



## Zbirka odločb sodne prakse

SODBA SODIŠČA (veliki senat)

z dne 6. oktobra 2015\*

„Predhodno odločanje — Osebni podatki — Varstvo posameznikov pri obdelavi teh podatkov — Listina Evropske unije o temeljnih pravicah — Členi 7, 8 in 47 — Direktiva 95/46/ES — Člena 25 in 28 — Prenos osebnih podatkov v tretje države — Odločba 2000/520/ES — Prenos osebnih podatkov v Združene države — Neustrezna raven varstva — Veljavnost — Pritožba posameznika, čigar podatki so bili preneseni iz Evropske unije v Združene države — Pristojnosti nacionalnih nadzornih organov“

V zadevi C-362/14,

katere predmet je predlog za sprejetje predhodne odločbe na podlagi člena 267 PDEU, ki ga je vložilo High Court (Irska) z odločbo z dne 17. julija 2014, ki je prispela na Sodišče 25. julija 2014, v postopku

**Maximillian Schrems**

proti

**Data Protection Commissioner,**

ob udeležbi

**Digital Rights Ireland Ltd,**

SODIŠČE (veliki senat),

v sestavi V. Skouris, predsednik, K. Lenaerts, podpredsednik, A. Tizzano, predsednik senata, R. Silva de Lapuerta, predsednica senata, T. von Danwitz (poročevalec), S. Rodin, predsednika senata, in K. Jürimäe, predsednica senata, A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. Šváby, sodniki, M. Berger, sodnica, F. Biltgen in C. Lycourgos, sodnika,

generalni pravobranilec: Y. Bot,

sodna tajnica: L. Hewlett, glavna administratorica,

na podlagi pisnega postopka in obravnave z dne 24. marca 2015,

ob upoštevanju stališč, ki so jih predložili:

- za M. Schremsa N. Travers, SC, P. O’Shea, BL, G. Rudden, solicitor, in H. Hofmann, odvetnik,
- za Data Protection Commissioner P. McDermott, BL, S. More O’Ferrall in D. Young, solicitors,

\* Jezik postopka: angleščina.

- za Digital Rights Ireland Ltd F. Crehan, BL, S. McGarr in E. McGarr, solicitors,
  - za Irsko A. Joyce, B. Counihan in E. Creedon, agenti, skupaj z D. Fennellyem, BL,
  - za belgijsko vlado J.-C. Halleux in C. Pochet, agenta,
  - za češko vlado M. Smolek in J. Vlácil, agenta,
  - za italijansko vlado G. Palmieri, agentka, skupaj s P. Gentilijem, avvocato dello Stato,
  - za avstrijsko vlado G. Hesse in G. Kunnert, agenta,
  - za poljsko vlado M. Kamejsza, M. Pawlicka in B. Majczyna, agenti,
  - za slovensko vlado A. Grum in V. Klemenc, agentki,
  - za vlado Združenega kraljestva L. Christie in J. Beeko, agenta, skupaj z J. Holmesom, barrister,
  - za Evropski parlament D. Moore, A. Caiola in M. Pencheva, agenti,
  - za Evropsko komisijo B. Schima, B. Martenczuk, B. Smulders in J. Vondung, agenti,
  - za Evropskega nadzornika za varstvo podatkov C. Docksey, A. Buchta in V. Pérez Asinari, agenti,
- po predstavitvi sklepnih predlogov generalnega pravobranilca na obravnavi 23. septembra 2015
- izreka naslednjo

### Sodbo

- 1 Predlog za sprejetje predhodne odločbe se nanaša na razlago – glede na člene 7, 8 in 47 Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina) – členov 25(6) in 28 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), kakor je bila spremenjena z Uredbo (ES) št. 1882/2003 Evropskega parlamenta in Sveta z dne 29. septembra 2003 (UL, posebna izdaja v slovenščini, poglavje 1, zvezek 4, str. 447, v nadaljevanju: Direktiva 95/46), ter v bistvu na veljavnost Odločbe 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).
- 2 Ta predlog je bil vložen v okviru spora med M. Schremsom in Data Protection Commissioner (pooblaščenec za varstvo podatkov, v nadaljevanju: pooblaščenec) v zvezi s tem, da pooblaščenec ni preučil pritožbe, ki jo je vložil M. Schrems, ker družba Facebook Ireland Ltd (v nadaljevanju: Facebook Ireland) v Združene države prenaša osebne podatke svojih uporabnikov in jih shranjuje na strežnikih, ki se nahajajo v tej državi.

## Pravni okvir

### Direktiva 95/46

3 V uvodnih izjavah 2, 10, 56, 57, 60, 62 in 63 Direktive 95/46 je navedeno:

„(2) [...] sistemi za obdelavo podatkov [so] namenjeni temu, da služijo človeku; [...] morajo, ne glede na državljanstvo ali stalno prebivališče fizičnih oseb, spoštovati njihove temeljne pravice in svoboščine, predvsem pravico do zasebnosti, ter prispevati k [...] blaginji posameznikov;

[...]

(10) [...] namen nacionalne zakonodaje o obdelavi osebnih podatkov [je] varovati temeljne pravice in svoboščine, predvsem pravico do zasebnosti, ki jo priznava člen 8 Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin [podpisane v Rimu 4. novembra 1950] pa tudi splošna načela zakonodaje Skupnosti; [...] zato približevanje teh zakonodaj ne sme povzročiti zmanjšanja varstva, ki ga zagotavljajo, ampak mora imeti za cilj zagotovitev visoke ravni varstva v Skupnosti;

[...]

(56) [...] čezmejni prenosi osebnih podatkov [so] potrebni za razvoj mednarodne trgovine; [...] varstvo posameznikov, ki ga ta direktiva zagotavlja v Skupnosti, ne ovira prenosa osebnih podatkov v tretje države, ki zagotavljajo primerno raven varstva; [...] primernost ravni varstva, ki jo zagotavlja tretja država, [se mora] oceniti glede na vse okoliščine, ki spremljajo postopek prenosa ali niz postopkov prenosa;

(57) [...] po drugi strani [se mora] prepovedati prenos osebnih podatkov v tretjo državo, ki ne zagotavlja primerne ravni varstva;

[...]

(60) [...] v vsakem primeru [se] prenosi v tretje države lahko opravijo samo v popolni skladnosti s predpisi, ki so jih sprejele države članice na podlagi te direktive in predvsem člena 8;

[...]

(62) [...] v državah članicah [je] ustanovitev nadzornih organov, ki opravljajo svoje naloge popolnoma samostojno, bistvena sestavina varstva posameznikov pri obdelavi osebnih podatkov;

(63) [...] taki organi [morajo] za opravljanje svojih nalog imeti potrebna sredstva, vključno s pooblastili za preiskavo in ukrepanje, predvsem pri pritožbah posameznikov, in pooblastila za sodelovanje v sodnih postopkih; [...]"

4 Členi 1, 2, 25, 26, 28 in 31 Direktive 95/46 določajo:

### „Člen 1

#### Namen direktive

1. V skladu s to direktivo države članice varujejo temeljne pravice in svoboščine fizičnih oseb in predvsem njihovo pravico do zasebnosti pri obdelavi osebnih podatkov.

[...]

## Člen 2

### Opredelitev pojmov

V tej direktivi:

- (a) ‚osebni podatki‘ pomeni katero koli informacijo, ki se nanaša na določeno ali določljivo fizično osebo („posameznik, na katerega se nanašajo osebni podatki“); določljiva oseba je tista, ki se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali socialno identiteto;
- (b) ‚obdelava osebnih podatkov‘ (‚obdelava‘) pomeni kakršen koli postopek ali niz postopkov, ki se izvajajo v zvezi z osebnimi podatki z avtomatskimi sredstvi ali brez njih, kakršno je zbiranje, beleženje, urejanje, shranjevanje, prilagajanje ali predelava, iskanje, posvetovanje, uporaba, posredovanje s prenosom, širjenje ali drugo razpolaganje, prilagajanje ali kombiniranje, blokiranje, izbris ali uničenje;

[...]

- (d) ‚upravljavec‘ pomeni fizično ali pravno osebo, javni organ, agencijo ali kateri koli drug organ, ki sam ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov; kadar namene in sredstva obdelave določa nacionalna zakonodaja ali zakonodaja Skupnosti, lahko upravljavca ali posebna merila za njegovo imenovanje določi nacionalna zakonodaja ali zakonodaja Skupnosti;

[...]

## Člen 25

### Načela

1. Države članice predvidijo, da se lahko prenos osebnih podatkov, ki so v obdelavi ali so namenjeni obdelavi po dovoljenem prenosu, 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; predvsem je treba upoštevati značaj podatkov, namen in trajanje predlaganega postopka ali postopkov obdelave, državo izvora in ciljno državo, pravno ureditev, bodisi splošno ali sektorsko, ki je v veljavi v tretji državi, ter strokovne predpise in varnostne ukrepe, ki se uporabljajo v tej državi.
3. Države članice in Komisija se medsebojno obveščajo o primerih, za katere menijo, da tretja država ne zagotavlja ustrezne ravni varstva v smislu odstavka 2.
4. Kadar Komisija na podlagi postopka iz člena 31(2) ugotovi, da tretja država ne zagotavlja ustrezne ravni varstva v smislu odstavka 2 tega člena, države članice sprejmejo ukrepe, ki so potrebni za preprečevanje kakršnih koli prenosov podatkov iste vrste v to tretjo državo.
5. Ko je ustrezno, Komisija začne pogajanja glede ureditve položaja, ki izhaja iz ugotovitve po odstavku 4.

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 [nacionalne] 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, ki so potrebni za uskladitev z odločitvijo Komisije.

#### Člen 26

#### Odstopanja

1. Z odstopanjem od člena 25 in če nacionalno pravo za posamične primere ne določa drugače, države članice določijo, da se prenos ali niz prenosov osebnih podatkov v tretjo državo, ki ne zagotavlja ustrezne ravni varstva v smislu člena 25(2), lahko izvede pod pogojem, da:

(a) je posameznik, na katerega se osebni podatki nanašajo, nedvoumno dal svojo privolitev k predlaganemu prenosu;

ali

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

ali

(c) je prenos potreben za sklenitev ali izvedbo pogodbe med upravljavcem in tretjo stranko, ki je v korist posameznika, na katerega se osebni podatki nanašajo;

ali

(d) je prenos potreben oziroma ga zahteva zakon na temelju pomembnega javnega interesa ali pa za uveljavitev, izvajanje ali obdržanje pravice do pravnih zahtevkov;

ali

(e) je prenos potreben, da bi zaščitili življenjske interese posameznikov, na katere se osebni podatki nanašajo;

ali

(f) se prenos opravi iz registra, ki je skladno z zakoni ali predpisi namenjen zagotavljanju informacij javnosti in je na voljo za vpogled javnosti na splošno ali kateri koli osebi, ki lahko izkaže zakoniti interes, v kolikor so v posameznem primeru izpolnjeni pogoji, ki jih za vpogled določa zakon.

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.

3. Država članica obvesti Komisijo in druge države članice o dovoljenjih, ki jih odobri v skladu z odstavkom 2.

Če država članica ali Komisija ugovarja iz utemeljenih razlogov, ki zadevajo varstvo zasebnosti ter temeljnih pravic in svoboščin posameznikov, Komisija sprejme ustrezne ukrepe v skladu s postopkom iz člena 31(2).

Države članice sprejmejo potrebne ukrepe za uskladitev z odločitvijo Komisije.

[...]

#### Člen 28

Nadzorni organ

1. Vsaka država članica določi, da je eden ali več javnih organov na njenem ozemlju odgovornih za spremljanje uporabe predpisov, ki so jih sprejele države članice v skladu s to direktivo.

Ti organi pri izvajanju nalog, ki so jim zaupane, delujejo popolnoma neodvisno.

2. Vsaka država članica zagotovi, da se ob pripravi zakonodajnih in upravnih aktov, ki se nanašajo na varstvo posameznikovih pravic in svoboščin pri obdelavi osebnih podatkov, posvetuje z nadzornimi organi.

3. 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, naložitevčasne 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.

Zoper odločitve [odločbe] nadzornega organa je zagotovljeno sodno pravno sredstvo.

4. Vsak nadzorni organ obravnava zahtevke [zahteve], ki jih je vložila katera koli oseba ali združenje, ki predstavlja to osebo, v zvezi z varstvom svojih pravic in svoboščin glede obdelave osebnih podatkov. Zadevna oseba je obveščena o odločitvah o zahtevkih [odločbah o zahtevah].

Vsak nadzorni organ obravnava predvsem zahtevke [zahteve] za preverjanje zakonitosti obdelave podatkov, ki jih vložijo katera koli oseba, kadar se uporabljajo nacionalne določbe, sprejete v skladu s členom 13 te direktive. Oseba mora biti v vsakem primeru obveščena, da je bilo opravljeno preverjanje.

[...]

6. Vsak nadzorni organ je pristojen, da na ozemlju lastne države članice izvaja pooblastila, ki so mu bila podeljena v skladu z odstavkom 3, ne glede na to, kateri nacionalni zakon se uporablja za zadevno obdelavo. Od vsakega nadzornega organa je mogoče zahtevati, da izvaja svoja pooblastila na prošnji nadzornega organa druge države članice.

[...]

### Člen 31

[...]

2. Pri sklicevanju na ta člen se uporabljata člena 4 in 7 Sklepa [Sveta z dne 28. junija 1999 o določitvi postopkov za uresničevanje Komisiji podeljenih izvedbenih pooblastil (1999/468/ES) (UL, posebna izdaja v slovenščini, poglavje 1, zvezek 3, str. 124)], ob upoštevanju določb člena 8 Sklepa.

[...]“

### Odločba 2000/520

5 Komisija je Odločbo 2000/520 sprejela na podlagi člena 25(6) Direktive 95/46.

6 V točkah 2, 5 in 8 obrazložitve te odločbe je navedeno:

„(2) Komisija lahko ugotovi, da tretja država zagotavlja ustrezno raven zaščite. V tem primeru se osebni podatki lahko prenesejo iz držav članic, ne da bi bila potrebna dodatna jamstva.

[...]

(5) Ustrezna raven zaščite pri prenosu podatkov iz Skupnosti v Združene države, ki jo priznava ta odločba, bi morala biti dosežena, če organizacije ravnajo po načelih zasebnosti varnega pristana za zaščito podatkov, ki se prenašajo iz države članice v Združene države, (v nadaljnjem besedilu ‚načela‘) in po najpogosteje zastavljenih vprašanjih (‚Frequently Asked Questions‘, v nadaljnjem besedilu ‚FAQ‘), ki zagotavljajo smernice za uveljavljanje načel in jih je izdala Vlada Združenih držav 21. julija 2000. Poleg tega morajo organizacije javno razglasiti svojo politiko varovanja zasebnosti in biti v okviru pristojnosti Federal Trade Commission (FTC) po oddelku 5 Federal Trade Commission Act, ki prepoveduje nepoštena ali goljufiva dejanja ali prakse v trgovini ali prakse, ki vplivajo na trgovino, ali v okviru pristojnosti kakega drugega z zakonom določenega organa, ki bo učinkovito zagotovil skladnost z načeli, uveljavljenimi v skladu s FAQ.

[...]

(8) Zaradi preglednosti in zaščite zmožnosti pristojnih organov v državah članicah, da zagotovijo varstvo posameznika glede obdelave njegovih osebnih podatkov, je treba s to odločbo določiti izjemne okoliščine, ki lahko upravičijo prekinitve prenosa posebnih podatkov, ne glede na ugotovitve o ustrezni zaščiti.“

7 Členi od 1 do 4 Odločbe 2000/520 določajo:

### „Člen 1

1. V členu 25(2) Direktive 95/46/ES se za vse dejavnosti, ki sodijo na področje uporabe navedene direktive, šteje, da ‚načela zasebnosti varnega pristana‘ (v nadaljnjem besedilu ‚načela‘), kakor so navedena v Prilogi I k tej odločbi in uveljavljena v skladu s smernicami iz najpogosteje zastavljenih vprašanj [‚frequently asked questions‘] (v nadaljnjem besedilu ‚FAQ‘), ki jih je izdalo Ministrstvo za

trgovino ZDA 21. julija 2000 in so navedena v Prilogi II k tej odločbi, zagotavljajo ustrezno raven zaščite osebnih podatkov, ki se prenašajo iz Skupnosti v organizacije s sedežem v Združenih državah, pri čemer se upoštevajo naslednji dokumenti, ki jih je izdalo Ministrstvo za trgovino ZDA:

- (a) pregled uveljavljanja varnega pristana iz Priloge III;
- (b) memorandum o odškodnini za kršitve zasebnosti in izrecnih pooblastilih v pravu ZDA iz Priloge IV;
- (c) pismo Federal Trade Commission iz Priloge V;
- (d) pismo Ministrstva za promet iz Priloge VI.

2. Pri vsakem prenosu podatkov morajo biti izpolnjeni naslednji pogoji:

- (a) organizacija, ki prejema podatke, je nedvomno in javno razglasila zavezanost k spoštovanju načel, uveljavljenih v skladu s FAQ; in
- (b) organizacija je podvržena zakonskim pooblastilom vladnega organa v Združenih državah, naštetega v Prilogi VII k tej odločbi, ki je pooblaščen za preiskave pritožb ter za pridobitev pomoči v primeru nepoštenih ali goljufivih praks, pa tudi odškodnine za posameznike, ne glede na njihovo državo stalnega prebivališča ali državljanstvo, kadar organizacije ne spoštujejo načel, uveljavljenih v skladu s FAQ.

3. Pogoji iz odstavka 2 štejejo za izpolnjene za vsako organizacijo, ki samocertificira zavezanost k načelom, uveljavljenim v skladu s FAQ, od datuma, ko organizacija uradno obvesti Ministrstvo za trgovino ZDA (ali njegovega pooblaščenega predstavnika) o javni razglasitvi zavezanosti iz odstavka 2(a) in o identiteti vladnega organa iz odstavka 2(b).

## *Člen 2*

Ta odločba zadeva samo primernost zaščite, ki jo v Združenih državah zagotavljajo po načelih, uveljavljenih v skladu s FAQ, zaradi izpolnitve zahtev iz člena 25(1) Direktive 95/46/ES, in ne vpliva na uporabo drugih določb navedene direktive, ki zadevajo obdelavo osebnih podatkov v državah članicah, zlasti člena 4 direktive.

## *Člen 3*

1. Brez poseganja v pooblastila pristojnih organov v državah članicah, da ukrepajo zaradi zagotovitve skladnosti z nacionalnimi predpisi, sprejetimi po drugih določbah, kakor so tiste iz člena 25 Direktive 95/46/ES, lahko ti organi izvršijo svoja obstoječa pooblastila za prekinitev prenosa podatkov v organizacijo, ki je samocertificirala zavezanost k načelom, uveljavljenim v skladu s FAQ, da bi zaščitili posameznike glede obdelave njihovih osebnih podatkov v primerih, kadar:

- (a) vladni organ v Združenih državah, naveden v Prilogi VII k tej odločbi, ali neodvisni pritožbeni mehanizem v smislu točke (a) načela uveljavljanja iz Priloge I k tej odločbi ugotovita, da organizacija krši načela, uveljavljena v skladu s FAQ; ali
- (b) obstaja precejšnja verjetnost, da se načela kršijo; obstaja utemeljena podlaga za prepričanje, da zadevni mehanizem uveljavljanja ne sprejema ali ne bo sprejel ustreznih in pravočasnih ukrepov za rešitev spornega primera; nadaljnji prenos podatkov bi povzročil neposredno nevarnost za nastanek velike škode za subjekte podatkov; in so si pristojni organi v državah članicah v danih okoliščinah razumno prizadevali, da bi organizacijo obvestili in ji dali priložnost za odgovor.



Prekinitev preneha takoj, ko je zagotovljena skladnost z načeli, uveljavljenimi v skladu s FAQ, in so zadevni pristojni organi v Skupnosti o tem uradno obveščeni.

2. Kadar države članice sprejmejo ukrepe na podlagi odstavka 1, o tem nemudoma obvestijo Komisijo.

3. Države članice in Komisija se prav tako medsebojno obvestijo, kadar ukrepanje organov, ki so v Združenih državah odgovorni za zagotavljanje skladnosti z načeli, uveljavljenimi v skladu s FAQ, takšne skladnosti ne zagotovi.

4. Če informacije, zbrane po odstavkih 1, 2 in 3, dokazujejo, da kateri koli organ, ki je v Združenih državah odgovoren za zagotavljanje skladnosti z načeli, uveljavljenimi v skladu s FAQ, njegove naloge ne opravlja učinkovito, Komisija obvesti Ministrstvo za trgovino ZDA ter po potrebi in po postopku iz člena 31 Direktive 95/46/ES predloži osnutek ukrepov za razveljavitev ali odložitev te odločbe ali omejitev področja njene uporabe.

#### Člen 4

1. Ta odločba se lahko kadar koli prilagodi glede na izkušnje z njeno uporabo in/ali če zakonodaja ZDA prevzame raven zaščite, ki jo zagotavljajo načela in FAQ. Komisija v vsakem primeru oceni izvajanje sedanje odločbe na podlagi razpoložljivih informacij tri leta po uradnem obvestilu držav članic o odločbi in poroča odboru, ustanovljenemu po členu 31 Direktive 95/46/ES, o vseh ustreznih ugotovitvah, vključno z vsemi dokazi, ki bi lahko vplivali na oceno, da določbe iz člena 1 te odločbe zagotavljajo ustrezno zaščito v smislu člena 25 Direktive 95/46/ES, in s katerim koli dokazom, da se sedanja odločba uporablja diskriminatorno.

2. Komisija po potrebi predloži osnutek ukrepov po postopku iz člena 31 direktive 95/46/ES.“

8 V Prilogi I k Odločbi 2000/520 je navedeno:

„Načela zasebnosti varnega pristana ki jih je izdalo Ministrstvo za trgovino ZDA 21. julija 2000 [...] [...] Ministrstvo za trgovino v okviru svojih zakonskih pooblastil za spodbujanje, pospeševanje in razvijanje mednarodne trgovine izdaja ta dokument in najpogosteje postavljena vprašanja – FAQ (načela). Razvoj načel je potekal v posvetovanju s predstavniki industrije in širše javnosti zaradi lažjanja trgovskih in gospodarskih stikov med Združenimi državami in Evropsko unijo. Načela so namenjena izključno organizacijam ZDA, ki prejemajo osebne podatke iz Evropske unije, da izpolnijo pogoje varnega pristana in iz njega izhajajoče domneve o ‚primernosti‘. Ker so bila načela oblikovana izključno za ta posebni namen, je lahko njihovo sprejetje v druge namene neustrezno. [...] Odločitev organizacij, da izpolnijo pogoje varnega pristana, je povsem prostovoljna, organizacije pa lahko izpolnijo pogoje varnega pristana na različne načine. [...] Zavezanost k načelom je lahko omejena: (a) če je to potrebno za izpolnjevanje zahtev nacionalne varnosti, javnega interesa ali odkrivanja in pregona; (b) z zakonom, vladnim podzakonskim aktom ali sodno prakso, ki ustvarijo nezdružljivost obveznosti ali izrecnih pooblastil, pod pogojem, da lahko organizacija pri izvajanju takih pooblastil dokaže, da je njeno neizpolnjevanje načel toliko omejeno, kolikor je potrebno za izpolnitev prednostnih zakonitih interesov na podlagi takšnih pooblastil; ali (c) če direktiva ali pravo države članice dovoljuje izjeme in odstopanja, če da se te izjeme in odstopanja uporabljajo v primerljivih okoliščinah. V skladu s ciljem krepitve varstva zasebnosti si morajo organizacije prizadevati, da načela uveljavijo v celoti in pregledno, vključno z navedbo v svoji politiki varstva zasebnosti, kdaj se bodo

izjeme, dovoljene z (b) zgoraj, redno uporabljale. Iz istega razloga se od organizacij pričakuje, da se, kadar načela in/ali pravo ZDA dopuščajo izbiro, po možnosti odločijo za možnost večjega varstva. [...]"

9 V Prilogi II k Odločbi 2000/520 je navedeno:

„Najpogosteje zastavljena vprašanja (FAQ)

[...] FAQ 6 - Samocertificiranje

V: *Kako organizacija samocertificira svojo zavezanost k načelom varnega pristana?*

O: Ugodnosti varnega pristana se zagotavljajo od datuma, ko organizacija v skladu s spodnjimi smernicami pri Ministrstvu za trgovino (ali njegovem pooblaščenem predstavniku) samocertificira svojo zavezanost k načelom.

Če se želi organizacija samocertificirati glede varnega pristana, lahko Ministrstvu za trgovino (ali njegovemu pooblaščenemu predstavniku) pošlje pismo, ki ga podpiše vodstveni delavec v imenu organizacije, ki pristopa k varnemu pristanu, in mora vsebovati vsaj naslednje podatke:

1. ime organizacije, poštni naslov, elektronski naslov, telefonsko številko in število faksa;
2. opis dejavnosti organizacije v zvezi z osebni podatki, ki jih prejema iz EU; in
3. opis politike organizacije glede varstva zasebnosti, vključno s podatki: (a) kje je ta politika na voljo za javnost, (b) datum dejanske uveljavitve te politike, (c) kontaktno službo, ki se ukvarja s pritožbami, zahtevami po dostopu in drugimi vprašanji, ki izhajajo iz načel varnega pristana, (d) posebno zakonsko telo, ki je pristojno za obravnavo morebitnih zahtevkov zoper organizacije zaradi morebitnih nepoštenih in goljufivih praks in kršitev zakonov ali predpisov o zasebnosti (in ki je navedeno v prilogi k načelom), (e) ime katerega koli programa za varstvo zasebnosti, katerega član je organizacija, (f) metodo preverjanja (znotraj organizacije, tretja stran), [...] in (g) neodvisni pritožbeni mehanizem, ki je na voljo za preiskave nerešenih pritožb.

Kadar organizacija želi, da bi ugodnosti varnega pristana zajele tudi podatke o človeških virih, ki so iz Evropske unije preneseni za uporabo na področju zaposlitvenih razmerij, lahko to stori, kadar obstaja zakonsko telo, pristojno za obravnavo pritožb v zvezi s podatki o človeških virih, ki je navedeno v prilogi k načelom. [...]

Ministrstvo za trgovino (ali od njega imenovan predstavnik) bo vodilo seznam vseh organizacij, ki predložijo taka pisma, pri čemer bo zagotavljalo razpoložljivost ugodnosti varnega pristana, ter bo letno ažuriralo podatke na tem seznamu na podlagi letnih pisem in uradnih obvestil, ki jih prejme v skladu s FAQ 11. [...]

[...] FAQ 11 – Reševanje sporov in uveljavljanje

V: *Kako se izvajajo zahteve glede reševanja sporov po načelu uveljavljanja in kako se bo obravnavalo vztrajno neizpolnjevanje načel s strani organizacije?*

O: Načelo uveljavljanja navaja zahteve za uveljavljanje varnega pristana. O izpolnjevanju zahtev iz točke (b) tega načela določa FAQ o preverjanju (FAQ 7). To FAQ 11 obravnava točki (a) in (c), ki obe zahtevata neodvisne pritožbene mehanizme. Ti mehanizmi so lahko različni, morajo pa izpolnjevati zahteve načela uveljavljanja. Organizacije lahko izpolnijo te zahteve z: (1)

usklajenostjo ravnanja s programi varstva zasebnosti zasebnega sektorja, ki v svojih pravilih vsebujejo načela varnega pristana in vključujejo učinkovite mehanizme uveljavljanja, kakor so opisani v načelu uveljavljanja; (2) usklajenostjo ravnanja z zakonskimi ali z drugimi predpisi predvidenimi nadzornimi organi, ki zagotavljajo obravnavo posameznikovih pritožb in reševanje sporov; ali (3) zavezo za sodelovanje z organi za zaščito podatkov v Evropski uniji ali z njihovimi pooblaščenimi predstavniki. Ta seznam je ilustrativen in ne omejuje. Zasebni sektor lahko oblikuje tudi druge mehanizme za zagotovitev uveljavljanja, če izpolnjujejo zahteve načela uveljavljanja in FAQ. Treba je paziti, da so zahteve načela uveljavljanja dodatek k zahtevam iz odstavka 3 uvoda k načelom, ki zahtevajo, da mora biti samourejanje izvedljivo po členu 5 Federal Trade Commission Act ali podobnem zakonu.

Pritožbeni mehanizmi.

Porabnike je treba spodbujati, da se s svojimi pritožbami najprej obrnejo na ustrezno organizacijo in šele nato uporabijo neodvisne pritožbene mehanizme. [...]

[...]

Ukrepi Federal Trade Commission.

Federal Trade Commission se je zavezala, da bo prednostno pregledovala zadeve, ki ji jih prejme od organizacij s samourejevalnim sistemom varstva zasebnosti, kakršni sta BBBonline in TRUSTe, in države članice EU, v zvezi z domnevnim neizpolnjevanjem načel varnega pristana ter ugotavljala, ali je bil kršen oddelek 5 Federal Trade Commission Act, ki prepoveduje nepoštena in goljufiva dejanja in prakse v trgovini. [...] [...]"

10 V Prilogi IV k Odločbi 2000/520 je navedeno:

„Odškodnina za kršitev zasebnosti, zakonska pooblastila ter združitve in prevzemi po pravu Združenih držav Amerike

To je odgovor na zahtevo Evropske komisije po pojasnitvi ameriškega prava glede (a) odškodninskih zahtevkov zaradi kršitve zasebnosti, (b) ‚izrecnih pooblastil‘ v ameriškem pravu v zvezi z uporabo osebnih podatkov na način, ki ni združljiv z načeli varnega pristana, in (c) učinek združitve in prevzema na obveznosti, prevzete po načelih varnega pristana.

[...]

B. Izrecna zakonska pooblastila Načela varnega pristana vsebujejo izjemo, ko zakoni, predpisi in sodna praksa ustvarijo ‚kolizijo obveznosti ali izrecna pooblastila, pod pogojem, da lahko organizacija pri izvajanju takih pooblastil dokaže, da njeno neizpolnjevanje načel sega le tako daleč, kolikor je potrebno za izpolnitev prednostnih zakonitih interesov, ki jih taka pooblastila podpirajo‘. Povsem jasno je, da kadar ameriško pravo odreja nasprotno obveznost, morajo ameriške organizacije, ne glede na to, ali so udeleženske varnega pristana ali ne, ravnati v skladu z zakonom. Kar zadeva izrecna pooblastila je sicer res, da je namen načel varnega pristana premostiti razlike med ameriškim in evropskim režimom varstva zasebnosti, dolžni pa smo upoštevati posebne pravice naših izvoljenih predstavnikov zakonodajne oblasti. Omejenost izjeme od stroge zavezanosti načelom varnega pristana je način, kako najti ravnotežje, ki bo ustreglo zakonitim interesom obeh strani. Izjema je omejena na primere, ko obstaja izrecno pooblastilo. Kar zadeva vprašanje praga, mora torej ustrezni zakon, predpis ali sodna odločba dati pozitivno pooblastilo za določeno ravnanje organizacije v varnem pristanu. Drugače povedano, izjema se ne uporablja, kadar zakon molči. Poleg tega se izjema uporabi samo, kadar je izrecno pooblastilo v koliziji z zavezanostjo k načelom varnega pristana. Celotno izjema ‚segga le tako daleč, kolikor je potrebno za izpolnitev prednostnih zakonitih interesov, ki jih taka pooblastila

podpirajo'. Če ponazorimo, kadar zakon preprosto pooblasti organizacijo za posredovanje osebnih informacij vladnemu organu, se izjema ne bo uporabila. Nasprotno pa, kadar zakon posebej pooblasti organizacijo za posredovanje osebnih informacij vladnemu organu brez privolitve posameznika, bo to pomenilo ‚izrecno pooblastilo‘ za ravnanje, ki je v koliziji z načeli varnega pristana. Lahko pa sta v izjemo zajeti tudi specifični izjemi v zvezi s pozitivnima zahtevama po zagotovitvi obvestila in soglasja (ker je to enakovredno posebni odobritvi, da se podatki razkrijejo brez obvestila in soglasja). Na primer, zakon, ki zdravnike pooblašča, da zdravstvene kartoteke svojih pacientov posredujejo zdravstvenim službam brez predhodnega soglasja pacientov, dopušča izjemo glede načel obvestila in izbire. To pooblastilo pa ne dopušča, da zdravnik te iste zdravstvene kartoteke posreduje organizacijam za vzdrževanje zdravja ali komercialnim farmacevtskim raziskovalnim laboratorijem, ker bi to preseglo obseg namenov iz zakonskega pooblastila in torej tudi obseg izjeme. [N]avedeno zakonsko pooblastilo je lahko ‚samostojno‘ pooblastilo za posebno ravnanje z osebnimi podatki, vendar, kakor kažejo primeri spodaj, gre največkrat za izjemo od obsežnejšega zakona, ki prepoveduje zbiranje, uporabo ali razkritje osebnih podatkov. [...]“

*Sporočilo Komisije COM(2013) 846 final*

- 11 Komisija je 27. novembra 2013 sprejela Sporočilo Komisije Evropskemu parlamentu in Svetu, naslovljeno „Obnovitev zaupanja v pretok podatkov med EU in ZDA“ (COM(2013) 846 final, v nadaljevanju: Sporočilo COM(2013) 846 final). K temu sporočilu je bilo priloženo poročilo, prav tako z dne 27. novembra 2013, ki je vsebovalo „ugotovitve predstavnikov Evropske unije, ki so sopredsedovali priložnostni delovni skupini EU/ZDA o varstvu podatkov“ (Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection). To poročilo je bilo pripravljeno, kot je navedeno v njegovi točki 1, v sodelovanju z Združenimi državami Amerike po tem, ko je bilo razkrito, da v tej državi obstaja več programov nadzora, vključno z obširnimi zbiranjem in obdelavo osebnih podatkov. Navedeno poročilo med drugim vsebuje podrobno analizo pravnega reda Združenih držav, zlasti glede pravnih podlag, ki dopuščajo obstoj programov nadzora ter ameriškim organom omogočajo zbiranje in obdelavo osebnih podatkov.
- 12 V točki 1 Sporočila COM(2013) 846 final je Komisija pojasnila, da je „[i]zmenjava podatkov v komercialne namene [...] predmet Odločbe [2000/520], in dodala, da ta odločba zagotavlja pravno podlago za prenose osebnih podatkov iz [Unije] družbam s sedežem v ZDA, ki so se zavezale k spoštovanju načel zasebnosti varnega pristana.“ Poleg tega je v tej točki 1 Komisija opozorila na vedno večji pomen pretoka osebnih podatkov, ki je zlasti povezan z razvojem digitalnega gospodarstva, ta je namreč „spodbudil eksponentno rast količine, kakovosti, raznovrstnosti in narave dejavnosti obdelave podatkov“.
- 13 Komisija je v točki 2 tega sporočila ugotovila, da „se je povečala tudi zaskrbljenost glede varnosti osebnih podatkov državljanov [Unije] pri njihovem pretoku v ZDA v okviru te sheme“ in da se je „[z]aradi prostovoljne in deklaratorne narave sheme [...] povečala potreba po preglednosti in nadzoru nad uveljavljanjem njenih načel“.
- 14 Poleg tega je v tej točki 2 navedla, da „[a]meriški organi oblasti lahko dostopajo do osebnih podatkov državljanov [Unije], poslanih v ZDA v okviru sheme varnega pristana, in jih obdelujejo pod pogoji, ki niso združljivi s tistimi, pod katerimi so bili ti podatki zbrani v [Uniji], in z nameni, za katere so bili poslani v ZDA“ ter da je „[v]ečina ameriških spletnih podjetij, ki jih ti programi bolj neposredno zadevajo, [...] certificiranih pod shemo varnega pristana“.
- 15 V točki 3.2 Sporočila COM(2013) 846 final je Komisija opozorila, da obstajajo nekatere pomanjkljivosti v zvezi z izvajanjem Odločbe 2000/520. Navedla je, prvič, da certificirana ameriška podjetja ne spoštujejo načel iz člena 1(1) Odločbe 2000/520 (v nadaljevanju: načela zasebnosti varnega pristana) in da bi bilo treba sprejeti izboljšave te odločbe, ki bi se morale nanašati na „strukturne pomanjkljivosti, povezane s preglednostjo in uveljavljanjem sheme, vsebinska načela varnega pristana in uporabo izjem

v interesu nacionalne varnosti“. Drugič, Komisija je ugotovila, da „[s]hema varnega pristana deluje tudi kot kanal za prenos osebnih podatkov državljanov [Unije] iz [Unije] v ZDA s strani podjetij, od katerih se zahteva, da te podatke posredujejo ameriškim obveščevalnim službam v skladu z ameriški programi zbiranja obveščevalnih podatkov“.

- 16 Komisija je v tej točki 3.2 sklenila, da čeprav „[t]renutnega izvajanja sheme v luči ugotovljenih pomanjkljivosti ni mogoče nadaljevati [...] pa bi preklic sheme negativno vplival na interese podjetij v [Uniji] in ZDA, ki sodelujejo v njej“. Komisija je nazadnje v isti točki dodala, da namerava „čim prej začeti razpravo o ugotovljenih pomanjkljivostih z ameriški organi oblasti“.

#### *Sporočilo Komisije COM(2013) 847 final*

- 17 Komisija je 27. novembra 2013 sprejela tudi Sporočilo Komisije Evropskemu parlamentu in Svetu o delovanju varnega pristana z vidika državljanov EU in družb, ustanovljenih v EU (COM(2013) 847 final, v nadaljevanju: Sporočilo COM(2013) 847 final). To sporočilo je, kot je razvidno iz njegove točke 1, temeljilo zlasti na informacijah, ki jih je pridobila posebej ustanovljena delovna skupina Evropska Unija-Združene države, in je sledilo dvema ocenjevalnima poročiloma Komisije, objavljenima leta 2002 in leta 2004.
- 18 V točki 1 tega sporočila je pojasnjeno, da izvajanje Odločbe 2000/520 „temelji na zavezah in samocertificiranju družb, ki so se zavezale k načelom varnega pristana“, ter navedeno, da je „[u]poraba teh ureditev [...] prostovoljna, vendar [da] so pravila za tiste, ki se k njim zavežejo, zavezujoča“.
- 19 Poleg tega je iz točke 2.2 Sporočila COM(2013) 847 final razvidno, da je bilo 26. septembra 2013 certificiranih 3246 podjetij iz številnih gospodarskih in storitvenih sektorjev. Ta podjetja so večinoma opravljala storitve na notranjem trgu Unije, zlasti v internetnem sektorju, nekatera od njih pa so bila podjetja iz Unije s hčerinskimi družbami v Združenih državah. Nekatera od teh podjetij so obdelovala podatke o svojih uslužbencih, zaposlenih v Evropi, ti podatki pa so se v Združene države prenašali zaradi upravljanja s človeškimi viri.
- 20 V točki 2.2 je Komisija tudi poudarila, da se „[v]sakršno pomanjkanje preglednosti ali izvrševanja na strani ZDA [...] izraža v preusmeritvi odgovornosti na evropske organe za varstvo podatkov in družbe, ki shemo uporabljajo“.
- 21 Kot je razvidno zlasti iz točk od 3 do 5 in 8 Sporočila COM(2013) 847 final, v praksi znatno število certificiranih podjetij ne spoštuje načel zasebnosti varnega pristana ali jih ne spoštuje v celoti.
- 22 Poleg tega je Komisija v točki 7 tega sporočila navedla, da „so vse družbe, ki so vključene v program PRISM [program za obširno zbiranje podatkov] in ki organom v ZDA dovoljujejo dostop do podatkov, shranjenih in obdelanih v ZDA, certificirane za varni pristan“ ter da je tako ta shema „postala ena od kanalov, po katerih je ameriški obveščevalni organom omogočen dostop do zbiranja osebnih podatkov, prvotno obdelanih v [Uniji]“. V zvezi s tem je Komisija v točki 7.1 navedenega sporočila ugotovila, da „številne pravne podlage zakonodaje ZDA omogočajo obsežno zbiranje in obdelovanje osebnih podatkov, ki jih shranjujejo ali drugače obdelujejo družbe s sedežem v ZDA“ ter da „[z]aradi obsežne narave teh programov lahko ameriški organi dostopajo do podatkov, prenesenih v okviru sheme varnega pristana, in jih nadalje obdelujejo v večji meri, kot je nujno potrebno in sorazmerno za zaščito nacionalne varnosti, kot to predvidevajo izjeme v [O]dločbi [2000/520]“.
- 23 V točki 7.2 Sporočila COM(2013) 847 final, naslovljeni „Omejitve in možnosti pravnega varstva“, je Komisija poudarila, da „je varstvo, ki ga določa pravo ZDA, večinoma zagotovljeno ameriški državljanom ali tamkajšnjim zakonitim prebivalcem“ in da „[p]oleg tega ni mogoče, da bi posamezniki

iz [Unije] ali ZDA, na katere se nanašajo osebni podatki, lahko dostopali do podatkov, jih popravljali ali izbrisali ali imeli dostop do upravnega ali sodnega varstva zaradi zbiranja in nadaljnje obdelave svojih osebnih podatkov v okviru ameriških programov nadzora“.

- 24 Glede na točko 8 Sporočila COM(2013) 847 final so med certificiranimi podjetji „[s]pletna podjetja, kot so Google, Facebook, Microsoft, Apple in Yahoo“, ki imajo „več sto milijonov strank v Evropi“ in prenašajo osebne podatke v Združene države, da bi se tam obdelovali.
- 25 Komisija je v tej točki 8 sklenila, da „obsežen dostop obveščevalnih agencij do podatkov, ki jih v ZDA prenašajo družbe, certificirane v okviru varnega pristana, sproža še dodatna resna vprašanja glede kontinuitete pravic do varstva podatkov Evropejcev, kadar se njihovi podatki prenašajo v ZDA“.

### **Spor o glavni stvari in vprašanja za predhodno odločanje**

- 26 M. Schrems, avstrijski državljani, ki prebiva v Avstriji, od leta 2008 uporablja družabno omrežje Facebook (v nadaljevanju: Facebook).
- 27 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 Amerike. Osebni podatki uporabnikov Facebook, 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.
- 28 M. Schrems je 25. junija 2013 pri pooblaščenцу vložil pritožbo, s katero je v bistvu zahteval, naj pooblaščenec uporabi svoja zakonska pooblastila in naj družbi Facebook Ireland prepove prenašanje osebnih podatkov v Združene države Amerike. V pritožbi je trdil, da veljavno pravo in praksa v tej državi ne zagotavljata zadostne zaščite osebnih podatkov, ki se hranijo na ozemlju te države, pred nadzorom, ki ga tam izvajajo državni organi. M. Schrems se je glede tega skliceval na razkritja Edwarda Snowdna v zvezi z dejavnostmi obveščevalnih služb Združenih držav Amerike, zlasti National Security Agency (v nadaljevanju: NSA).
- 29 Pooblaščenec, ki je menil, da mu ni treba preiskati dejstev, ki jih je M. Schrems navedel v pritožbi, je pritožbo zavrgel kot očitno neutemeljeno. Menil je namreč, da ni dokazov, da je NSA dostopala do osebnih podatkov M. Schremsa. Pooblaščenec je dodal, da očitkov, ki jih je M. Schrems navedel v pritožbi, ni mogoče veljavno uveljavljati, saj je treba vsa vprašanja glede ustreznosti varstva osebnih podatkov v Združenih državah reševati v skladu z Odločbo 2000/520, in da je Komisija v tej odločbi ugotovila, da Združene države zagotavljajo ustrezno raven varstva.
- 30 M. Schrems je pri High Court vložil tožbo zoper odločbo iz postopka v glavni stvari. Potem ko je to sodišče preučilo dokaze, ki sta jih predložili stranki v postopku v glavni stvari, je ugotovilo, da se elektronski nadzor in prestrezanje osebnih podatkov, ki se prenašajo iz Unije v Združene države, uporabljata za doseg obveznih in nujnih ciljev v javnem interesu. Vendar je navedeno sodišče dodalo, da so razkritja E. Snowdna pokazala, da so NSA in drugi zvezni organi „znatno presegle pooblastila“.
- 31 V skladu z navedbami tega sodišča pa naj državljani Unije ne bi imeli nobene dejanske pravice do izjave. Nadzor dejavnosti obveščevalnih služb naj bi se opravljal po tajnem in nekontradiktornem postopku. Po tem, ko so bili osebni podatki preneseni v Združene države, naj bi NSA in drugi zvezni organi, kakršen je Federal Bureau of Investigation (FBI), lahko dostopali do teh podatkov v okviru neselektivnega nadzora in prestrezanja, ki ju obširno izvajajo.

- 32 High Court je navedlo, da irsko pravo prepoveduje prenos osebnih podatkov z nacionalnega ozemlja, razen kadar zadevna tretja država zagotavlja ustrezno raven varstva zasebnega življenja ter temeljnih pravic in svoboščin. Pomen pravic do spoštovanja zasebnega življenja in nedotakljivosti stanovanja, zagotovljenih v irski ustavi, naj bi zahteval, da je vsak poseg v ti pravici sorazmeren in skladen z zakonsko določenimi zahtevami.
- 33 Množično in neselektivno dostopanje do osebnih podatkov pa naj bi bilo očitno neskladno z načelom sorazmernosti in temeljnimi vrednotami, ki jih varuje irska ustava. Da bi se prestrezanja elektronskih komunikacij lahko štela za skladna s to ustavo, bi bilo treba dokazati, da so ta prestrezanja ciljna, da je nadzor nad določenimi osebami ali določenimi skupinami objektivno utemeljen v interesu nacionalne varnosti ali zatiranja kriminalitete in da obstajajo ustrezna in preverljiva jamstva. Tako bi bilo treba po mnenju High Court, če bi bilo zadevo v glavni stvari treba rešiti zgolj na podlagi irskega prava, zato ugotoviti, da bi glede na obstoj resnih dvomov, da Združene države Amerike zagotavljajo ustrezno raven varstva osebnih podatkov, pooblaščenec moral preiskati dejstva, ki jih je M. Schrems navedel v pritožbi, in da je storil napako s tem, da je to pritožbo zavrgel.
- 34 Vendar High Court meni, da se obravnavana zadeva nanaša na izvajanje prava Unije v smislu člena 51 Listine, zato bi bilo treba odločbo iz postopka v glavni stvari presojati glede na pravo Unije. Po mnenju tega sodišča Odločba 2000/520 ne izpolnjuje zahtev, ki izhajajo iz členov 7 in 8 Listine ter iz načel, ki jih je Sodišče navedlo v sodbi Digital Rights Ireland in drugi (C-293/12 in C-594/12, EU:C:2014:238). Pravici do spoštovanja zasebnega življenja, zagotovljeni v členu 7 Listine in s temeljnimi vrednotami, skupnimi tradicijam držav članic, naj bi bilo odvzeto bistvo, če bi lahko javni organi naključno in vesplošno dostopali do elektronskih komunikacij brez kakršne koli objektivne utemeljitve iz razlogov državne varnosti ali preprečevanja kriminalitete, ki se nanašajo specifično na zadevne posameznike, in ne da bi bila v zvezi s temi dejavnostmi določena ustrezna in preverljiva jamstva.
- 35 High Court poleg tega ugotavlja, da M. Schrems v tožbi v bistvu izpodbija zakonitost sistema „varnega pristana“, ki je bil uveden z Odločbo 2000/520 in iz katere izhaja odločba iz postopka v glavni stvari. Čeprav torej M. Schrems ni formalno izpodbijal veljavnosti niti Direktive 95/46 niti Odločbe 2000/520, se po mnenju tega sodišča zastavlja vprašanje, ali je bil pooblaščenec na podlagi člena 25(6) te direktive vezan na ugotovitev Komisije iz te odločbe, da Združene države Amerike zagotavljajo ustrezno raven varstva, ali pa je člen 8 Listine pooblaščenca omogočal, da, če je to potrebno, te ugotovitve ne upošteva.
- 36 V teh okoliščinah je High Court prekinilo odločanje in Sodišču v predhodno odločanje predložilo ti vprašanji:
- „1. Ali je neodvisni nosilec funkcije, ki ima po zakonu nalogo, da izvaja zakonodajo o varstvu podatkov in jo uveljavlja, pri odločanju o pritožbi, da se osebni podatki prenašajo v tretjo državo (v tem primeru Združene države Amerike), za katero pritožnik trdi, da njena zakonodaja in praksa ne vsebujeta ustreznega varstva za posameznike, na katere se nanašajo podatki, absolutno zavezan upoštevati nasprotno ugotovitev Skupnosti iz Odločbe [2000/520] ob upoštevanju členov 7, 8 in 47 [Listine], ne glede na določbe člena 25(6) Direktive [95/46]?
  2. Ali pa lahko nosilec funkcije opravi in/ali mora opraviti lastno preiskavo zadeve glede na dejanski razvoj dogodkov v času od prvotne objave Odločbe Komisije?“

### Vprašanji za predhodno odločanje

- 37 Z vprašanjema za predhodno odločanje, ki ju je treba preučiti skupaj, predložitveno sodišče v bistvu sprašuje, ali in v kolikšnem obsegu je treba člen 25(6) Direktive 95/46 ob upoštevanju členov 7, 8 in 47 Listine razlagati tako, da odločba, sprejeta na podlagi te določbe, kot je Odločba 2000/520, v kateri Komisija ugotavlja, da tretja država zagotavlja ustrezno raven varstva, preprečuje, da bi

nadzorni organ države članice v smislu člena 28 te direktive lahko preučil zahtevo posameznika v zvezi z varstvom njegovih pravic in svoboščin glede obdelave osebnih podatkov, ki se nanašajo nanj in ki so bili iz države članice preneseni v to tretjo državo, kadar ta posameznik zatrjuje, da veljavno pravo in praksa v tej državi ne zagotavljata ustrezne ravni varstva.

*Pooblastila nacionalnih nadzornih organov v smislu člena 28 Direktive 95/46, kadar Komisija sprejme odločbo na podlagi člena 25(6) te direktive*

- 38 Uvodoma je treba navesti, da je treba določbe Direktive 95/46, ki urejajo obdelavo osebnih podatkov, ki lahko ogroža temeljne svoboščine ter zlasti pravico do spoštovanja zasebnega življenja, nujno razlagati ob upoštevanju temeljnih pravic, ki jih zagotavlja Listina (glej sodbe *Österreichischer Rundfunk* in drugi, C-465/00, C-138/01 in C-139/01, EU:C:2003:294, točka 68; *Google Spain* in *Google*, C-131/12, EU:C:2014:317, točka 68, in *Ryneš*, C-212/13, EU:C:2014:2428, točka 29).
- 39 Iz člena 1 ter uvodnih izjav 2 in 10 Direktive 95/46 je razvidno, da je njen namen zagotoviti ne le učinkovito in celostno varstvo temeljnih pravic posameznikov, zlasti temeljne pravice do spoštovanja zasebnega življenja v zvezi z obdelavo osebnih podatkov, ampak tudi visoko raven varstva teh temeljnih svoboščin in pravic. Poleg tega je pomen tako temeljne pravice do spoštovanja zasebnega življenja, zagotovljene v členu 7 Listine, kot tudi temeljne pravice do varstva osebnih podatkov, določene v členu 8 te listine, poudarjen v sodni praksi Sodišča (glej sodbe *Rijkeboer*, C-553/07, EU:C:2009:293, točka 47, *Digital Rights Ireland* in drugi, C-293/12 in C-594/12, EU:C:2014:238, točka 53, in *Google Spain* in *Google*, C-131/12, EU:C:2014:317, točke 53, 66, 74 in navedena sodna praksa).
- 40 Glede pooblastil, ki jih imajo nacionalni nadzorni organi v zvezi s prenosom osebnih podatkov v tretje države, je treba navesti, da člen 28(1) Direktive 95/46 državam članicam nalaga, naj ustanovijo enega ali več javnih organov, ki delujejo popolnoma neodvisno in ki so pristojni za nadzor nad spoštovanjem pravic Unije o varstvu posameznikov pri obdelavi osebnih podatkov. Ta zahteva izhaja tudi iz primarnega prava Unije, zlasti iz člena 8(3) Listine in člena 16(2) PDEU (glej v tem smislu sodbi *Komisija/Avstrija*, C-614/10, EU:C:2012:631, točka 36, in *Komisija/Madžarska* C-288/12, EU:C:2014:237, točka 47).
- 41 Cilj jamstva neodvisnosti nacionalnih nadzornih organov je zagotoviti učinkovit in zanesljiv nadzor nad spoštovanjem določb na področju varstva posameznikov pri obdelavi osebnih podatkov, zato ga je treba tudi razlagati glede na ta cilj. To jamstvo je bilo določeno za okrepitev varstva oseb in subjektov, na katere se nanašajo odločbe teh organov. Ustanovitev neodvisnih nadzornih organov v državah članicah je torej, kot je navedeno v uvodni izjavi 62 Direktive 95/46, bistveni element spoštovanja varstva oseb pri obdelavi osebnih podatkov (glej sodbi *Komisija/Nemčija*, C-518/07, EU:C:2010:125, točka 25 in *Komisija/Madžarska* C-288/12, EU:C:2014:237, točka 48 in navedena sodna praksa).
- 42 Za zagotovitev tega varstva morajo nacionalni nadzorni organi zlasti vzpostaviti pravo ravnotežje med spoštovanjem temeljne pravice do zasebnega življenja in interesi, ki narekujejo prosti pretok osebnih podatkov (glej v tem smislu sodbi *Komisija/Nemčija*, C-518/07, EU:C:2010:125, točka 24, in *Komisija/Madžarska*, C-288/12, EU:C:2014:237, točka 51).
- 43 V ta namen imajo ti organi širok razpon pooblastil, ta pooblastila, netaksativno naštetá v členu 28(3) Direktive 95/46, pa pomenijo potrebna sredstva za opravljanje njihovih nalog, kakor je navedeno v uvodni izjavi 63 te direktive. Tako imajo navedeni organi med drugim preiskovalna pooblastila, kakršna so pooblastila za zbiranje vseh informacij, ki so potrebne za izvajanje njihovih nadzornih nalog, učinkovita pooblastila za posredovanje, kot je začasna ali dokončna prepoved obdelave, in tudi pooblastilo za sodelovanje v sodnih postopkih.



- 44 Sicer je res, da iz člena 28(1) in (6) Direktive 95/46 izhaja, da se pooblastila nacionalnih nadzornih organov nanašajo na obdelavo osebnih podatkov, ki poteka na ozemlju države članice, ki ji pripadajo ti organi, tako da na podlagi tega člena 28 navedeni organi nimajo pooblastil v zvezi z obdelavo teh podatkov, ki poteka na ozemlju tretje države.
- 45 Vendar postopek prenosa osebnih podatkov iz države članice v tretjo državo sam po sebi pomeni obdelavo osebnih podatkov v smislu člena 2(b) Direktive 95/46 (glej v tem smislu sodbo Parlament/Svet in Komisija, C-317/04 in C-318/04, EU:C:2006:346, točka 56), ki poteka na ozemlju države članice. V tej določbi je namreč „obdelava osebnih podatkov“ opredeljena kot „kakršen koli postopek ali niz postopkov, ki se izvajajo v zvezi z osebnimi podatki z avtomatskimi sredstvi ali brez njih“ in so primeroma navedeni „posredovanje s prenosom, širjenje ali drugo razpolaganje“.
- 46 V uvodni izjavi 60 Direktive 95/46 je navedeno, da se prenosi osebnih podatkov v tretje države lahko opravijo samo ob popolnem upoštevanju predpisov, ki so jih države članice sprejele na podlagi te direktive. V zvezi s tem je bila s poglavjem IV navedene direktive, v katerega spadata člena 25 in 26, uvedena ureditev, katere namen je zagotoviti, da države članice nadzirajo prenose osebnih podatkov v tretje države. Ta ureditev dopolnjuje splošno ureditev, uvedeno s poglavjem II te direktive, ki določa splošna pravila o zakonitosti obdelave osebnih podatkov (glej v tem smislu sodbo Lindqvist, C-101/01, EU:C:2003:596, točka 63).
- 47 Ker so nacionalni nadzorni organi v skladu s členom 8(3) Listine in členom 28 Direktive 95/46 odgovorni za nadzor nad spoštovanjem predpisov Unije v zvezi z varstvom posameznikov glede obdelave osebnih podatkov, je vsak od teh organov pristojen za preveritev, ali prenos osebnih podatkov iz države članice, kateri pripada, v tretjo državo izpolnjuje zahteve, določene v Direktivi 95/46.
- 48 Direktiva 95/46, v uvodni izjavi 56 katere je priznано, da so čezmejni prenosi osebnih podatkov iz držav članic v tretje države potrebni za razvoj mednarodne trgovine, pa v členu 25(1) kot načelo določa, da se tak prenos lahko izvede le, če te tretje države zagotavljajo ustrezno raven varstva.
- 49 Poleg tega je v uvodni izjavi 57 navedene direktive pojasnjeno, da se morajo prenosi osebnih podatkov v tretje države, ki ne zagotavljajo ustrezne ravni varstva, prepovedati.
- 50 Da bi se lahko prenosi osebnih podatkov v tretje države nadzirali v odvisnosti od ravni varstva teh podatkov v vsaki od teh držav, je v členu 25 Direktive 95/46 državam članicam in Komisiji naloženih več obveznosti. Med drugim je iz tega člena razvidno, kot je navedel tudi generalni pravobranilec v točki 86 sklepnih predlogov, da lahko tako države članice kot tudi Komisija ugotovijo, ali tretja država zagotavlja ustrezno raven varstva ali ne.
- 51 Komisija lahko na podlagi člena 25(6) Direktive 95/46 sprejme odločbo, s katero ugotovi, da tretja država zagotavlja ustrezno raven varstva. V skladu z drugim pododstavkom te določbe so naslovnice te odločbe države članice, ki morajo sprejeti ukrepe, potrebne za uskladitev z odločbo Komisije. Na podlagi člena 288, četrty odstavek, PDEU, je ta odločba zavezujoča za vse države članice naslovnice in jo morajo vsi njihovi organi upoštevati (glej v tem smislu sodbi Albako Margarinefabrik, 249/85, EU:C:1987:245, točka 17, in Mediaset, C-69/13, EU:C:2014:71, točka 23) v delu, v katerem dovoljuje prenose osebnih podatkov iz držav članic v tretjo državo, na katero se nanaša.
- 52 Zato, dokler Sodišče odločbe Komisije ne razglasi za neveljavno, države članice in njihovi organi, med katere spadajo tudi njihovi neodvisni nadzorni organi, zagotovo ne smejo sprejeti ukrepov v nasprotju s to odločbo, kot so akti, v katerih se z zavezujočim učinkom ugotovi, da tretja država, na katero se nanaša navedena odločba Komisije, ne zagotavlja ustrezne ravni varstva. Za akte institucij Unije se namreč načeloma domneva, da so zakoniti, in imajo zato pravne učinke toliko časa, dokler niso

preklicani, razglašeni za nične v okviru ničnostne tožbe ali razglašeni za neveljavne v okviru postopka predhodnega odločanja ali ugovora nezakonitosti (sodba Komisija/Grčija, C-475/01, EU:C:2004:585, točka 18 in navedena sodna praksa).

- 53 Vendar pa odločba Komisije, sprejeta na podlagi člena 25(6) Direktive 95/46, kakršna je Odločba 2000/520, osebam, katerih osebni podatki so bili ali bi lahko bili preneseni v tretjo državo, ne more preprečiti, da pri nacionalnih nadzornih organih vložijo zahtevo v smislu člena 28(4) te direktive v zvezi z varstvom njihovih pravic in svoboščin glede obdelave teh podatkov. Poleg tega taka odločba, kot je generalni pravobranilec navedel med drugim v točkah 61, 93 in 116 sklepnih predlogov, ne more niti izničiti niti zmanjšati pooblastil, ki so nacionalnim nadzornim organom izrecno priznana s členom 8(3) Listine in členom 28 navedene direktive.
- 54 Niti v členu 8(3) Listine niti v členu 28 Direktive 95/46 s področja pristojnosti nacionalnih nadzornih organov ni izključen nadzor nad prenosi osebnih podatkov v tretje države, v zvezi s katerimi je bila na podlagi člena 25(6) sprejeta odločba Komisije.
- 55 Predvsem člen 28(4), prvi pododstavek, Direktive 95/46, ki določa, da lahko „katera koli oseba“ pri nacionalnih nadzornih organih vloži zahtevo „v zvezi z varstvom svojih pravic in svoboščin glede obdelave osebnih podatkov“ ne določa glede tega nobene izjeme v primeru, da Komisija sprejme odločbo na podlagi člena 25(6) te direktive.
- 56 Poleg tega bi bilo v nasprotju s sistemom, uvedenim z Direktivo 95/46, ter z namenom členov 25 in 28 te direktive, če bi odločba, ki jo Komisija sprejme na podlagi člena 25(6) navedene direktive, učinkovala tako, da bi nacionalnemu nadzornemu organu preprečevala, da preuči zahtevo posameznika v zvezi z varstvom njegovih pravic in svoboščin glede obdelave osebnih podatkov, ki so bili ali bi lahko bili preneseni iz države članice v tretjo državo, na katero se nanaša ta odločba.
- 57 Nasprotno, člen 28 Direktive 95/46 se po sami naravi uporablja za vsako obdelavo osebnih podatkov. Tako tudi v primeru, da Komisija sprejme odločbo na podlagi člena 25(6) te direktive, nacionalni nadzorni organi, pri katerih posameznik vloži zahtevo v zvezi z varstvom svojih pravic in svoboščin glede obdelave osebnih podatkov, ki se nanašajo nanj, morajo imeti možnost popolnoma neodvisno preučiti, ali prenos teh podatkov izpolnjuje zahteve, določene v navedeni direktivi.
- 58 V nasprotnem primeru bi bila posameznikom, katerih osebni podatki so bili ali bi lahko bili preneseni v zadevno tretjo državo, odvzeta pravica, zagotovljena v členu 8(1) in (3) Listine, da pri nacionalnih nadzornih organih vložijo zahtevo, da bi se zaščitile njihove temeljne pravice (glej po analogiji sodbo Digital Rights Ireland in drugi, C-293/12 in C-594/12, EU:C:2014:238, točka 68).
- 59 Zahtevo v smislu člena 28(4) Direktive 95/46, s katero posameznik, katerega osebni podatki so bili ali bi lahko bili preneseni v tretjo državo, zatrjuje, kot v postopku v glavni stvari, da pravo in praksa te države ne zagotavljata – ne glede na to, kar je ugotovila Komisija v odločbi, sprejeti na podlagi člena 25(6) te direktive – ustrezne ravni varstva, je treba razumeti tako, da se v bistvu nanaša na skladnost te odločbe z varstvom zasebnega življenja in temeljnih svoboščin in pravic posameznikov.
- 60 V zvezi s tem je treba opozoriti na ustaljeno sodno prakso Sodišča, v skladu s katero Unija temelji na vladavini prava in se v njej nadzoruje skladnost vseh aktov njenih institucij, zlasti s Pogodbama, splošnimi pravnimi načeli in temeljnimi pravicami (glej v tem smislu sodbe Komisija in drugi/Kadi, C-584/10<sup>P</sup>, C-593/10<sup>P</sup> in C-595/10<sup>P</sup>, EU:C:2013:518, točka 66, Inuit Tapiriit Kanatami in drugi/Parlament in Svet, C-583/11<sup>P</sup>, EU:C:2013:625, točka 91, in Telefónica/Komisija, C-274/12<sup>P</sup>, EU:C:2013:852, točka 56). Odločbe Komisije, sprejete na podlagi člena 25(6) Direktive 95/46, se torej ne morejo izogniti temu nadzoru.

- 61 Sodišče je edino pristojno za ugotovitev neveljavnosti akta Unije, kot je odločba Komisije, sprejeta na podlagi člena 25(6) Direktive 95/46, namen izključnosti te pristojnosti je namreč zagotavljanje pravne varnosti z enotno uporabo prava Unije (glej sodbi Melki in Abdeli, C-188/10 in C-189/10, EU:C:2010:363, točka 54, in CIVAD, C-533/10, EU:C:2012:347, točka 40).
- 62 Čeprav so nacionalna sodišča vsekakor pristojna za preučitev veljavnosti akta Unije, kot je odločba Komisije, sprejeta na podlagi člena 25(6) Direktive 95/46, pa nimajo pristojnosti sama ugotoviti neveljavnosti takega akta (glej v tem smislu sodbi Foto-Frost, 314/85, EU:C:1987:452, točke od 15 do 20, ter IATA in ELFAA, C-344/04, EU:C:2006:10, točka 27). *A fortiori*, pri prečitvi zahteve v smislu člena 28(4) te direktive, ki se nanaša na skladnost odločbe Komisije, sprejete na podlagi člena 25(6) navedene direktive, z varstvom zasebnega življenja ter temeljnih svoboščin in pravic posameznikov, nacionalni nadzorni organi niso upravičeni, da sami ugotovijo neveljavnost take odločbe.
- 63 Ob upoštevanju teh ugotovitev mora nacionalni nadzorni organ, kadar mu posameznik, katerega osebni podatki so bili ali bi lahko bili preneseni v tretjo državo, na katero se nanaša odločba Komisije, sprejeta na podlagi člena 25(6) Direktive 95/46, predloži zahtevo v zvezi z varstvom svojih pravic in svoboščin glede obdelave teh podatkov in v tej zahtevi, kot v postopku v glavni stvari, izpodbija skladnost te odločbe z varstvom zasebnega življenja ter temeljnih svoboščin in pravic, navedeno zahtevo preučiti z vso potrebno skrbnostjo.
- 64 Kadar navedeni organ ugotovi, da argumenti, navedeni v utemeljitev take zahteve, niso utemeljeni, in zato to zahtevo zavrne, mora imeti posameznik, ki je vložil navedeno zahtevo – kot izhaja iz člena 28(3), drugi pododstavek, Direktive 95/46 ob upoštevanju člena 47 Listine – imeti dostop do pravnih sredstev, s katerimi lahko izpodbija tako odločbo, ki posega v njegov položaj, pred nacionalnimi sodišči. Glede na sodno prakso, navedeno v točkah 61 in 62 te sodbe, morajo ta sodišča prekiniti odločanje in Sodišču predložiti predlog za sprejetje predhodne odločbe glede presoje veljavnosti, če presodijo, da je eden ali več razlogov za neveljavnost, ki jih navajajo stranke oziroma so bili odkriti po uradni dolžnosti, utemeljen (glej v tem smislu sodbo T & L Sugars in Sidul Açúcares/Komisija, C-456/13 P, EU:C:2015:284, točka 48 in navedena sodna praksa).
- 65 V nasprotnem primeru mora navedeni organ, kadar meni, da so očitki posameznika, ki mu je predložil zahtevo v zvezi z varstvom svojih pravic in svoboščin glede obdelave svojih osebnih podatkov, utemeljeni, v skladu s členom 28(3), tretji pododstavek, Direktive 95/46, zlasti ob upoštevanju člena 8(3) Listine, imeti možnost sodelovati v sodnih postopkih. V zvezi s tem mora nacionalni zakonodajalec določiti pravna sredstva, ki zadevnemu nacionalnemu nadzornemu organu omogočajo, da očitke, ki jih šteje za utemeljene, predloži nacionalnim sodiščem, da bi ta, če bi prav tako kot ta organ dvomila o veljavnosti odločbe Komisije, sprožila postopek predhodnega odločanja za preizkus veljavnosti navedene odločbe.
- 66 Glede na zgornje navedbe je treba na zastavljeni vprašanji odgovoriti, da je treba člen 25(6) Direktive 95/46 ob upoštevanju členov 7, 8 in 47 Listine razlagati tako, da odločba, sprejeta na podlagi te določbe, kot je Odločba 2000/520, v kateri Komisija ugotavlja, da tretja država zagotavlja ustrezno raven varstva, ne preprečuje, da nadzorni organ države članice v smislu člena 28 navedene direktive preuči zahtevo posameznika v zvezi z varstvom njegovih pravic in svoboščin glede obdelave osebnih podatkov, ki se nanašajo nanj in ki so bili iz države članice preneseni v to tretjo državo, kadar ta posameznik zatrjuje, da veljavno pravo in praksa v tej državi ne zagotavljata ustrezne ravni varstva.

#### *Veljavnost Odločbe 2000/520*

- 67 Kot je razvidno iz pojasnil predložitvenega sodišča v zvezi s postavljenima vprašanjema, M. Schrems v postopku v glavni stvari trdi, da pravo in praksa Združenih držav ne zagotavljata ustrezne ravni varstva v smislu člena 25 Direktive 95/46. Kot je generalni pravobranilec navedel v točkah 123 in 124

sklepnih predlogov, M. Schrems navaja dvome, ki jih v bistvu tudi predložitveno sodišče deli in ki se nanašajo na veljavnost Odločbe 2000/520. V teh okoliščinah je glede na ugotovitve iz točk od 60 do 63 te sodbe, da bi bilo mogoče navedenemu sodišču dati celosten odgovor, treba preučiti, ali ta odločba ustreza zahtevam, določenim v tej direktivi, razlagani ob upoštevanju Listine.

Zahteve, ki izhajajo iz člena 25(6) Direktive 95/46

- 68 Kot je že bilo navedeno v točkah 48 in 49 te sodbe, so s členom 25(1) Direktive 95/46 prepovedani prenosi osebnih podatkov v tretjo državo, ki ne zagotavlja ustrezne ravni varstva.
- 69 Vendar člen 25(6), prvi pododstavek, te direktive v zvezi z nadzorom takih prenosov določa, da Komisija „lahko [...] ugotovi, da tretja država zagotavlja ustrezno raven varstva v smislu odstavka 2 tega člena zaradi svoje domače [nacionalne] zakonodaje ali mednarodnih obveznosti [...] za zaščito zasebnega življenja in temeljnih svoboščin in pravic posameznikov“.
- 70 Res je, da niti člen 25(2) Direktive 95/46 niti nobena druga določba te direktive ne vsebuje opredelitve pojma ustrezne ravni varstva. V členu 25(2) navedene direktive je določeno zgolj, da se ustreznost ravni varstva, ki jo nudi tretja država, „oceni glede na vse okoliščine, ki so povezane s postopkom prenosa ali z nizom postopkov prenosa podatkov“, in so netaksativno naštetje okoliščine, ki jih je treba upoštevati pri taki oceni.
- 71 Vendar, prvič, kot je razvidno iz samega besedila člena 25(6) Direktive 95/46, ta določba zahteva, da tretja država „zagotavlja“ ustrezno raven varstva zaradi svoje nacionalne zakonodaje ali mednarodnih obveznosti. Drugič, iz te določbe je razvidno tudi, da se ustrezna raven varstva, ki ga zagotavlja tretja država, presoja glede na „zaščito zasebnega življenja in temeljnih svoboščin in pravic posameznikov“.
- 72 Tako se s členom 25(6) Direktive 95/46 izvaja izrecna obveznost varstva osebnih podatkov, ki je določena v členu 8(1) Listine in namen katere je zagotoviti, kot je generalni pravobranilec navedel v točki 139 sklepnih predlogov, ohranitev visoke ravni tega varstva v primeru prenosa osebnih podatkov v tretjo državo.
- 73 Res je, da izraz „ustrezna“ iz člena 25(6) Direktive 95/46 pomeni, da ni mogoče zahtevati, da tretja država zagotavlja povsem enako raven varstva kot je raven, zagotovljena v pravnem redu Unije. Vendar je treba, kot je generalni pravobranilec navedel v točki 141 sklepnih predlogov, izraz „ustrezna raven varstva“ razumeti tako, da se z njim zahteva, da ta tretja država zaradi svoje nacionalne zakonodaje ali mednarodnih obveznosti dejansko zagotavlja raven varstva temeljnih svoboščin in pravic, ki je v bistvenem enaka ravni, zagotovljeni v Uniji na podlagi Direktive 95/46, razlagani ob upoštevanju Listine. Če namreč ne bi bilo take zahteve, cilj, naveden v prejšnji točki te sodbe, ne bi bil upoštevan. Poleg tega bi bilo v tem primeru visoko raven varstva, zagotovljeno z Direktivo 95/46, razlagano ob upoštevanju Listine, enostavno zaobiti s prenosi osebnih podatkov iz Unije v tretje države, da bi se v teh državah obdelovali.
- 74 Iz samega besedila člena 25(6) Direktive 95/46 je razvidno, da je pravni red tretje države, na katero se nanaša odločba Komisije, tisti, ki mora zagotavljati ustrezno raven varstva. Četudi so sredstva, ki jih ta tretja država uporabi za zagotovitev take ravni varstva, lahko drugačna od sredstev, uporabljenih znotraj Unije za zagotovitev spoštovanja zahtev, določenih v tej direktivi, razlagani ob upoštevanju Listine, se morajo ta sredstva vseeno izkazati kot učinkovita za zagotovitev varstva, ki je v bistvenem enakovredno varstvu, zagotovljenemu znotraj Unije.

- 75 Glede na to mora Komisija pri preučitvi ravni varstva, ki jo zagotavlja tretja država, presoditi vsebino predpisov, ki se uporabljajo v tej državi in ki je razvidna tako iz njene nacionalne zakonodaje ali mednarodnih obveznosti kot tudi iz tega, kako se spoštovanje teh predpisov zagotavlja v praksi, pri čemer mora ta institucija v skladu s členom 25(2) Direktive 95/46 upoštevati vse okoliščine prenosa osebnih podatkov v tretjo državo.
- 76 Poleg tega in glede na to, da se raven varstva, ki jo zagotavlja tretja država, lahko spremeni, mora Komisija po sprejetju odločbe na podlagi člena 25(6) Direktive 95/46 redno preverjati, ali je ugotovitev v zvezi z ustrežno ravni varstva, ki ga zagotavlja zadevna tretja država, še zmeraj dejansko in pravno utemeljena. Vsekakor je taka preveritev potrebna, kadar je na podlagi indicev mogoče o tem dvomiti.
- 77 Poleg tega, kakor je generalni pravobranilec navedel v točkah 134 in 135 sklepnih predlogov, je pri preučitvi veljavnosti odločbe Komisije, sprejete na podlagi člena 25(6) Direktive 95/46, treba upoštevati tudi okoliščine, ki so nastale po sprejetju te odločbe.
- 78 Glede tega je treba ugotoviti, da je ob upoštevanju, prvič, pomembne vloge varstva osebnih podatkov z vidika temeljne pravice do spoštovanja zasebnega življenja ter, drugič, znatnega števila posameznikov, katerih temeljne pravice bi lahko bile kršene zaradi prenosa osebnih podatkov v tretjo državo, ki ne zagotavlja ustreznih ravni varstva, diskrecijska pravica Komisije glede ustreznosti ravni varstva, ki ga zagotavlja tretja država, zmanjšana, tako da je treba izvajati strog nadzor nad zahtevami, določenimi v členu 25 Direktive 95/46, razlagane ob upoštevanju Listine (glej po analogiji sodbo Digital Rights Ireland in drugi, C-293/12 in C-594/12, EU:C:2014:238, točki 47 in 48).

#### Člen 1 Odločbe 2000/520

- 79 Komisija je v členu 1(1) Odločbe 2000/520 ugotovila, da načela, navedena v Prilogi I k tej odločbi, ki se uveljavljajo v skladu s smernicami iz FAQ, navedenih v Prilogi II k navedeni odločbi, zagotavljajo ustrežno raven zaščite osebnih podatkov, ki se prenašajo iz Unije v organizacije s sedežem v Združenih državah. Iz te določbe je razvidno, da je tako načela kot FAQ objavilo ameriško ministrstvo za trgovino.
- 80 Zavezanost organizacije k načelom zasebnosti varnega pristana se potrdi na podlagi sistema samocertificiranja, kot je razvidno iz člena 1(2) in (3) te odločbe v povezavi s FAQ 6, navedenim v prilogi II k navedeni odločbi.
- 81 Čeprav to, da tretja država uporablja sistem samocertificiranja, samo po sebi ni v nasprotju z zahtevo iz člena 25(6) Direktive 95/46, da mora zadevna tretja država zagotoviti ustrežno raven varstva „zaradi svoje domače [nacionalne] zakonodaje ali mednarodnih obveznosti“, pa je zanesljivost takega sistema, kar zadeva to zahtevo, predvsem odvisna od uvedbe učinkovitih mehanizmov za prepoznavanje in nadzor, ki v praksi omogočajo odkrivanje in sankcioniranje morebitnih kršitev pravil, s katerimi se zagotavlja varstvo temeljnih pravic, zlasti pravice do spoštovanja zasebnega življenja in pravice do varstva osebnih podatkov.
- 82 V obravnavani zadevi so načela zasebnosti varnega pristana na podlagi Priloge I, drugi odstavek, Odločbe 2000/520 „namenjena izključno organizacijam ZDA, ki prejemajo osebne podatke iz Evropske unije, da izpolnijo pogoje varnega pristana in iz njega izhajajoče domneve o ‚primernosti‘“. Ta načela se torej uporabljajo zgolj za samocertificirane ameriške organizacije, ki prejemajo osebne podatke iz Unije, ne zahteva pa se, da tudi ameriški javni organi spoštujejo navedena načela.

- 83 Poleg tega na podlagi člena 2 Odločbe 2000/520 ta odločba „zadeva samo primernost zaščite, ki jo v Združenih državah zagotavljajo po načelih [zasebnosti varnega pristana], uveljavljenih v skladu s FAQ, zaradi izpolnitve zahtev iz člena 25(1) Direktive 95/46“, ne vsebuje pa zadostnih ugotovitev glede ukrepov, s katerimi Združene države Amerike zagotavljajo ustrezno raven varstva v smislu člena 25(6) te direktive zaradi svoje nacionalne zakonodaje ali mednarodnih obveznosti.
- 84 Dodati je treba, da je v skladu s Prilogo I, četrti odstavek, Odločbe 2000/520 uporabljivost navedenih načel lahko omejena z „zahtevami nacionalne varnosti, javnega interesa ali odkrivanja in pregona“ ter z „zakonom, vladnim podzakonskim aktom ali sodno prakso, ki ustvarijo nezdružljivost obveznosti ali izrecn[a] pooblastil[a], pod pogojem, da lahko organizacija pri izvajanju takih pooblastil dokaže, da je njeno neizpolnjevanje načel toliko omejeno, kolikor je potrebno za izpolnitev prednostnih zakonitih interesov na podlagi takšnih pooblastil“.
- 85 V zvezi s tem je v naslovu B Priloge IV k Odločbi 2000/520 glede mej uporabljivosti načel zasebnosti varnega pristana poudarjeno, da je „[p]ovsem jasno [...], da kadar ameriško pravo odreja nasprotno obveznost, morajo ameriške organizacije, ne glede na to, ali so udeleženke varnega pristana ali ne, ravnati v skladu z zakonom“.
- 86 Tako je v Odločbi 2000/520 določena prevlada „zahtev nacionalne varnosti, javnega interesa ali odkrivanja in pregona“ nad načeli zasebnosti varnega pristana, 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.
- 87 Glede na splošnost izjeme iz Priloge I, četrti odstavek, Odločbe 2000/520 ta izjema tako omogoča posege – ki temeljijo na zahtevah nacionalne varnosti, javnega interesa ali odkrivanja in pregona – v temeljne pravice oseb, katerih osebni podatki se prenašajo ali bi se lahko prenašali iz Unije v Združene države. V zvezi s tem za dokaz, ali obstaja tako poseganje v temeljno pravico do spoštovanja zasebnega življenja, ni pomembno, ali so zadevni podatki o zasebnem življenju občutljivi, niti to, ali so bile zadevne osebe zaradi tega posega oškodovane ali ne (sodba Digital Rights Ireland in drugi, C-293/12 in C-594/12, EU:C:2014:238, točka 33 in navedena sodna praksa).
- 88 Poleg tega Odločba 2000/520 ne vsebuje nobene ugotovitve glede tega, ali v Združenih državah obstajajo državni predpisi, katerih namen bi bil omejiti morebitne posege v temeljne pravice posameznikov, katerih podatki se prenašajo iz Unije v Združene države, posege, ki naj bi jih državni subjekti v tej državi lahko izvajali, kadar poskušajo doseči legitimne cilje, kot je nacionalna varnost.
- 89 K temu je treba dodati, da Odločba 2000/520 ne omenja obstoja učinkovitega sodnega varstva v primeru takih posegov. Kot je generalni pravobranilec navedel v točkah od 204 do 206 sklepnih predlogov, se mehanizmi zasebnega reševanja sporov in postopki pred zvezno komisijo za trgovino (Federal Trade Commission), katerih pristojnosti, opisane med drugim v FAQ 11 v Prilogi II k tej odločbi, so omejene na gospodarske spore, nanašajo na to, ali ameriška podjetja spoštujejo načela zasebnosti varnega pristana, ni pa jih mogoče uporabiti za spore, ki se nanašajo na zakonitost posegov v temeljne pravice, ki so posledica državnih ukrepov.
- 90 Poleg tega zgornjo analizo Odločbe 2000/520 potrjuje presoja položaja, do katerega je prišlo pri izvajanju te odločbe, ki jo je opravila Komisija sama. Zlasti v točkah 2 in 3.2 Sporočila COM(2013) 846 final ter v točkah 7.1, 7.2 in 8 Sporočila COM(2013) 847 final, katerih vsebina je predstavljena v točkah od 13 do 16 ter 22, 23 in 25 te sodbe, je ta institucija namreč ugotovila, da ameriški organi lahko dostopajo do osebnih podatkov, prenesenih v Združene države iz držav članic, in jih obdelujejo na način, ki med drugim ni v skladu z namenom njihovega prenosa, in obširneje, kot bi bilo nujno potrebno in sorazmerno za zaščito nacionalne varnosti. Komisija je tudi ugotovila, da

zadevni posamezniki nimajo dostopa do upravnega in sodnega varstva, ki bi med drugim omogočalo, da pridobijo dostop do podatkov, ki se nanje nanašajo, ali, če bi bilo to potrebno, da dosežejo njihovo popravo ali njihov izbris.

- 91 Kar zadeva raven varstva temeljnih svoboščin in pravic, zagotovljenega v Uniji, mora predpis Unije, ki pomeni poseg v temeljne pravice, zagotovljene v členih 7 in 8 Listine, v skladu z ustaljeno sodno prakso Sodišča določati jasna in natančna pravila, ki urejajo obseg in uporabo ukrepa ter določajo minimalne zahteve, tako da imajo osebe, za osebne podatke katerih gre, zadostna jamstva, ki omogočajo učinkovito varovanje njihovih podatkov. Potreba po takih jamstvih je toliko pomembnejša, če so osebni podatki predmet avtomatske obdelave in obstaja veliko tveganje nezakonitega dostopa do teh podatkov (sodba Digital Rights Ireland in drugi, C-293/12 in C-594/12, EU:C:2014:238, točki 54 ter 55 in navedena sodna praksa).
- 92 Poleg tega in predvsem, varstvo temeljne pravice do spoštovanja zasebnega življenja na ravni Unije zahteva, da se odstopanja od varstva osebnih podatkov in njegove omejitve določijo v mejah tega, kar je nujno potrebno (sodba Digital Rights Ireland in drugi, C-293/12 in C-594/12, EU:C:2014:238, točka 52 in navedena sodna praksa).
- 93 Torej ni zgolj na nujno potrebno omejena ureditev, ki splošno dovoljuje hrambo vseh osebnih podatkov vseh posameznikov, katerih podatki so bili preneseni iz Unije v Združene države, ne da bi se uporabljalo kakršno koli razlikovanje, omejitev ali izjema glede na cilj, ki se ga poskuša doseči, in ne da bi bilo predvideno objektivno merilo, ki bi omogočalo dostop javnih organov do podatkov in poznejšo uporabo teh podatkov samo v namene, ki so natančno določeni, strogo omejeni in bi lahko utemeljevali poseg, ki ga pomenita dostop in uporaba teh podatkov (glej v tem smislu, kar zadeva Direktivo 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL L 105, str. 54), sodbo Digital Rights Ireland in drugi, C-293/12 in C-594/12, EU:C:2014:238, točke od 57 do 61).
- 94 Predvsem je treba šteti, da ureditev, ki javnim organom omogoča splošen dostop do vsebine elektronskih komunikacij, pomeni poseg v bistvo temeljne pravice do spoštovanja zasebnega življenja, zagotovljene v členu 7 Listine (glej v tem smislu sodbo Digital Rights Ireland in drugi, C-293/12 in C-594/12, EU:C:2014:238, točka 39).
- 95 Poleg tega 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 ali izbris takih podatkov, posega v bistvo temeljne pravice do učinkovitega sodnega varstva, določene v členu 47 Listine. Člen 47, prvi odstavek, Listine namreč določa, 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 zvezi s tem je sam obstoj učinkovitega sodnega nadzora, namenjenega zagotovitvi spoštovanja določb prava Unije, neločljivo povezan z obstojem pravne države (glej v tem smislu sodbe Les Verts/Parlament, 294/83, EU:C:1986:166, točka 23, Johnston, 222/84, EU:C:1986:206, točki 18 in 19, Heylens in drugi, 222/86, EU:C:1987:442, točka 14, ter UGT-Rioja in drugi, od C-428/06 do C-434/06, EU:C:2008:488, točka 80).
- 96 Kakor je bilo torej ugotovljeno zlasti v točkah 71, 73 in 74 te sodbe, mora Komisija, da lahko sprejme odločbo na podlagi člena 25(6) Direktive 95/46, obrazloženo ugotoviti, da zadevna tretja država zaradi svoje nacionalne zakonodaje ali mednarodnih obveznosti dejansko zagotavlja raven varstva temeljnih pravic, ki je v bistvenem enaka ravni, zagotovljeni v pravnem redu Unije, to je ravni, ki je razvidna zlasti iz prejšnjih točk te sodbe.
- 97 Vendar je treba ugotoviti, da Komisija v Odločbi 2000/520 ni ugotovila, da Združene države Amerike dejansko „zagotavljajo“ ustrezno raven varstva zaradi svoje nacionalne zakonodaje ali mednarodnih obveznosti.

98 Zato je treba, ne da bi bilo treba preučiti vsebino načel zasebnosti varnega pristana, skleniti, da člen 1 te odločbe krši zahteve, določene v členu 25(6) Direktive 95/46, razlagane ob upoštevanju Listine, in da je zato neveljaven.

### Člen 3 Odločbe 2000/520

99 Iz ugotovitev, navedenih v točkah 53, 57 in 63 te sodbe, je razvidno, da morajo nacionalni nadzorni organi glede na člen 28 Direktive 95/46, razlagan zlasti ob upoštevanju člena 8 Listine, imeti možnost popolnoma neodvisno preučiti vsako zahtevo v zvezi z varstvom pravic in svoboščin posameznika glede osebnih podatkov, ki se nanj nanašajo. To še posebej velja, kadar ta posameznik v taki zahtevi navaja pomisleke glede skladnosti odločbe Komisije, sprejete na podlagi člena 25(6) te direktive, z varstvom zasebnega življenja ter temeljnih svoboščin in pravic posameznikov.

100 Člen 3(1), prvi pododstavek, Odločbe 2000/520 pa vsebuje specifično ureditev pooblastil, ki jih imajo nacionalni nadzorni organi v zvezi z ugotovitvijo Komisije glede ustrezne ravni varstva v smislu člena 25 Direktive 95/46.

101 Tako lahko v skladu s to določbo ti organi „[b]rez poseganja v [svoja] pooblastila [...], da ukrepajo zaradi zagotovitve skladnosti z nacionalnimi predpisi, sprejetimi po drugih določbah, kakor so tiste iz člena 25 Direktive [95/46], [...] prekini[ejo] prenos[...] podatkov v organizacijo, ki je samocertificirala zavezanost k načelom [Odločbe 2000/520]“, pod restriktivnimi pogoji, ki zagotavljajo visok prag za poseg. Čeprav ta določba ne posega v pooblastila teh organov, da sprejmejo ukrepe za zagotovitev spoštovanja nacionalnih predpisov, sprejetih za izvajanje te direktive, pa navedenim organom odvzema možnost sprejeti ukrepe za zagotovitev spoštovanja člena 25 te direktive.

102 Člen 3(1), prvi pododstavek, Odločbe 2000/520 je treba torej razumeti tako, da nacionalnim nadzornim organom odvzema pooblastila, ki jih imajo na podlagi člena 28 Direktive 95/46, kadar posameznik v zahtevi, vloženi na podlagi te določbe, navaja elemente, ki lahko izpodbijejo skladnost odločbe Komisije, v kateri je ta na podlagi člena 25(6) te direktive ugotovila, da tretja država zagotavlja ustrezno raven varstva, z varstvom zasebnega življenja ter temeljnih svoboščin in pravic posameznikov.

103 Izvedbeno pooblastilo, ki ga je zakonodajalec Unije Komisiji podelil v členu 25(6) Direktive 95/46, pa tej instituciji ne daje pristojnosti za zožitev pooblastil nacionalnih nadzornih organov iz prejšnje točke te sodbe.

104 V teh okoliščinah je treba ugotoviti, da je Komisija s sprejetjem člena 3 Odločbe 2000/520 prekoračila pooblastilo, ki ji je podeljeno v členu 25(6) Direktive 95/46, razlagane ob upoštevanju Listine, in da je ta člen zato neveljaven.

105 Ker sta člena 1 in 3 Odločbe 2000/520 neločljivo povezana s členoma 2 in 4 ter s prilogami k tej odločbi, njuna neveljavnost vpliva na veljavnost te odločbe v celoti.

106 Glede na zgornje navedbe je treba skleniti, da je Odločba 2000/520 neveljavna.

### **Stroški**

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



Iz teh razlogov je Sodišče (veliki senat) razsodilo:

1. Člen 25(6) 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, kakor je bila spremenjena z Uredbo (ES) št. 1882/2003 Evropskega parlamenta in Sveta z dne 29. septembra 2003, je treba ob upoštevanju členov 7, 8 in 47 Listine Evropske unije o temeljnih pravicah razlagati tako, da odločba, sprejeta na podlagi te določbe, kot je Odločba 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, v kateri Evropska komisija ugotavlja, da tretja država zagotavlja ustrezno raven varstva, ne preprečuje, da nadzorni organ države članice v smislu člena 28 navedene direktive, kakor je bila spremenjena, preuči zahtevo posameznika v zvezi z varstvom njegovih pravic in svoboščin glede obdelave osebnih podatkov, ki se nanašajo nanj in ki so bili iz države članice preneseni v to tretjo državo, kadar ta posameznik zatrjuje, da veljavno pravo in praksa v tej državi ne zagotavljata ustrezne ravni varstva.
2. Odločba 2000/520 je neveljavna.

Podpisi