člen 6(3) PEU, temeljne pravice, ki so vsebovane v EKČP, kot splošna načela del prava Unije in čeprav člen 52(3) Listine določa, da imajo pravice iz Listine, ki ustrezajo pravicam, zagotovljenim z EKČP, enak pomen in obseg, kot sta zanje določena z navedeno konvencijo, ta konvencija, dokler Unija ne postane njena pogodbenica, ni pravni instrument, ki bi bil formalno vključen v pravni red Unije (sodbi z dne 26. februarja 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, točka 44 in navedena sodna praksa, in z dne 20. marca 2018, Menci, C-524/15, EU:C:2018:197, točka 22).

99 V teh okoliščinah je Sodišče presodilo, da je treba pravo Unije razlagati in veljavnost aktov Unije preizkusiti z vidika temeljnih pravic, ki jih zagotavlja Listina (glej po analogiji sodbo z dne 20. marca 2018, Menci, C-524/15, EU:C:2018:197, točka 24).

100 Poleg tega iz ustaljene sodne prakse izhaja, da veljavnosti določb prava Unije in – če ni izrecnega sklicevanja na nacionalno pravo držav članic – njihove razlage ni mogoče presojati z vidika tega nacionalnega prava, tudi če je to na ravni ustave, zlasti ne z vidika temeljnih pravic, kot so določene v nacionalni ustavi vsake od držav članic (glej v tem smislu sodbe z dne 17. decembra 1970, Internationale Handelsgesellschaft, 11/70, EU:C:1970:114, točka 3; z dne 13. decembra 1979, Hauer, 44/79, EU:C:1979:290, točka 14, in z dne 18. oktobra 2016, Nikiforidis, C-135/15, EU:C:2016:774, točka 28 in navedena sodna praksa).

101 Iz tega sledi, da ker na eni strani prenos osebnih podatkov, kakršen je ta v postopku v glavni stvari, ki ga gospodarski subjekt s sedežem v državi članici v komercialne namene opravi drugemu gospodarskemu subjektu s sedežem v tretji državi – kot je razvidno iz odgovora na prvo vprašanje – spada na področje uporabe Splošne uredbe o varstvu podatkov in ker je na drugi strani cilj te uredbe, kot je razvidno iz njene uvodne izjave 10, zagotoviti dosledno in visoko raven varstva posameznikov v Uniji ter s tem namenom zagotoviti dosledno in enotno uporabo pravil za varstvo svoboščin in temeljnih pravic posameznikov pri obdelavi osebnih podatkov v celotni Uniji, je treba raven varstva temeljnih pravic, ki se zahteva s členom 46(1) te uredbe, določiti na podlagi določb iste uredbe, razlaganih ob upoštevanju temeljnih pravic, ki jih zagotavlja Listina.

102 Predložitveno sodišče želi izvedeti še, katere elemente je treba upoštevati pri ugotavljanju ustreznosti ravni varstva v okviru prenosa osebnih podatkov v tretjo državo na podlagi standardnih določil o varstvu podatkov, sprejetih na podlagi člena 46(2)(c) Splošne uredbe o varstvu podatkov.

103 V zvezi s tem je treba ugotoviti, da v tej določbi sicer niso navedeni različni elementi, ki jih je treba upoštevati pri presoji ustreznosti ravni varstva, ki jo je treba zagotoviti v okviru takega prenosa, vendar pa člen 46(1) te uredbe določa, da morajo biti posameznikom, na katere se nanašajo osebni podatki, zagotovljeni ustrezni zaščitni ukrepi ter izvršljive pravice in učinkovita pravna sredstva.

104 Pri presoji, ki se zahteva v zvezi s takim prenosom, je treba med drugim upoštevati tako pogodbena določila, dogovorjena med upravljavcem ali njegovim obdelovalcem s sedežem v Uniji in prejemnikom prenosa s sedežem v zadevni tretji državi, kot – v zvezi z morebitnim dostopom javnih organov te tretje države do prenesenih osebnih podatkov – upoštevne elemente njenega pravnega sistema. V zvezi z zadnjenavedenim je treba ugotoviti, da elementi, ki jih je treba upoštevati v okviru člena 46 te uredbe, ustrezajo tistim, ki so primeroma našteti v njenem členu 45(2).

105 Zato je treba na drugo, tretje in šesto vprašanje odgovoriti, da je treba člen 46(1) in člen 46(2)(c) Splošne uredbe o varstvu podatkov razlagati tako, da je treba z ustreznimi zaščitnimi ukrepi, izvršljivimi pravicami in učinkovitimi pravnimi sredstvi, ki se zahtevajo s tema določbama zagotoviti, da je osebam, katerih osebni podatki se prenesejo v tretjo državo na podlagi standardnih določil o varstvu podatkov, zagotovljena raven varstva, ki je v bistvu enakovredna ravni varstva, ki se v Uniji zagotavlja s to uredbo v povezavi z Listino. Da bi se to doseglo, je treba pri presoji ravni varstva, ki se zagotavlja v okviru takega prenosa, med drugim upoštevati tako pogodbena določila, dogovorjena med upravljavcem ali njegovim obdelovalcem s sedežem v Uniji in prejemnikom prenosa s sedežem v tretji državi, kot – v zvezi z morebitnim dostopom javnih organov te tretje države do tako prenesenih osebnih podatkov – upoštevne elemente pravnega sistema te države, med drugim tiste, navedene v členu 45(2) navedene uredbe.

Osmo vprašanje

106 Predložitveno sodišče želi z osmim vprašanjem v bistvu izvedeti, ali je treba člen 58(2)(f) in (j) Splošne uredbe o varstvu podatkov razlagati tako, da mora pristojni nadzorni organ začasno ustaviti ali prepovedati prenos osebnih podatkov v tretjo državo, ki temelji na standardnih določilih o varstvu podatkov, ki jih je sprejela Komisija, če ta nadzorni organ meni, da ta določila v tej tretji državi niso ali ne morejo biti spoštovana ter da varstva prenesenih podatkov, ki se zahteva s pravom Unije, zlasti s členoma 45 in 46 Splošne uredbe o varstvu podatkov in z Listino, ni mogoče zagotoviti, ali tako, da je izvrševanje teh pooblastil omejeno na izjemne primere.

107 Nacionalni nadzorni organi so v skladu s členom 8(3) Listine ter členom 51(1) in členom 57(1)(a) Splošne uredbe o varstvu podatkov pristojni za nadzor nad spoštovanjem pravil Unije, ki se nanašajo na varstvo posameznikov pri obdelavi osebnih podatkov. Zato je vsak od teh organov pristojen za

preveritev, ali prenos osebnih podatkov iz države članice, ki ji ta organ pripada, v tretjo državo izpolnjuje zahteve, določene v tej uredbi (v zvezi s členom 28 Direktive 95/46 glej po analogiji sodbo z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 47).

108 Iz teh določb izhaja, da je glavna naloga nadzornih organov nadzor nad uporabo in spoštovanjem Splošne uredbe o varstvu podatkov. Izvajanje te naloge je posebej pomembno pri prenosu osebnih podatkov v tretjo državo, saj se lahko – kot je razvidno celo iz besedila uvodne izjave 116 te uredbe – „pri čezmejnem prenosu osebnih podatkov zunaj Unije […] poveča tveganje v zvezi z zmožnostjo posameznikov za uresničevanje pravic do varstva podatkov, zlasti da se zaščitijo pred nezakonito uporabo ali razkritjem navedenih podatkov“. V tem primeru, kot je pojasnjeno v isti uvodni izjavi, „lahko nadzorni organi ugotovijo, da ne morejo obravnavati pritožb ali izvesti preiskav v zvezi z dejavnostmi zunaj svojih meja“.

109 Poleg tega mora v skladu s členom 57(1)(f) Splošne uredbe o varstvu podatkov vsak nadzorni organ na svojem ozemlju obravnavati pritožbe, ki jih lahko v skladu s členom 77(1) te uredbe vloži vsaka oseba, kadar meni, da obdelava osebnih podatkov, ki se nanašajo nanjo, pomeni kršitev navedene uredbe, in v ustreznem obsegu preučiti vsebino pritožbe. Nadzorni organ mora tako pritožbo obravnavati z vso potrebno skrbnostjo (v zvezi s členom 25(6) Direktive 95/46 glej po analogiji sodbo z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 63).

110 Člen 78(1) in (2) Splošne uredbe o varstvu podatkov vsakomur priznava pravico do učinkovitega pravnega sredstva, med drugim kadar nadzorni organ ne obravnava njegove pritožbe. Tudi v uvodni izjavi 141 te uredbe je omenjena ta „pravica do učinkovitega pravnega sredstva v skladu s členom 47 Listine“, če ta nadzorni organ „ne ukrepa, kadar je tak ukrep potreben za zaščito pravic posameznika, na katerega se nanašajo osebni podatki“.

111 Za obravnavo vloženih pritožb daje člen 58(1) Splošne uredbe o varstvu podatkov vsakemu nadzornemu organu obširna preiskovalna pooblastila. Kadar tak organ po koncu preiskave presodi, da oseba, katere osebni podatki so bili preneseni v tretjo državo, v tej državi nima zagotovljene ustrezne ravni varstva, se mora na podlagi prava Unije ustrezno odzvati, da bi odpravil ugotovljeno pomanjkljivost, in to ne glede na izvor ali naravo te pomanjkljivosti. Za to so v členu 58(2) te uredbe našteti različni popravljalni ukrepi, ki jih nadzorni organ lahko sprejme.

112 Čeprav je za izbiro ustreznega in potrebnega sredstva pristojen nadzorni organ in mora ta to izbiro opraviti ob upoštevanju vseh okoliščin zadevnega prenosa osebnih podatkov, mora ta organ kljub temu z vso potrebno skrbnostjo opraviti svojo nalogo zagotavljanja doslednega spoštovanja Splošne uredbe o varstvu podatkov.

113 V zvezi s tem in kot je generalni pravobranilec prav tako navedel v točki 148 sklepnih predlogov, mora ta organ v skladu s členom 58(2)(f) in (j) te uredbe začasno ustaviti ali prepovedati prenos osebnih podatkov v tretjo državo, če glede na vse okoliščine tega prenosa meni, da v tej tretji državi standardna določila o varstvu podatkov niso ali ne morejo biti spoštovana in da varstva prenesenih podatkov, kot se zahteva v pravu Unije, ni mogoče zagotoviti na noben drug način, kadar upravljavec ali njegov obdelovalec s sedežem v Uniji nista sama začasno ustavila prenosa ali z njim prenehala.

114 Razlage iz prejšnje točke ni mogoče ovreči s trditvijo pooblaščenca, da je bila s členom 4 Sklepa 2010/87 v različici pred začetkom veljavnosti Izvedbenega sklepa 2016/2297 v povezavi z uvodno izjavo 11 tega sklepa pristojnost nadzornih organov, da začasno ustavijo ali prepovejo prenos osebnih podatkov v tretjo državo, omejena na nekatere izjemne primere. V členu 4 Sklepa SPK, kakor je bil spremenjen z Izvedbenim sklepom 2016/2297, je namreč omenjena pristojnost, ki jo imajo zdaj ti organi na podlagi člena 58(2)(f) in (j) Splošne uredbe o varstvu podatkov, da začasno ustavijo ali prepovejo tak prenos, ne da bi bilo izvajanje te pristojnosti kakor koli omejeno na izjemne okoliščine.

115 Nikakor pa izvršilna pooblastila, ki jih ima Komisija na podlagi člena 46(2)(c) Splošne uredbe o varstvu podatkov za sprejemanje standardnih določil o varstvu podatkov, Komisiji ne dajejo pristojnosti, da bi omejevala pooblastila, ki jih imajo nadzorni organi na podlagi člena 58(2) te uredbe (v zvezi s členom 25(6) in členom 28 Direktive 95/46 glej po analogiji sodbo z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točki 102 in 103). Poleg tega je v točki 5 obrazložitve Izvedbenega sklepa 2016/2297 potrjeno, da Sklep SPK „nadzornim organom ne preprečuje izvrševanja njihovih pristojnosti za nadzor pretoka podatkov, vključno s pooblastilom za začasno ustavitev ali prepoved prenosa osebnih podatkov, če se ugotovi, da izvajanje prenosa krši zakonodajo EU ali nacionalno zakonodajo o varstvu podatkov“.

116 Kljub temu je treba pojasniti, da mora pristojni nadzorni organ v celoti spoštovati sklep, v katerem je Komisija, glede na okoliščine, na podlagi člena 45(1), prvi stavek, Splošne uredbe o varstvu podatkov ugotovila, da neka tretja država zagotavlja ustrezno raven varstva. V takem primeru namreč iz člena 45(1), drugi stavek, te uredbe v povezavi z njeno uvodno izjavo 103 izhaja, da se lahko osebni podatki v zadevno tretjo državo prenesejo, ne da bi bilo treba pridobiti posebno dovoljenje.

117 Na podlagi člena 288, četrti odstavek, PDEU je sklep o ustreznosti v vseh svojih elementih zavezujoč za vse države članice naslovnice in ga morajo vsi njihovi organi upoštevati v delu, v katerem je v njem ugotovljeno, da zadevna tretja država zagotavlja ustrezno raven varstva, in v katerem se z njim dovoljuje prenos podatkov (v zvezi s členom 25(6) Direktive 95/46 glej po analogiji sodbo z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 51 in navedena sodna praksa).

118 Zato, dokler Sodišče sklepa o ustreznosti ne razglasi za neveljavnega, države članice in njihovi organi, med katere spadajo tudi njihovi neodvisni nadzorni organi, ne smejo sprejeti ukrepov v nasprotju s tem sklepom, kot so akti, v katerih se z zavezujočim učinkom ugotovi, da tretja država, na katero se nanaša ta sklep, ne zagotavlja ustrezne ravni varstva (sodba z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 52 in navedena sodna praksa), in tako začasno ustaviti ali prepovedati prenosa osebnih podatkov v to tretjo državo.

119 Vendar pa sklep Komisije o ustreznosti, sprejet na podlagi člena 45(3) Splošne uredbe o varstvu podatkov, osebam, katerih osebni podatki so bili ali bi lahko bili preneseni v tretjo državo, ne preprečuje tega, da bi na podlagi člena 77(1) Splošne uredbe o varstvu podatkov pri pristojnem nacionalnem nadzornem organu vložile pritožbo z namenom varstva njihovih pravic in svoboščin pri obdelavi teh podatkov. Poleg tega s takim sklepom ni mogoče niti razveljaviti niti zmanjšati pooblastil, ki so nacionalnim nadzornim organom izrecno priznana s členom 8(3) Listine ter členom 51(1) in členom 57(1)(a) navedene uredbe (v zvezi s členom 25(6) in členom 28 Direktive 95/46 glej po analogiji sodbo z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 53).

120 Tako mora pristojni nacionalni nadzorni organ, pri katerem oseba vloži pritožbo z namenom varstva njenih pravic in svoboščin pri obdelavi osebnih podatkov, ki se nanjo nanašajo, tudi če obstaja sklep Komisije o ustreznosti, imeti možnost popolnoma neodvisno preučiti, ali se pri prenosu teh podatkov izpolnjujejo zahteve iz Splošne uredbe o varstvu podatkov, in po potrebi na nacionalna sodišča vložiti tožbo zato, da ta sodišča, če se strinjajo s pomisleki tega organa glede veljavnosti sklepa o ustreznosti, sprožijo postopek predhodnega odločanja za preučitev te veljavnosti (v zvezi s členom 25(6) in členom 28 Direktive 95/46 glej po analogiji sodbo z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točki 57 in 65).

121 Glede na navedeno je treba na osmo vprašanje odgovoriti, da je treba člen 58(2)(f) in (j) Splošne uredbe o varstvu podatkov razlagati tako, da mora pristojni nadzorni organ, razen če obstaja sklep o ustreznosti, ki ga je veljavno sprejela Komisija, začasno ustaviti ali prepovedati prenos osebnih podatkov v tretjo državo, ki temelji na standardnih določilih o varstvu podatkov, ki jih je sprejela Komisija, če ta nadzorni organ glede na vse okoliščine tega prenosa meni, da ta določila v tej tretji državi niso ali ne morejo biti spoštovana ter da varstva prenesenih podatkov, ki se zahteva s pravom

Unije, zlasti s členoma 45 in 46 Splošne uredbe o varstvu podatkov in z Listino, ni mogoče zagotoviti na noben drug način, kadar upravljavec ali njegov obdelovalec s sedežem v Uniji nista sama začasno ustavila prenosa ali z njim prenehala.

Sedmo in enajsto vprašanje

122 Predložitveno sodišče s sedmim in enajstim vprašanjem, ki ju je treba obravnavati skupaj, Sodišče v bistvu sprašuje o veljavnosti Sklepa SPK glede na člene 7, 8 in 47 Listine.

123 Natančneje, kot je razvidno iz besedila sedmega vprašanja in s tem povezanih pojasnil iz predloga za sprejetje predhodne odločbe, se predložitveno sodišče sprašuje, ali se lahko s Sklepom SPK zagotovi ustrezna raven varstva osebnih podatkov, prenesenih v tretje države, ker standardna določila o varstvu podatkov, ki jih ta sklep določa, organov teh tretjih držav ne zavezujejo.

124 Člen 1 Sklepa SPK določa, da standardna določila o varstvu podatkov iz Priloge k temu sklepu veljajo za takšna, ki zagotavljajo ustrezne zaščitne ukrepe glede varstva zasebnosti ter temeljnih pravic in svoboščin posameznikov, kakor zahteva člen 26(2) Direktive 95/46. Zadnjenavedena določba je bila v bistvu povzeta v členu 46(1) in (2)(c) Splošne uredbe o varstvu podatkov.

125 Čeprav so ta določila zavezujoča za upravljavca s sedežem v Uniji in prejemnika prenosa osebnih podatkov s sedežem v tretji državi, če sta se v pogodbi sklicevala na ta določila, pa ni sporno, da ta določila ne morejo zavezovati organov te tretje države, saj ti niso pogodbena stranka.

126 Čeprav tako obstajajo položaji, v katerih glede na stanje prava in prakso, ki velja v zadevni tretji državi, prejemnik takega prenosa lahko zagotovi potrebno varstvo podatkov zgolj na podlagi standardnih določil o varstvu podatkov, pa obstajajo tudi drugi položaji, v katerih določbe teh določil v praksi morda ne bi zagotavljale zadostnega sredstva za zagotovitev učinkovitega varstva osebnih podatkov, prenesenih v zadevno tretjo državo. Tako je zlasti takrat, kadar pravo te tretje države njenim javnim organom omogoča posege v pravice posameznikov, na katere se osebni podatki nanašajo.

127 Tako se postavlja vprašanje, ali je sklep Komisije, ki se nanaša na standardna določila o varstvu podatkov, sprejet na podlagi člena 46(2)(c) Splošne uredbe o varstvu podatkov, neveljaven, ker ne vsebuje zaščitnih ukrepov, na katere bi se bilo mogoče opreti v razmerju do javnih organov tretjih držav, v katere so ali bi bili lahko osebni podatki preneseni na podlagi teh določil.

128 Člen 46(1) Splošne uredbe o varstvu podatkov določa, da lahko upravljavec ali obdelovalec, če sklep o ustreznosti ni sprejet, osebne podatke prenese v tretjo državo le, če je predvidel ustrezne zaščitne ukrepe in če imajo posamezniki, na katere se osebni podatki nanašajo, na voljo izvršljive pravice in učinkovita pravna sredstva. Člen 46(2)(c) te uredbe določa, da se lahko ti zaščitni ukrepi zagotovijo s standardnimi določili o varstvu podatkov, ki jih sprejme Komisija. V teh določbah pa ni navedeno, da morajo biti vsi ti zaščitni ukrepi nujno določeni s sklepom Komisije, kot je Sklep SPK.

129 V zvezi s tem je treba poudariti, da se tak sklep razlikuje od sklepa o ustreznosti, sprejetega na podlagi člena 45(3) Splošne uredbe o varstvu podatkov, katerega namen je, da se po preučitvi ureditve zadevne tretje države ob upoštevanju zlasti upoštevne zakonodaje na področjih nacionalne varnosti in dostopa javnih organov do osebnih podatkov, z zavezujočim učinkom ugotovi, da tretja država, ozemlje ali eden oziroma več določenih sektorjev v tej tretji državi zagotavljajo ustrezno raven varstva podatkov, zaradi česar dostop javnih organov navedene tretje države do takih podatkov ne pomeni ovire za prenos teh podatkov v isto tretjo državo. Tak sklep o ustreznosti lahko torej Komisija sprejme le, če ugotovi, da upoštevna zakonodaja tretje države na tem področju dejansko vsebuje vse zahtevane zaščitne ukrepe, na podlagi katerih je mogoče šteti, da zagotavlja ustrezno raven varstva.

130 Glede sklepa Komisije, s katerim so bila sprejeta standardna določila o varstvu podatkov, kot je Sklep SPK, pa iz člena 46(1) in člena 46(2)(c) Splošne uredbe o varstvu podatkov ni mogoče sklepati, da bi morala Komisija pred sprejetjem takega sklepa opraviti oceno ustreznosti ravni varstva, ki jo zagotavljajo tretje države, v katere bi se osebni podatki na podlagi teh določil lahko prenesli, saj se tak sklep ne nanaša na določeno tretjo državo, ozemlje ali enega oziroma več sektorjev v tej tretji državi.

131 V zvezi s tem je treba spomniti, da člen 46(1) te uredbe določa, da mora upravljavec ali obdelovalec s sedežem v Uniji, če Komisija ne sprejme sklepa o ustreznosti, zagotoviti, med drugim, ustrezne zaščitne ukrepe. Uvodni izjavi 108 in 114 navedene uredbe potrjujeta, da če se Komisija ni izrekla o ustreznosti ravni varstva podatkov v tretji državi, bi moral upravljavec ali, odvisno od primera, njegov obdelovalec „sprejeti ukrepe, na podlagi katerih [se] pomanjkanje varstva podatkov v tretji državi [nadomesti] z ustreznimi zaščitnimi ukrepi za posameznika, na katerega se nanašajo osebni podatki“, ter da bi bilo treba „s temi zaščitnimi ukrepi […] zagotoviti skladnost z zahtevami glede varstva podatkov in pravicami posameznikov, na katere se nanašajo osebni podatki, ki ustrezajo obdelavi znotraj Unije, vključno z razpoložljivostjo izvršljivih pravic posameznikov, na katere se nanašajo osebni podatki, in učinkovitih pravnih sredstev […] v Uniji ali tretji državi“.

132 Ker – kot izhaja iz točke 125 te sodbe – iz pogodbene narave standardnih določil o varstvu podatkov izhaja, da ta določila ne morejo zavezovati javnih organov tretjih držav, hkrati pa člen 44 in člen 46(1) in (2)(c) Splošne uredbe o varstvu podatkov, razlagana v povezavi s členi 7, 8 in 47 Listine, zahtevata, da raven varstva posameznikov, ki se zagotavlja s to uredbo, ne sme biti ogrožena, se lahko izkaže, da bi bilo treba zaščitne ukrepe, vsebovane v standardnih določilih o varstvu podatkov, dopolniti. V zvezi s tem je v uvodni izjavi 109 navedene uredbe navedeno, da „možnost, ki jo ima upravljavec […] glede uporabe standardnih določil Komisije […], upravljavcem […] ne bi smela preprečiti[,] […] da dodajo druga določila ali dodatne zaščitne ukrepe“, pri čemer je pojasnjeno zlasti, da bi jih „bilo treba spodbujati, da vzpostavijo dodatne zaščitne ukrepe […], ki bi dopolnjeval[i] [standardna določila o varstvu podatkov]“.

133 Tako je treba ugotoviti, da je namen standardnih določil o varstvu podatkov, ki jih je Komisija sprejela na podlagi člena 46(2)(c) iste uredbe, zgolj zagotoviti upravljavcem ali njihovim podizvajalcem s sedežem v Uniji pogodbena jamstva, ki se enotno uporabljajo v vseh tretjih državah, in torej ne glede na raven varstva, ki se zagotavlja v vsaki od teh držav. Ker s temi standardnimi določili o varstvu podatkov zaradi njihove narave ni mogoče zagotoviti jamstev, ki bi presegala pogodbeno obveznost zagotavljanja spoštovanja ravni varstva, ki se zahteva s pravom Unije, se lahko izkaže, da bo moral upravljavec glede na položaj v neki tretji državi za zagotovitev te ravni varstva sprejeti dodatne ukrepe.

134 V zvezi s tem, kot je generalni pravobranilec navedel v točki 126 sklepnih predlogov, pogodbeni mehanizem iz člena 46(2)(c) Splošne uredbe o varstvu podatkov temelji na nalaganju odgovornosti upravljavcu ali njegovemu obdelovalcu s sedežem v Uniji in, podredno, pristojnemu nadzornemu organu. Zato mora ta upravljavec ali njegov obdelovalec zlasti v vsakem primeru posebej in po potrebi v sodelovanju s prejemnikom prenosa preveriti, ali pravo tretje namembne države zagotavlja ustrezno varstvo osebnih podatkov, ki so bili preneseni na podlagi standardnih določil o varstvu podatkov, z vidika prava Unije, tako da po potrebi zagotovi dodatne zaščitne ukrepe poleg tistih, ki so zagotovljeni s temi določili.

135 Če upravljavec ali njegov obdelovalec s sedežem v Uniji ne more sprejeti zadostnih dodatnih ukrepov za zagotovitev takega varstva, mora sam ali, podredno, pristojni nadzorni organ začasno ustaviti ali prenehati prenos osebnih podatkov v zadevno tretjo državo. Tako je zlasti, kadar so s pravom te tretje države prejemniku prenosa osebnih podatkov iz Unije naložene obveznosti, ki so v nasprotju z navedenimi določili in ki so zato take, da lahko ogrozijo pogodbeno jamstvo ustrezne ravni varstva pred dostopom javnih organov te tretje države do teh podatkov.

136 Zato zgolj dejstvo, da standardna določila o varstvu podatkov iz sklepa Komisije, sprejetega na podlagi člena 46(2)(c) Splošne uredbe o varstvu podatkov, kot so ta iz Priloge k Sklepu SPK, ne zavezujejo organov tretjih držav, v katere se lahko osebni podatki prenesejo, ne more vplivati na veljavnost tega sklepa.

137 Nasprotno pa je veljavnost tega sklepa odvisna od tega, ali v skladu z zahtevo, ki izhaja iz člena 46(1) in člena 46(2)(c) Splošne uredbe o varstvu podatkov, razlaganih v povezavi s členi 7, 8 in 47 Listine, tak sklep vsebuje učinkovite mehanizme, ki v praksi omogočajo zagotovitev ravni varstva, ki se zahteva s pravom Unije, in to, da se prenosi osebnih podatkov, ki temeljijo na takih določilih, v primeru kršitve teh določil ali v primeru, da jih ni mogoče spoštovati, začasno ustavijo ali prepovejo.

138 V zvezi z zaščitnimi ukrepi, vsebovanimi v standardnih določilih o varstvu podatkov iz Priloge k Sklepu SPK, iz klavzule 4(a) in (b), klavzule 5(a), klavzule 9 in klavzule 11(1) te priloge izhaja, da se upravljavec s sedežem v Uniji, prejemnik prenosa osebnih podatkov in njegov morebitni obdelovalec vzajemno zavežejo, da se je obdelava takih podatkov, vključno z njihovim prenosom, izvajala in se bo še naprej izvajala v skladu z „veljavnim pravom o varstvu podatkov“, to je – v skladu z opredelitvijo iz člena 3(f) tega sklepa – „zakonodajo, ki varuje temeljne pravice in svoboščine posameznikov ter zlasti njihovo pravico do zasebnosti glede obdelave osebnih podatkov, ki jo uporablja upravljavec podatkov v državi članici, v kateri je sedež izvoznika podatkov“. Določbe Splošne uredbe o varstvu podatkov v povezavi z Listino pa so del te zakonodaje.

139 Poleg tega se prejemnik prenosa osebnih podatkov s sedežem v tretji državi na podlagi klavzule 5(a) zaveže, da bo upravljavca s sedežem v Uniji nemudoma obvestil o morebitni nezmožnosti izpolnitve obveznosti, ki jih ima na podlagi sklenjene pogodbe. Natančneje, v skladu s klavzulo 5(b) ta prejemnik potrdi, da nima razloga za domnevo, da mu zakonodaja, ki velja zanj, preprečuje izpolnjevanje obveznosti iz sklenjene pogodbe, in se zaveže, da bo v primeru spremembe nacionalne zakonodaje, ki velja zanj in bo verjetno imela znaten negativen učinek na jamstva in obveznosti iz standardnih določil o varstvu podatkov iz Priloge k Sklepu SPK, to spremembo upravljavcu podatkov sporočil takoj, ko bo zanjo izvedel. Poleg tega, čeprav klavzula 5(d)(i) prejemniku prenosa osebnih podatkov v primeru zakonodaje, ki mu to preprečuje, kot je prepoved po kazenski zakonodaji zaradi ohranjanja zaupnosti kazenske preiskave, omogoča, da upravljavca, ki ima sedež v Uniji, ne obvesti o pravno zavezujočih zahtevah organa kazenskega pregona za posredovanje osebnih podatkov, pa mora na podlagi klavzule 5(a) iz Priloge k Sklepu SPK upravljavca vseeno obvestiti, da ne more upoštevati standardnih določil o varstvu podatkov.

140 V obeh primerih, ki sta določena v klavzuli 5(a) in (b) te priloge, ta klavzula upravljavcu s sedežem v Uniji podeljuje pravico, da začasno ustavi prenos podatkov in/ali odstopi od pogodbe. Glede na zahteve, ki izhajajo iz člena 46(1) in (2)(c) Splošne uredbe o varstvu podatkov v povezavi s členoma 7 in 8 Listine, sta začasna ustavitev prenosa podatkov in/ali odstop od pogodbe za upravljavca obvezna, če prejemnik prenosa ni ali ne more več spoštovati standardnih določil o varstvu podatkov. V nasprotnem primeru bi upravljavec kršil zahteve, ki jih ima na podlagi klavzule 4(a) iz Priloge k Sklepu SPK, razlagane v povezavi z določbami Splošne uredbe o varstvu podatkov in Listine.

141 Tako je treba ugotoviti, da klavzula 4(a) in klavzula 5(a) in (b) iz te priloge upravljavcu s sedežem v Uniji in prejemniku prenosa osebnih podatkov nalagata obveznost, da se pred prenosom osebnih podatkov v to tretjo državo prepričata, da zakonodaja tretje namembne države temu prejemniku omogoča spoštovanje standardnih določil o varstvu podatkov iz Priloge k Sklepu SPK. V zvezi s tem preverjanjem je v opombi k navedeni klavzuli 5 pojasnjeno, da obvezne zahteve te zakonodaje, ki ne presegajo tega, kar je v demokratični družbi potrebno za zaščito, med drugim, nacionalne varnosti, obrambe in javne varnosti, niso v nasprotju s temi standardnimi določili o varstvu podatkov. Nasprotno je treba – kot je generalni pravobranilec poudaril v točki 131 sklepnih predlogov – spoštovanje zahtev namembne tretje države, ki presega to, kar je za te namene potrebno, šteti za

kršitev teh določil. Ti subjekti morajo pri presoji nujnosti te zahteve po potrebi upoštevati ugotovitev o ustreznosti ravni varstva v zadevni tretji državi iz sklepa o ustreznosti, ki ga je Komisija sprejela na podlagi člena 45(3) Splošne uredbe o varstvu podatkov.

142 Iz tega izhaja, da morata upravljavec s sedežem v Uniji in prejemnik prenosa osebnih podatkov v zadevni tretji državi predhodno preveriti, ali se v zadevni tretji državi spoštuje raven varstva, ki se zahteva s pravom Unije. Prejemnik tega prenosa mora po potrebi na podlagi iste klavzule 5(b) upravljavca obvestiti o svoji morebitni nezmožnosti spoštovanja teh določil, ta pa mora začasno ustaviti prenos podatkov in/ali odstopiti od pogodbe.

143 Če je prejemnik prenosa osebnih podatkov v tretjo državo upravljavca na podlagi klavzule 5(b) iz Priloge k Sklepu SPK obvestil, da mu zakonodaja zadevne tretje države ne omogoča spoštovanja standardnih določil o varstvu podatkov iz te priloge, iz klavzule 12 iz navedene priloge izhaja, da je treba podatke, ki so bili že preneseni v to tretjo državo, in njihove kopije v celoti vrniti ali uničiti. Vsekakor je s klavzulo 6 iz iste priloge kršitev teh standardnih določil sankcionirana tako, da se posamezniku, na katerega se osebni podatki nanašajo, podeljuje pravica do odškodnine za nastalo škodo.

144 Dodati je treba, da se upravljavec s sedežem v Uniji v skladu s klavzulo 4(f) iz Priloge k Sklepu SPK za primer morebitnega prenosa posebnih vrst podatkov tretji državi, ki ne zagotavlja ustrezne ravni varstva, zaveže, da bo zadevno osebo pred prenosom ali čim prej po njem o tem prenosu obvestil. Ta informacija lahko tej osebi omogoči, da zoper upravljavca uveljavlja pravico do pravnega sredstva, ki ga ima na podlagi klavzule 3(1) iz te priloge, da bi ta začasno ustavil načrtovani prenos, odstopil od pogodbe, sklenjene s prejemnikom prenosa osebnih podatkov, ali po potrebi od njega zahteval vračilo ali uničenje prenesenih podatkov.

145 Nazadnje, v skladu s klavzulo 4(g) iz navedene priloge mora upravljavec s sedežem v Uniji, kadar ga prejemnik osebnih podatkov na podlagi klavzule 5(b) te priloge obvesti o spremembi nacionalne zakonodaje, ki velja zanj ter ki bi lahko imela znaten negativen učinek na jamstva in obveznosti iz standardnih določil o varstvu podatkov, če se kljub temu odloči nadaljevati prenos ali odpraviti začasno ustavitev, to obvestilo posredovati pristojnemu nadzornemu organu. Posredovanje take prijave temu nadzornemu organu in njegova pravica, da na podlagi klavzule 8(2) iste priloge opravi pregled prejemnika prenosa osebnih podatkov, navedenemu nadzornemu organu omogočata, da preveri, ali je treba zaradi zagotovitve ustrezne ravni varstva načrtovani prenos začasno ustaviti ali prepovedati.

146 V tem okviru člen 4 Sklepa SPK v povezavi s točko 5 obrazložitve Izvedbenega sklepa 2016/2297 potrjuje, da Sklep SPK pristojnemu nadzornemu organu nikakor ne preprečuje tega, da po potrebi začasno ustavi ali prepove prenos osebnih podatkov v tretjo državo, ki temelji na standardnih določilih o varstvu podatkov iz Priloge k temu sklepu. V zvezi s tem je treba ugotoviti, da mora, kot je razvidno iz odgovora na osmo vprašanje, pristojni nadzorni organ, razen če obstaja sklep o ustreznosti, ki ga je veljavno sprejela Komisija, v skladu s členom 58(2)(f) in (j) Splošne uredbe o varstvu podatkov tak prenos začasno ustaviti ali prepovedati, če glede na vse okoliščine tega prenosa meni, da v tej tretji državi ta določila niso ali ne morejo biti spoštovana in da varstva prenesenih podatkov, kot se zahteva v pravu Unije, ni mogoče zagotoviti na noben drug način, kadar upravljavec ali njegov obdelovalec s sedežem v Uniji nista sama začasno ustavila prenosa ali z njim prenehala.

147 V zvezi z okoliščino, ki jo navaja pooblaščenec, in sicer da bi lahko v zvezi s prenosi osebnih podatkov v tako tretjo državo nadzorni organi v različnih državah članicah sprejemali razhajajoče se odločitve, je treba dodati, da iz člena 55(1) in člena 57(1)(a) Splošne uredbe o varstvu podatkov izhaja, da je naloga nadzora nad spoštovanjem te uredbe načeloma zaupana vsakemu nadzornemu organu na ozemlju države članice, iz katere ta organ je. Poleg tega člen 64(2) navedene uredbe za preprečevanje razhajajočih se odločitev določa, da se lahko nadzorni organ, ki meni, da je treba prenos podatkov

v tretjo državo na splošno prepovedati, obrne na Evropski odbor za varstvo podatkov (EOVP), ta pa lahko na podlagi člena 65(1)(c) omenjene uredbe sprejme zavezujočo odločitev, med drugim če nadzorni organ izdanega mnenja ne upošteva.

148 Iz tega sledi, da Sklep SPK določa učinkovite mehanizme, ki v praksi zagotavljajo, da se prenos osebnih podatkov v tretjo državo na podlagi standardnih določil o varstvu podatkov iz Priloge k temu sklepu začasno ustavi ali prepove, če prejemnik prenosa ne spoštuje teh določi ali jih ne more spoštovati.

149 Glede na vse navedeno je treba na sedmo in enajsto vprašanje odgovoriti, da pri preučitvi Sklepa SPK z vidika členov 7, 8 in 47 Listine ni bil ugotovljen noben element, ki bi lahko vplival na veljavnost tega sklepa.

Četrto, peto, deveto in deseto vprašanje

150 Predložitveno sodišče želi z devetim vprašanjem v bistvu izvedeti, ali in v kolikšnem obsegu je nadzorni organ države članice vezan na ugotovitve iz Sklepa o zasebnostnem ščitu, da Združene države zagotavljajo ustrezno raven varstva. Omenjeno sodišče s četrtim, petim in desetim vprašanjem v bistvu sprašuje, ali je ob upoštevanju njegovih ugotovitev v zvezi s pravom Združenih držav prenos osebnih podatkov v to tretjo državo na podlagi standardnih določil o varstvu podatkov iz Priloge k Sklepu SPK v nasprotju s pravicami, ki jih zagotavljajo členi 7, 8 in 47 Listine, in Sodišče sprašuje zlasti, ali je vzpostavitev varuha človekovih pravic, omenjenega v Prilogi III k Sklepu o zasebnostnem ščitu, združljiva s tem členom 47.

151 Najprej je treba poudariti, da se sicer tožba iz postopka v glavni stvari, ki jo je vložil pooblaščenec, nanaša zgolj na veljavnost Sklepa SPK, vendar je bila ta tožba pri predložitvenem sodišču vložena pred sprejetjem Sklepa o zasebnostnem ščitu. Ker to sodišče s četrtim in petim vprašanjem Sodišče na splošno sprašuje o varstvu, ki ga je treba v skladu s členi 7, 8 in 47 Listine zagotoviti pri takem prenosu, je treba pri presoji Sodišča upoštevati posledice sprejetja Sklepa o zasebnostnem ščitu v vmesnem času. To velja še toliko bolj, ker navedeno sodišče v desetem vprašanju izrecno sprašuje, ali se varstvo, ki se zahteva s tem členom 47, zagotavlja z varuhom človekovih pravic, omenjenim v zadnjenavedenem sklepu.

152 Poleg tega je iz navedb v predlogu za sprejetje predhodne odločbe razvidno, da je družba Facebook Ireland v postopku v glavni stvari trdila, da Sklep o zasebnostnem ščitu pooblaščenca zavezuje glede ugotovitve o ustreznosti ravni varstva, ki jo zagotavljajo Združene države, in zato glede ugotovitve o zakonitosti prenosa osebnih podatkov, ki temelji na standardnih določilih o varstvu podatkov iz Priloge k Sklepu SPK, v to tretjo državo.

153 Kot pa je razvidno iz točke 59 te sodbe, je predložitveno sodišče v sodbi z dne 3. oktobra 2017, ki je priložena k predlogu za sprejetje predhodne odločbe, poudarilo, da mora upoštevati spremembe prava, do katerih je prišlo med vložitvijo tožbe in obravnavo pred tem sodiščem. Tako kaže, da je navedeno sodišče dolžno pri odločanju v sporu o glavni stvari upoštevati spremenjene okoliščine, ki izhajajo iz sprejetja Sklepa o zasebnostnem ščitu, in morebitne zavezujoče učinke tega sklepa.

154 Natančneje, vprašanje, ali ima ugotovitev iz Sklepa o zasebnostnem ščitu, da je raven varstva v Združenih državah ustrezna, zavezujoče učinke, je upoštevno tako za presojo obveznosti, navedenih v točkah 141 in 142 te sodbe, ki jih imata upravljavec in prejemnik prenosa osebnih podatkov v tretjo državo na podlagi standardnih določil o varstvu podatkov iz Priloge k Sklepu SPK, kot tudi za presojo obveznosti, ki jih ima nadzorni organ, da po potrebi tak prenos začasno ustavi ali prepove.

155 Glede zavezujočih učinkov Sklepa o zasebnostnem ščitu člen 1(1) tega sklepa namreč določa, da za namene člena 45(1) Splošne uredbe o varstvu podatkov „ZDA zagotavljajo ustrezno raven varstva osebnih podatkov, ki se v okviru zasebnostnega ščita EU-ZDA prenašajo iz Unije organizacijam

v ZDA“. V skladu s členom 1(3) tega sklepa se šteje, da se osebni podatki prenašajo v okviru tega ščita, kadar se prenašajo iz Unije organizacijam v Združenih državah, ki so vključene na seznam organizacij, ki so pristopile k navedenemu ščitu, ki ga v skladu s členoma I in III načel iz Priloge II k istemu sklepu vodi in objavlja ministrstvo za trgovino Združenih držav.

156 Kot izhaja iz sodne prakse, navedene v točkah 117 in 118 te sodbe, je Sklep o zasebnostnem ščitu za nadzorne organe zavezujoč v delu, v katerem je v njem ugotovljeno, da Združene države zagotavljajo ustrezno raven varstva, zato učinkuje tako, da so prenosi osebnih podatkov, opravljeni v okviru zasebnostnega ščita EU-ZDA, dovoljeni. Zato pristojni nadzorni organ, dokler Sodišče tega sklepa ne razglasi za neveljavnega, ne more začasno ustaviti ali prepovedati prenosa osebnih podatkov subjektu, ki je pristopil k temu ščitu, ker v nasprotju z oceno Komisije iz omenjenega sklepa meni, da zakonodaja Združenih držav, ki ureja dostop do osebnih podatkov, prenesenih v okviru navedenega ščita, in uporabo teh podatkov s strani javnih organov te tretje države za namene nacionalne varnosti, kazenskega pregona in drugih javnih interesov, ne zagotavlja ustrezne ravni varstva.

157 To ne spremeni dejstva, da mora v skladu s sodno prakso, navedeno v točkah 119 in 120 te sodbe, pristojni nadzorni organ, kadar neka oseba pri njem vloži pritožbo, popolnoma neodvisno preučiti, ali je zadevni prenos osebnih podatkov v skladu z zahtevami iz Splošne uredbe o varstvu podatkov, in če meni, da so očitki, s katerimi ta oseba izpodbija veljavnost sklepa o ustreznosti, utemeljeni, vložiti tožbo pri nacionalnih sodiščih, da bi ta pri Sodišču vložila predlog za sprejetje predhodne odločbe za presojo veljavnosti tega sklepa.

158 Pritožbo, vloženo na podlagi člena 77(1) Splošne uredbe o varstvu podatkov, s katero posameznik, katerega osebni podatki so bili ali bi lahko bili preneseni v tretjo državo, zatrjuje, da pravo in praksa te države – ne glede na to, kar je ugotovila Komisija v sklepu, sprejetem na podlagi člena 45(3) te uredbe – ne zagotavljata ustrezne ravni varstva, je treba namreč razumeti tako, da se v bistvu nanaša na skladnost tega sklepa z varstvom zasebnega življenja ter svoboščin in temeljnih pravic posameznikov (v zvezi s členom 25(6) in členom 28(4) Direktive 95/46 glej po analogiji sodbo z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 59).

159 V obravnavanem primeru je M. Schrems pooblaščencu v bistvu predlagal, naj prepove ali začasno ustavi prenos njegovih osebnih podatkov od družbe Facebook Ireland na družbo Facebook Inc. s sedežem v Združenih državah, ker ta tretja država ne zagotavlja ustrezne ravni varstva. Pooblaščenec je po preučitvi trditev M. Schremsa vložil tožbo pri predložitvenem sodišču, to pa se, kot kaže, glede na predložene dokaze in kontradiktorno razpravo, ki je potekala pred njim, kljub temu, kar je Komisija medtem ugotovila v Sklepu o zasebnostnem ščitu, sprašuje o utemeljenosti dvomov M. Schremsa glede ustreznosti ravni varstva, ki se zagotavlja v navedeni tretji državi, zaradi česar je to sodišče Sodišču postavilo četrto, peto in deseto vprašanje za predhodno odločanje.

160 Kot je generalni pravobranilec navedel v točki 175 sklepnih predlogov, je treba torej ta vprašanja za predhodno odločanje razumeti tako, da se z njimi v bistvu izpodbija ugotovitev Komisije iz Sklepa o zasebnostnem ščitu, da Združene države zagotavljajo ustrezno raven varstva osebnih podatkov, ki se prenesejo iz Unije v to tretjo državo, in s tem veljavnost tega sklepa.

161 Glede na preudarke, navedene v točkah 121 in od 157 do 160 te sodbe, in zato, da bi se predložitvenemu sodišču zagotovil popoln odgovor, je treba torej preizkusiti, ali je Sklep o zasebnostnem ščitu skladen z zahtevami, ki izhajajo iz Splošne uredbe o varstvu podatkov v povezavi z Listino (glej po analogiji sodbo z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 67).

162 Za to, da bi Komisija lahko sprejela sklep o ustreznosti na podlagi člena 45(3) Splošne uredbe o varstvu podatkov, mora ta institucija ustrezno obrazložiti ugotovitev, da zadevna tretja država zaradi svoje nacionalne zakonodaje ali mednarodnih obveznosti dejansko zagotavlja raven varstva temeljnih pravic, ki je v bistvu enakovredna ravni, zagotovljeni v pravnem redu Unije (v zvezi s členom 25(6) Direktive 95/46 glej po analogiji sodbo z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 96).

Vsebina Sklepa o zasebnostnem ščitu

163 Komisija je v členu 1(1) Sklepa o zasebnostnem ščitu ugotovila, da Združene države zagotavljajo ustrezno raven varstva osebnih podatkov, ki se v okviru zasebnostnega ščita EU-ZDA prenašajo iz Unije organizacijam v Združenih državah, pri čemer ta ščit, kot je določeno v členu 1(2) tega sklepa, med drugim sestavljajo načela, ki jih je 7. julija 2016 izdalo ministrstvo Združenih držav za trgovino, kakor so navedena v Prilogi II k navedenemu sklepu, ter uradna zagotovila in zaveze iz dokumentov, navedenih v prilogah I in od III do VII k istemu sklepu.

164 Vendar je bilo v Sklepu o zasebnostnem ščitu v točki I.5 Priloge II k temu sklepu, naslovljeni „Načela okvira zasebnostnega ščita EU-ZDA“, natančneje pojasnjeno, da je zavezanost tem načelom lahko omejena, če je to potrebno, med drugim za izpolnjevanje „zahtev nacionalne varnosti, javnega interesa ali kazenskega pregona“. Tako je v tem sklepu, enako kot v Odločbi 2000/520, določena prevlada teh zahtev nad temi načeli, to je prevlada, na podlagi katere so samocertificirane ameriške organizacije, ki iz Unije prejemajo osebne podatke, zavezane brez omejitve odkloniti uporabo teh načel, kadar so ta v nasprotju s temi zahtevami in se torej izkažejo za neskladna z njimi (v zvezi z Odločbo 2000/520 glej po analogiji sodbo z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 86).

165 Glede na splošnost izjeme iz točke I.5 Priloge II k Sklepu o zasebnostnem ščitu ta izjema tako omogoča posege – ki temeljijo na zahtevah nacionalne varnosti, javnega interesa ali nacionalne zakonodaje – v temeljne pravice oseb, katerih osebni podatki se prenašajo ali bi se lahko prenašali iz Unije v Združene države (v zvezi z Odločbo 2000/520 glej po analogiji sodbo z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 87). Natančneje, kot je bilo ugotovljeno v Sklepu o zasebnostnem ščitu, sta lahko posledica takih posegov dostop do osebnih podatkov, prenesenih iz Unije v Združene države, in uporaba teh podatkov s strani ameriških javnih organov v okviru programov nadzora PRISM in UPSTREAM, ki temeljita na členu 702 FISA, ter na podlagi Odredbe št. 12333.

166 V zvezi s tem je Komisija v točkah od 67 do 135 obrazložitve Sklepa o zasebnostnem ščitu opravila oceno omejitev in zaščitnih ukrepov, ki so določeni v ureditvi Združenih držav, zlasti v členu 702 FISA, Odredbi št. 12333 in v PPD-28, glede dostopa do osebnih podatkov, ki so bili preneseni v okviru zasebnostnega ščita EU-ZDA, in uporabe teh podatkov s strani javnih organov za namene nacionalne varnosti, kazenskega pregona in drugih javnih interesov.

167 Komisija je na koncu te ocene v točki 136 obrazložitve tega sklepa ugotovila, da „ZDA zagotavljajo ustrezno stopnjo varstva osebnih podatkov, ki se […] prenašajo iz Unije samocertificiranim organizacijam“, v točki 140 obrazložitve tega sklepa pa je presodila, da „na podlagi razpoložljivih informacij o pravnem redu ZDA […] meni, da bodo kakršni koli posegi javnih organov ZDA v temeljne pravice oseb, katerih podatki se v okviru zasebnostnega ščita prenašajo iz Unije v ZDA za namene nacionalne varnosti, kazenskega pregona ali drugih javnih interesov, in iz tega izhajajoče omejitve, uvedene za samocertificirane organizacije v zvezi z njihovim spoštovanjem načel, omejeni na tisto, kar je nujno potrebno za doseganje zadevnega zakonitega cilja, in da obstaja učinkovito pravno varstvo pred takim posegom“.

Ugotovitev glede ustrezne ravni varstva

168 Glede na elemente, ki jih je Komisija navedla v Sklepu o zasebnostnem ščitu, in elemente, ki jih je predložitveno sodišče ugotovilo v postopku v glavni stvari, to sodišče dvomi o tem, ali pravo Združenih držav dejansko zagotavlja ustrezno raven varstva, ki se zahteva s členom 45 Splošne uredbe o varstvu podatkov v povezavi s temeljnimi pravicami, zagotovljenimi s členi 7, 8 in 47 Listine. Navedeno sodišče zlasti meni, da pravo te tretje države ne določa potrebnih omejitev in zaščitnih ukrepov v zvezi s posegi, ki jih dovoljuje njena nacionalna ureditev, prav tako pa ne zagotavlja učinkovitega sodnega varstva pred takimi posegi. V zvezi z zadnjenavedenim dodaja, da se po njegovem mnenju z vzpostavitvijo varuha človekovih pravic na področju zasebnostnega ščita te pomanjkljivosti ne morejo odpraviti, ker tega varuha ni mogoče enačiti s sodiščem v smislu člena 47 Listine.

169 Na prvem mestu je treba v zvezi s členoma 7 in 8 Listine, ki prispevata k zahtevani ravni varstva v Uniji in katerih spoštovanje mora Komisija ugotoviti, preden sprejme sklep o ustreznosti na podlagi člena 45(1) Splošne uredbe o varstvu podatkov, opozoriti, da člen 7 Listine vsakomur zagotavlja pravico do spoštovanja zasebnega in družinskega življenja, stanovanja ter komunikacij. Člen 8(1) Listine vsakomur izrecno priznava pravico do varstva osebnih podatkov, ki se nanašajo nanj.

170 Tako dostop do osebnih podatkov fizične osebe za njihovo hrambo ali uporabo vpliva na temeljno pravico te osebe do spoštovanja zasebnega življenja, zagotovljeno v členu 7 Listine, pri čemer se ta pravica nanaša na katero koli informacijo v zvezi z določeno ali določljivo fizično osebo. Poleg tega spadajo te obdelave podatkov tudi na področje uporabe člena 8 Listine, ker gre za obdelave osebnih podatkov v smislu tega člena in morajo zato nujno izpolnjevati zahteve v zvezi z varstvom podatkov iz navedenega člena (glej v tem smislu sodbi z dne 9. novembra 2010, Volker und Markus Schecke in Eifert, C-92/09 in C-93/09, EU:C:2010:662, točki 49 in 52; z dne 8. aprila 2014, Digital Rights Ireland in drugi, C-293/12 in C-594/12, EU:C:2014:238, točka 29, in mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točki 122 in 123).

171 Sodišče je že presodilo, da gre pri sporočanju osebnih podatkov tretji osebi, kot je javni organ, za poseganje v temeljne pravice iz členov 7 in 8 Listine, ne glede na nadaljnjo uporabo sporočenih informacij. Enako velja za hrambo osebnih podatkov in za dostop do teh podatkov za njihovo uporabo s strani javnih organov, ne glede na to, ali so informacije o zasebnem življenju občutljive, in ne glede na to, ali so bile zadevne osebe zaradi navedenega posega morda oškodovane (glej v tem smislu sodbi z dne 20. maja 2003, Österreichischer Rundfunk in drugi, C-465/00, C-138/01 in C-139/01, EU:C:2003:294, točki 74 in 75, in z dne 8. aprila 2014, Digital Rights Ireland in drugi, C-293/12 in C-594/12, EU:C:2014:238, točke od 33 do 36, ter mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točki 124 in 126).

172 Vendar pravice iz členov 7 in 8 Listine niso absolutne, temveč jih je treba upoštevati glede na njihovo funkcijo v družbi (glej v tem smislu sodbi z dne 9. novembra 2010, Volker und Markus Schecke in Eifert, C-92/09 in C-93/09, EU:C:2010:662, točka 48 in navedena sodna praksa, in z dne 17. oktobra 2013, Schwarz, C-291/12, EU:C:2013:670, točka 33 in navedena sodna praksa, ter mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točka 136).

173 Glede tega je treba poudariti tudi, da se morajo v skladu s členom 8(2) Listine osebni podatki obdelovati med drugim „za določene namene in na podlagi privolitve prizadete osebe ali na drugi legitimni podlagi, določeni z zakonom“.

174 Poleg tega člen 52(1), prvi stavek, Listine določa, da mora biti kakršno koli omejevanje uresničevanja pravic in svoboščin, ki jih priznava ta listina, predpisano z zakonom in spoštovati bistveno vsebino teh pravic in svoboščin. Člen 52(1), drugi stavek, Listine pa določa, da so ob upoštevanju načela

sorazmernosti omejitve teh pravic in svoboščin dovoljene samo, če so potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih oseb.

175 V zvezi z zadnjenavedenim je treba dodati, da zahteva, da mora biti kakršno koli omejevanje uresničevanja temeljnih pravic predpisano z zakonom, pomeni, da mora biti že v pravni podlagi, ki omogoča poseg v te pravice, opredeljen obseg omejitve uresničevanja zadevne pravice (mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točka 139 in navedena sodna praksa).

176 Nazadnje, da bi bila izpolnjena zahteva po sorazmernosti, v skladu s katero morajo biti odstopanja in omejitve pri varstvu osebnih podatkov strogo omejeni na tisto, kar je nujno, morajo biti z zadevno ureditvijo, s katero se ureja poseg, določena jasna in natančna pravila, ki urejajo obseg in uporabo zadevnega ukrepa ter minimalne zahteve, tako da imajo osebe, katerih podatki so bili preneseni, na voljo zadostna jamstva, ki omogočajo učinkovito varovanje njihovih osebnih podatkov pred tveganjem zlorab. Zlasti mora biti v tej ureditvi navedeno, v kakšnih okoliščinah in pod katerimi pogoji je mogoče sprejeti ukrep, ki določa obdelavo takih podatkov, s čimer se tako zagotovi, da je poseganje omejeno na to, kar je nujno. Nujnost obstoja takih jamstev je toliko pomembnejša, če se osebni podatki obdelujejo samodejno (glej v tem smislu mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točki 140 in 141 in navedena sodna praksa).

177 V zvezi s tem je v členu 45(2)(a) Splošne uredbe o varstvu podatkov pojasnjeno, da Komisija pri ocenjevanju ustreznosti ravni varstva v tretji državi med drugim upošteva „dejanske in izvršljive pravice […] posameznikov, na katere se nanašajo osebni podatki“, ki se prenašajo.

178 V tej zadevi je ugotovitev Komisije v Sklepu o zasebnostnem ščitu, da Združene države zagotavljajo raven varstva, ki je v bistvu enakovredna ravni, ki se v Uniji zagotavlja s Splošno uredbo o varstvu podatkov v povezavi s členoma 7 in 8 Listine, sporna med drugim zato, ker naj za posege, ki se izvajajo v okviru programov nadzora, ki temeljijo na členu 702 FISA in Odredbi št. 12333, ne bi veljale zahteve, s katerimi bi se glede spoštovanja načela sorazmernosti zagotavljala raven varstva, ki je v bistvu enakovredna ravni, ki se zagotavlja s členom 52(1), drugi stavek, Listine. Preizkusiti je torej treba, ali se ti programi nadzora izvajajo ob spoštovanju takih zahtev, pri čemer pred tem ni treba preveriti, ali ta tretja država spoštuje pogoje, ki so v bistvu enakovredni tistim iz člena 52(1), prvi stavek, Listine.

179 V zvezi s tem je Komisija glede programov nadzora, ki temeljijo na členu 702 FISA, v točki 109 obrazložitve Sklepa o zasebnostnem ščitu ugotovila, da v skladu z navedenim členom „FISC […] ne dovoljuje posameznih nadzornih ukrepov, temveč dovoljuje nadzorne programe (kot sta programa PRISM in UPSTREAM) na podlagi letnih potrdil, ki jih pripravita generalni državni tožilec in direktor nacionalne obveščevalne službe“. Kot je razvidno iz iste točke obrazložitve, je namen nadzora, ki ga izvaja FISC, preveriti, ali ti programi nadzora ustrezajo cilju pridobivanja tujih obveščevalnih podatkov, ne nanaša pa se na „ustreznost ciljnega osredotočanja na posameznike za pridobivanje tujih obveščevalnih podatkov“.

180 Tako kaže, da člen 702 FISA nikakor ne vsebuje omejitev v njem vsebovanega pooblastila za izvajanje programov nadzora za pridobivanje tujih obveščevalnih podatkov in tudi ne zaščitnih ukrepov za neameriške osebe, na katere se lahko ti programi nanašajo. V teh okoliščinah in kot je generalni pravobranilec v bistvu navedel v točkah 291, 292 in 297 sklepnih predlogov, ta člen ne more zagotoviti ravni varstva, ki je v bistvu enakovredna ravni varstva, zagotovljeni z Listino, kot jo razložena v sodni praksi, navedeni v točkah 175 in 176 te sodbe, v skladu s katero morajo biti v aktu, ki je pravna podlaga za poseg v temeljne pravice, zaradi spoštovanja načela sorazmernosti določene omejitve izvrševanja zadevne pravice ter jasna in natančna pravila, ki urejajo obseg in uporabo zadevnega ukrepa ter minimalne zahteve.

181 Iz ugotovitev v Sklepu o zasebnostnem ščitu izhaja, da se morajo programi nadzora, ki temeljijo na členu 702 FISA, res izvajati v skladu z zahtevami iz PPD-28. Komisija je v točkah 69 in 77 obrazložitve Sklepa o zasebnostnem ščitu sicer poudarila, da so take zahteve za ameriške obveščevalne službe zavezujoče, vendar je ameriška vlada v odgovor na vprašanje Sodišča priznala, da PPD-28 osebam, na katere se osebni podatki nanašajo, ne daje pravic, ki bi jih bilo mogoče zoper ameriške organe uveljavljati pred sodišči. Zato s PPD-28 ni mogoče zagotoviti ravni varstva, ki bi bila v bistvu enakovredna ravni varstva, ki izhaja iz Listine, kar je v nasprotju z zahtevo iz člena 45(2)(a) Splošne uredbe o varstvu podatkov, iz katerega izhaja, da je ugotovitev take ravni varstva odvisna med drugim od tega, ali imajo osebe, katerih podatki so bili preneseni v zadevno tretjo državo, na voljo dejanske in izvršljive pravice.

182 V zvezi s programi nadzora, ki temeljijo na Odredbi št. 12333, iz spisa, ki je na voljo Sodišču, izhaja, da tudi ta odredba ne dodeljuje pravic, na katere bi se bilo mogoče pred sodišči sklicevati zoper ameriške organe.

183 Dodati je treba, da PPD-28, ki jo je treba spoštovati pri izvajanju programov iz prejšnjih dveh točk, omogoča „‚množično' zbiranje […] relativno velikega obsega obveščevalnih informacij ali podatkov SIGINT v okoliščinah, v katerih obveščevalna skupnost ne more uporabiti identifikatorja, povezanega z določeno ciljno osebo […], da bi osredotočila zbiranje", kot je navedeno v dopisu urada direktorja nacionalne obveščevalne službe (Office of the Director of National Intelligence) ameriškemu ministrstvu za trgovino in upravi za mednarodno trgovino z dne 21. junija 2016, ki je v Prilogi VI k Sklepu o zasebnostnem ščitu. Ta možnost, ki v okviru programov nadzora, ki temeljijo na Odredbi št. 12333, omogoča dostopanje do podatkov v tranzitu proti Združenim državam, ne da bi bilo to dostopanje predmet kakršnega koli sodnega nadzora, pa nikakor ne vsebuje dovolj jasne in natančne omejitve obsega takega množičnega zbiranja osebnih podatkov.

184 Zato kaže, da niti člen 702 FISA niti Odredba št. 12333 v povezavi s PPD-28 ne ustrezata minimalnim zahtevam, ki so v pravu Unije povezane z načelom sorazmernosti, tako da ni mogoče šteti, da so programi nadzora, ki temeljijo na teh določbah, omejeni na tisto, kar je nujno.

185 V teh okoliščinah omejitve varstva osebnih podatkov, ki izhajajo iz notranje ureditve Združenih držav v zvezi z dostopom in uporabo takih podatkov, prenesenih iz Unije v Združene države, s strani ameriških javnih organov, in ki jih je Komisija ocenila v Sklepu o zasebnostnem ščitu, niso urejene tako, da bi izpolnjevale zahteve, ki so v bistvu enakovredne zahtevam, ki jih v pravu Unije določa člen 52(1), drugi stavek, Listine.

186 Na drugem mestu je treba v zvezi s členom 47 Listine, ki prav tako prispeva k ravni varstva, ki se zahteva v Uniji, in katere spoštovanje mora Komisija ugotoviti, preden sprejme sklep o ustreznosti na podlagi člena 45(1) Splošne uredbe o varstvu podatkov, opozoriti, da prvi odstavek tega člena 47 zahteva, da ima vsakdo, ki so mu kršene pravice in svoboščine, zagotovljene s pravom Unije, pravico do učinkovitega pravnega sredstva pred sodiščem v skladu s pogoji, določenimi v tem členu. V skladu z drugim odstavkom tega člena ima vsakdo pravico, da o njegovi zadevi odloča neodvisno in nepristransko sodišče.

187 Iz ustaljene sodne prakse izhaja, da je obstoj učinkovitega sodnega nadzora, namenjenega zagotovitvi spoštovanja določb prava Unije, neločljivo povezan z obstojem pravne države. Tako ureditev, ki ne določa nobene možnosti, da bi posameznik lahko uporabil pravna sredstva za pridobitev dostopa do osebnih podatkov, ki se nanj nanašajo, ali dosegel popravo oziroma izbris takih podatkov, posega v bistvo temeljne pravice do učinkovitega sodnega varstva, določene v členu 47 Listine (sodba z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650, točka 95 in navedena sodna praksa).

188 V zvezi s tem je v členu 45(2)(a) Splošne uredbe o varstvu podatkov pojasnjeno, da Komisija pri ocenjevanju ustreznosti ravni varstva v tretji državi med drugim upošteva „učinkovito upravno in sodno varstvo posameznikov, na katere se nanašajo osebni podatki, ki se prenašajo". V uvodni

izjavi 104 Splošne uredbe o varstvu podatkov je v zvezi s tem poudarjeno, da bi morala tretja država „zagotavljati učinkovit neodvisen nadzor varstva podatkov ter mehanizme sodelovanja z organi za varstvo podatkov držav članic“, in pojasnjeno, da bi „[morali imeti] posamezniki, na katere se nanašajo osebni podatki, […] učinkovite in izvršljive pravice ter dostop do učinkovitega upravnega in sodnega varstva“.

189 Možnost učinkovitega uveljavljanja pravnih sredstev v zadevni tretji državi je še posebej pomembna pri prenosu osebnih podatkov v to tretjo državo, ker, kot to izhaja iz uvodne izjave 116 Splošne uredbe o varstvu podatkov, so lahko posamezniki, na katere se nanašajo osebni podatki, soočeni z dejstvom, da upravni in sodni organi držav članic ne bodo imeli pristojnosti in sredstev, da bi učinkovito obravnavali njihove pritožbe v zvezi z zatrjevano nezakonito obdelavo tako prenesenih njihovih podatkov v tej tretji državi, zaradi česar se bodo morali obrniti na nacionalne organe in sodišča iste tretje države.

190 V tej zadevi je bila ugotovitev Komisije v Sklepu o zasebnostnem ščitu, da Združene države zagotavljajo raven varstva, ki je v bistvu enakovredna ravni varstva, ki se zagotavlja s členom 47 Listine, sporna med drugim zato, ker vzpostavitev varuha človekovih pravic na področju zasebnostnega ščita ne more odpraviti vrzeli, ki jih je v zvezi s sodnim varstvom oseb, katerih osebni podatki so preneseni v to tretjo državo, ugotovila sama Komisija.

191 V zvezi s tem je Komisija v točki 115 obrazložitve Sklepa o zasebnostnem ščitu navedla, da „čeprav imajo […] posamezniki, vključno s posamezniki iz [Unije], na katere se nanašajo osebni podatki, na voljo različne možnosti pravnega varstva, če so predmet nezakonitega (elektronskega) nadzora za namene nacionalne varnosti, je prav tako jasno, da vsaj nekatere pravne podlage, ki jih lahko uporabijo obveščevalni organi ZDA (npr. Odredba št. 12333), niso zajete“. Tako je v tej točki 115 obrazložitve poudarila, da v zvezi z Odredbo št. 12333 ne obstaja nobeno pravno sredstvo. V skladu s sodno prakso, navedeno v točki 187 te sodbe, pa taka vrzel v sodnem varstvu glede posegov, povezanih z obveščevalnimi programi, ki temeljijo na tej predsedniški odredbi, preprečuje ugotovitev, do katere je Komisija prišla v Sklepu o zasebnostnem ščitu, da pravo Združenih držav zagotavlja raven varstva, ki je v bistvu enakovredna ravni varstva, ki se zagotavlja s členom 47 Listine.

192 Poleg tega je bilo tako v zvezi s programi nadzora, ki temeljijo na členu 702 FISA, kot tistimi, ki temeljijo na Odredbi št. 12333, v točkah 181 in 182 te sodbe ugotovljeno, da niti PPD-28 niti Odredba št. 12333 osebam, na katere se osebni podatki nanašajo, ne dajeta pravic, ki bi jih lahko pred sodišči uveljavljale proti ameriškim organom, zato te osebe nimajo na voljo učinkovitega pravnega sredstva.

193 Kljub temu je Komisija v točkah 115 in 116 obrazložitve Sklepa o zasebnostnem ščitu ugotovila, da se zaradi mehanizma varuha človekovih pravic, ki so ga vzpostavili ameriški organi in kot je opisan v dopisu ameriškega ministra za zunanje zadeve evropski komisarki za pravosodje, potrošnike in enakost spolov z dne 7. julija 2016 iz Priloge III k temu sklepu, in zaradi narave nalog, zaupanih temu varuhu, ki je v obravnavanem primeru „višji koordinator za mednarodno diplomacijo v informacijski tehnologiji“, lahko šteje, da Združene države zagotavljajo raven varstva, ki je v bistvu enakovredna ravni, ki se zagotavlja s členom 47 Listine.

194 Pri presoji vprašanja, ali mehanizem varuha človekovih pravic, ki je omenjen v Sklepu o zasebnostnem ščitu, dejansko lahko nadomesti omejitve pravice do sodnega varstva, ki jih je ugotovila Komisija, se je treba glede na zahteve, ki izhajajo iz člena 47 Listine in sodne prakse, navedene v točki 187 te sodbe, opreti na načelo, da morajo imeti posamezniki možnost uveljavljanja pravnih sredstev pred neodvisnim in nepristranskim sodiščem, da bi si tako zagotovili dostop do osebnih podatkov, ki se nanje nanašajo, ali dosegli popravo oziroma izbris takih podatkov.

195 V dopisu, omenjenem v točki 193 te sodbe, pa je bil varuh človekovih pravic na področju zasebnostnega ščita, čeprav je bil opisan kot „neodvisen od obveščevalnih skupnosti“, predstavljen tako, da „poroča neposredno zunanjemu ministru, ki zagotovi, da varuh človekovih pravic opravlja

svoje funkcije objektivno in neodvisno od neprimernega vpliva, ki bi lahko imel učinek na odgovor“. Razen dejstva, ki ga je Komisija ugotovila v točki 116 obrazložitve tega sklepa, in sicer da varuha človekovih pravic imenuje zunanji minister in da je ta sestavni del zunanjega ministrstva Združenih držav, navedeni sklep, kot je generalni pravobranilec navedel v točki 337 sklepnih predlogov, ne vsebuje nobene informacije, da bi za odpoklic varuha človekovih pravic ali razveljavitev njegovega imenovanja veljala kakšna posebna jamstva, kar vzbuja dvom o neodvisnosti tega varuha od izvršilne veje oblasti (glej v tem smislu sodbo z dne 21. januarja 2020, Banco de Santander, C-274/14, EU:C:2020:17, točki 60 in 63 ter navedena sodna praksa).

196 Poleg tega, kot je generalni pravobranilec poudaril v točki 338 sklepnih predlogov, čeprav je v točki 120 obrazložitve Sklepa o zasebnostnem ščitu navedena zaveza ameriške vlade, da bo morala zadevna obveščevalna služba odpraviti vsako kršitev veljavnih pravil, ki jih odkrije varuh človekovih pravic na področju zasebnostnega ščita, pa ta sklep ne vsebuje nobene navedbe, da bi bil ta varuh pristojen za sprejemanje zavezujočih odločitev v zvezi s temi službami, v njem pa prav tako niso omenjeni nobeni zakonski zaščitni ukrepi, ki bi spremljali to zavezo in na katere bi se lahko oprle osebe, na katere se osebni podatki nanašajo.

197 Zato mehanizem varuha človekovih pravic iz Sklepa o zasebnostnem ščitu ne zagotavlja pravnega sredstva pred organom, ki bi osebam, katerih podatki se prenesejo v Združene države, zagotavljal jamstva, ki so v bistvu enakovredna tistim, ki se zahtevajo s členom 47 Listine.

198 Zato je Komisija s tem, da je v členu 1(1) Sklepa o zasebnostnem ščitu ugotovila, da Združene države zagotavljajo ustrezno raven varstva osebnih podatkov, ki se v okviru zasebnostnega ščita EU-ZDA prenašajo iz Unije organizacijam v tej tretji državi, kršila zahteve iz člena 45(1) Splošne uredbe o varstvu podatkov v povezavi s členi 7, 8 in 47 Listine.

199 Iz tega izhaja, da člen 1 Sklepa o zasebnostnem ščitu ni združljiv s členom 45(1) Splošne uredbe o varstvu podatkov v povezavi s členi 7, 8 in 47 Listine ter zato ni veljaven.

200 Ker je člen 1 Sklepa o zasebnostnem ščitu neločljivo povezan s členi od 2 do 6 in s prilogami k temu sklepu, njegova neveljavnost povzroči neveljavnost tega sklepa v celoti.

201 Glede na zgornje navedbe je treba ugotoviti, da Sklep o zasebnostnem ščitu ni veljaven.

202 V zvezi z vprašanjem, ali je treba učinke tega sklepa ohraniti v veljavi, da bi se izognili nastanku pravne praznine (glej v tem smislu sodbo z dne 28. aprila 2016, Borealis Polyolefine in drugi, C-191/14, C-192/14, C-295/14, C-389/14 in od C-391/14 do C-393/14, EU:C:2016:311, točka 106), je treba ob upoštevanju člena 49 Splošne uredbe o varstvu podatkov ugotoviti, da zaradi razglasitve ničnosti sklepa o ustreznosti, kakršen je Sklep o zasebnostnem ščitu, nikakor ne more nastati taka pravna praznina. V tem členu so namreč natančno določeni pogoji, pod katerimi se osebni podatki lahko prenesejo v tretje države, če sklep o ustreznosti v skladu s členom 45(3) te uredbe ni bil sprejet ali pa niso bili sprejeti ustrezni zaščitni ukrepi v skladu s členom 46 iste uredbe.

Stroški

203 Ker je ta postopek za stranke v postopku v glavni stvari ena od stopenj v postopku pred predložitvenim sodiščem, to odloči o stroških. Stroški za predložitev stališč Sodišču, ki niso stroški omenjenih strank, se ne povrnejo.

Iz teh razlogov je Sodišče (veliki senat) razsodilo:

1. **Člen 2(1) in (2) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) je treba razlagati tako, da prenos osebnih podatkov, ki ga gospodarski subjekt s sedežem v državi članici v komercialne namene opravi drugemu gospodarskemu subjektu s sedežem v tretji državi, spada na področje uporabe te uredbe, ne glede na to, da lahko organi te tretje države te podatke med tem prenosom ali po njem obdelujejo za namene javne varnosti, obrambe in državne varnosti.**

2. **Člen 46(1) in člen 46(2)(c) Uredbe 2016/679 je treba razlagati tako, da je treba z ustreznimi zaščitnimi ukrepi, izvršljivimi pravicami in učinkovitimi pravnimi sredstvi, ki se zahtevajo s tema določbama, zagotoviti, da je osebam, katerih osebni podatki se prenesejo v tretjo državo na podlagi standardnih določil o varstvu podatkov, zagotovljena raven varstva, ki je v bistvu enakovredna ravni varstva, ki se v Evropski uniji zagotavlja s to uredbo v povezavi z Listino Evropske unije o temeljnih pravicah. Da bi se to doseglo, je treba pri presoji ravni varstva, ki se zagotavlja v okviru takega prenosa, med drugim upoštevati tako pogodbena določila, dogovorjena med upravljavcem ali njegovim obdelovalcem s sedežem v Evropski uniji in prejemnikom prenosa s sedežem v tretji državi, kot – v zvezi z morebitnim dostopom javnih organov te tretje države do tako prenesenih osebnih podatkov – upoštevne elemente pravnega sistema te države, med drugim tiste, navedene v členu 45(2) navedene uredbe.**

3. **Člen 58(2)(f) in (j) Uredbe 2016/679 je treba razlagati tako, da mora pristojni nadzorni organ, razen če obstaja sklep o ustreznosti, ki ga je veljavno sprejela Evropska komisija, začasno ustaviti ali prepovedati prenos osebnih podatkov v tretjo državo, ki temelji na standardnih določilih o varstvu podatkov, ki jih je sprejela Komisija, če ta nadzorni organ glede na vse okoliščine tega prenosa meni, da ta določila v tej tretji državi niso ali ne morejo biti spoštovana ter da varstva prenesenih podatkov, ki se zahteva s pravom Unije, zlasti s členoma 45 in 46 te uredbe in z Listino o temeljnih pravicah, ni mogoče zagotoviti na noben drug način, kadar upravljavec ali njegov obdelovalec s sedežem v Uniji nista sama začasno ustavila prenosa ali z njim prenehala.**

4. **Pri preučitvi Sklepa Komisije z dne 5. februarja 2010 o standardnih pogodbenih klavzulah za prenos osebnih podatkov obdelovalcem s sedežem v tretjih državah v skladu z Direktivo Evropskega parlamenta in Sveta 95/46/ES (2010/87/EU), kakor je bil spremenjen z Izvedbenim sklepom Komisije (EU) 2016/2297 z dne 16. decembra 2016, z vidika členov 7, 8 in 47 Listine o temeljnih pravicah ni bil ugotovljen noben element, ki bi lahko vplival na veljavnost tega sklepa.**

5. **Izvedbeni sklep Komisije (EU) 2016/1250 z dne 12. julija 2016 na podlagi Direktive Evropskega parlamenta in Sveta 95/46/ES o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA ni veljaven.**

Podpisi