

DOMSTOLENS DOM (stora avdelningen)

den 6 oktober 2015 (*)

”Begäran om förhandsavgörande – Personuppgifter – Skydd för enskilda personer med avseende på behandling av personuppgifter – Europeiska unionens stadga om de grundläggande rättigheterna – Artiklarna 7, 8 och 47 – Direktiv 95/46/EG – Artiklarna 25 och 28 – Överföring av personuppgifter till tredjeländer – Beslut 2000/520/EG – Överföring av personuppgifter till Förenta staterna – Inadekvat skyddsnivå – Giltighet – Anmälan från en enskild person vars uppgifter har överförts från Europeiska unionen till Förenta staterna – De nationella tillsynsmyndigheternas befogenheter”

I mål C-362/14,

angående en begäran om förhandsavgörande enligt artikel 267 FEUF, framställd av High Court (Irland) genom beslut av den 17 juli 2014, som inkom till domstolen den 25 juli 2014, i målet

Maximillian Schrems

mot

Data Protection Commissioner,

ytterligare deltagare i rättegången:

Digital Rights Ireland Ltd,

meddelar

DOMSTOLEN (stora avdelningen)

sammansatt av ordföranden V. Skouris, vice ordföranden K. Lenaerts, avdelningsordförandena A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (referent), S. Rodin och K. Jürimäe samt domarna A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. Šváby, M. Berger, F. Biltgen och C. Lycourgos,

generaladvokat: Y. Bot,

justitiesekreterare: förste handläggaren L. Hewlett,

efter det skriftliga förfarandet och förhandlingen den 24 mars 2015,

med beaktande av de yttranden som avgetts av:

- Maximillian Schrems, genom N. Travers, SC, P. O’Shea, BL, och G. Rudden, solicitor, samt genom H. Hofmann, Rechtsanwalt,
- Data Protection Commissioner, genom M. P. McDermott, BL, S. More O’Ferrall och D. Young, solicitors,
- Digital Rights Ireland Ltd, genom F. Crehan, BL, samt genom S. McGarr och E. McGarr, solicitors,
- Irland, genom A. Joyce, B. Coughlan och E. Creedon, samtliga i egenskap av ombud, biträdda av D. Fennelly, BL,
- Belgiens regering, genom J.-C. Halleux och C. Pochet, båda i egenskap av ombud,

- Tjeckiens regering, genom M. Smolek och J. Vlácil, båda i egenskap av ombud,
- Italiens regering, genom G. Palmieri, i egenskap av ombud, biträdd av P. Gentili, avvocato dello Stato,
- Österrikes regering, genom G. Hesse och G. Kunnert, båda i egenskap av ombud,
- Polens regering, genom M. Kamejsza, M. Pawlicka och B. Majczyna, samtliga i egenskap av ombud,
- Sloveniens regering, genom A. Grum och V. Klemenc, båda i egenskap av ombud,
- Förenade kungarikets regering, genom L. Christie och J. Beeko, båda i egenskap av ombud, biträdda av J. Holmes, barrister,
- Europaparlamentet, genom D. Moore, A. Caiola och M. Pencheva, samtliga i egenskap av ombud,
- Europeiska kommissionen, genom B. Schima, B. Martenczuk, B. Smulders och J. Vondung, samtliga i egenskap av ombud,
- Europeiska datatillsynsmannen, genom C. Docksey, A. Buchta och V. Pérez Asinari, samtliga i egenskap av ombud,

och efter att den 23 september 2015 ha hört generaladvokatens förslag till avgörande, följande

Dom

- 1 Begäran om förhandsavgörande avser tolkningen av artiklarna 25.6 och 28 i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, s. 31), i dess lydelse enligt Europaparlamentets och rådets förordning (EG) nr 1882/2003 av den 29 september 2003 (EUT L 284, s. 1), mot bakgrund av artiklarna 7, 8 och 47 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan), och, i princip, giltigheten av kommissionens beslut av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (*Safe Harbor Privacy Principles*) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat (EGT L 215, s. 7).
- 2 Begäran har framställts i ett mål mellan Maximillian Schrems och Data Protection Commissioner (dataskyddsombudsmannen) (nedan kallad ombudsmannen). Målet rör ombudsmannens beslut att inte utreda Maximillian Schrems anmälan mot Facebook Ireland Ltd (nedan kallat Facebook Ireland) med avseende på att det bolaget överför Facebookanvändarnas personuppgifter till Förenta staterna och lagrar dessa uppgifter på servrar i det landet.

Tillämpliga bestämmelser

Direktiv 95/46

- 3 Skälen 2, 10, 56, 57, 60, 62 och 63 i direktiv 95/46 har följande lydelse:

“(2) Systemen för databehandling av uppgifter är till för människornas skull. Oavsett fysiska personers medborgarskap eller hemvist måste systemen respektera dessa personers grundläggande fri- och rättigheter - särskilt rätten till privatlivet - och bidra till ... enskilda personers välfärd.

...

(10) Ändamålet med den nationella lagstiftningen om behandling av personuppgifter är att skydda grundläggande fri- och rättigheter, särskilt den rätt till privatlivet som erkänns både i artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna [, som undertecknades i Rom den 4 november 1950] och i gemenskapsrättens allmänna rättsprinciper. Av denna anledning får tillnärmningen av denna lagstiftning inte medföra någon inskränkning i det skydd de ger, utan skall i stället syfta till att garantera en hög skydds nivå inom gemenskapen.

...

(56) Gränsöverskridande flöden av personuppgifter är nödvändiga för den internationella handelns utveckling. Det skydd som genom detta direktiv tillförsäkras enskilda personer inom gemenskapen hindrar inte att personuppgifter överförs till sådana tredje länder som garanterar en adekvat skydds nivå. Frågan om skydds nivåns adekvans skall bedömas med hänsyn till alla de omständigheter som har samband med en överföring eller en grupp av överföringar.

(57) Om ett tredje land inte garanterar en adekvat skydds nivå skall överföring av personuppgifter till det landet förbjudas.

...

(60) Överföring till tredje land får i vilket fall som helst endast utföras i enlighet med bestämmelser som medlemsstaterna antagit för genomförande av detta direktiv, särskilt artikel 8 i detta.

...

(62) För skyddet av enskilda personer med avseende på behandlingen av personuppgifter är det av avgörande betydelse att medlemsstaterna inrättar oberoende tillsynsmyndigheter.

(63) Dessa myndigheter måste ges nödvändiga resurser för att utföra sina uppgifter, såsom befogenhet att – särskilt när det gäller klagomål från enskilda personer – undersöka och intervensera samt befogenheter att inleda rättsliga förfaranden. ...”

4 I artiklarna 1, 2, 25, 26, 28 och 31 i direktiv 95/46 föreskrivs följande:

”Artikel 1

Direktivets syfte

1. Medlemsstaterna skall i enlighet med detta direktiv skydda fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, i samband med behandling av personuppgifter.

...

Artikel 2

I detta direktiv avses med

- a) *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (den registrerade). En identifierbar person är en person som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet,
- b) *behandling av personuppgifter* (behandling): varje åtgärd eller serie av åtgärder som vidtas beträffande personuppgifter, vare sig det sker på automatisk väg eller inte, till

exempel insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring,

...

- d) *registeransvarig*: den fysiska eller juridiska person, den myndighet, den institution eller det andra organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. När ändamålen och medlen för behandlingen bestäms av nationella lagar och andra författningar eller av gemenskapsrätten kan den registeransvarige eller de särskilda kriterierna för att utse honom anges i nationell rätt eller i gemenskapsrätten,

...

Artikel 25

Principer

1. Medlemsstaterna skall föreskriva att överföringen av personuppgifter som är under behandling eller som är avsedda att behandlas efter överföring till tredje land endast får ske om ifrågavarande tredje land – utan att detta påverkar tillämpningen av de nationella bestämmelser som antagits till följd av de andra bestämmelserna i detta direktiv – säkerställer en adekvat skyddsnivå.
2. Bedömningen av om skyddsnivån i ett tredje land är adekvat skall ske på grundval av alla de förhållanden som har samband med en överföring eller en grupp av överföringar av uppgifter. Härvid skall särskilt beaktas uppgiftens art, den eller de avsedda behandlingarnas ändamål och varaktighet, ursprungslandet och det slutliga bestämmelselandet, de allmänna respektive särskilda rättsregler som gäller i ifrågavarande tredje land liksom de regler för yrkesverksamhet och säkerhet som gäller där.
3. Medlemsstaterna och kommissionen skall informera varandra när de anser att ett tredje land inte erbjuder en adekvat skyddsnivå enligt punkt 2.
4. Om kommissionen i enlighet med ett sådant förfarande som beskrivs i artikel 31.2 finner att ett tredje land inte erbjuder en sådan adekvat skyddsnivå som beskrivs i punkt 2 i denna artikel, skall medlemsstaterna vidta de åtgärder som är nödvändiga för att hindra överföring av uppgifter av samma slag till ifrågavarande tredje land.
5. Vid lämpligt tillfälle skall kommissionen inleda förhandlingar för att avhjälpa den situation som uppstått när kommissionen kommit till den slutsats som anges i punkt 4.
6. Kommissionen kan, i enlighet med det i artikel 31.2 angivna förfarandet, konstatera att ett tredje land genom sin interna lagstiftning eller på grund av de internationella förpliktelser som – särskilt till följd av sådana förhandlingar som anges i punkt 5 och som gäller skyddet för privatliv och enskilda personers grundläggande fri- och rättigheter – åligger landet har [säkerställer] en skyddsnivå som är adekvat i den mening som avses i punkt 2 i denna artikel.

Medlemsstaterna skall vidta de åtgärder som är nödvändiga för att följa kommissionens beslut.

Artikel 26

Undantag

1. Med undantag från artikel 25 skall medlemsstaterna – om det inte finns tvingande regler om detta i deras lagstiftning – föreskriva att överföring av personuppgifter till ett tredje land som inte har en adekvat skyddsnivå i den mening som avses i artikel 25.2 får ske om
 - a) den registrerade otvetydigt har samtyckt till den planerade överföringen, eller

- b) överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den registeransvarige eller för att på den registrerades begäran genomföra åtgärder som vidtas innan avtalet ingås, eller
- c) överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan den registeransvarige och tredje man i den registrerades intresse, eller
- d) överföringen är nödvändig eller bindande enligt författning av skäl som rör viktiga allmänna intressen eller för att fastslå, göra gällande eller försvara rättsliga anspråk, eller
- e) överföringen är nödvändig för att skydda intressen som är av avgörande betydelse för den registrerade, eller
- f) överföringen görs från ett offentligt register som enligt lagar eller andra författningar är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse, i den utsträckning som de i lagstiftningen angivna villkoren för tillgänglighet uppfylls i det enskilda fallet.

2. Utan att detta påverkar tillämpningen av punkt 1 får en medlemsstat tillåta överföring av personuppgifter till ett tredje land som inte säkerställer en skydds nivå som är adekvat enligt artikel 25.2, om den registeransvarige ställer tillräckliga garantier för att privatliv och enskilda personers grundläggande fri- och rättigheter skyddas samt för utövningen av motsvarande rättigheter. Sådana garantier kan framgå av lämpliga avtalsklausuler.

3. Medlemsstaten skall informera kommissionen och de övriga medlemsstaterna om de överföringar som tillåts enligt punkt 2.

Om en medlemsstat eller kommissionen på grunder som är berättigade med hänsyn till skyddet för privatliv och enskilda personers grundläggande fri- och rättigheter gör en invändning skall kommissionen vidta lämpliga åtgärder i enlighet med det förfarande som avses i artikel 31.2.

Medlemsstaterna skall vidta de åtgärder som är nödvändiga för att följa kommissionens beslut.

...

Artikel 28

Tillsynsmyndighet

1. Varje medlemsstat skall tillse att det utses en eller flera myndigheter som har till uppgift att inom dess territorium övervaka tillämpningen av de bestämmelser som medlemsstaterna antar till följd av detta direktiv.

Dessa myndigheter skall fullständigt oberoende utöva de uppgifter som åläggs dem.

2. Varje medlemsstat skall tillse att tillsynsmyndigheten hörs när sådana lagar eller andra författningar utarbetas som rör skyddet av enskilda personers fri- och rättigheter med avseende på behandlingen av personuppgifter.

3. Varje tillsynsmyndighet skall särskilt ha

- undersökningsbefogenheter, såsom befogenhet att få tillgång till uppgifter som blir föremål för behandling och befogenhet att inhämta alla uppgifter som är nödvändiga för att sköta tillsynen,
- effektiva befogenheter att ingripa, som till exempel att kunna avge yttranden i enlighet med artikel 20 innan en behandling äger rum, och se till att sådana yttranden i lämplig omfattning offentliggörs, att kunna besluta om blockering, utplåning eller förstöring av uppgifter, att kunna besluta om tillfälligt eller slutligt förbud mot behandling, att kunna

ge den registeransvarige varning eller tillrättavisning eller att kunna hänvisa saken till nationella parlament eller till andra politiska institutioner,

- befogenhet att inleda rättsliga förfaranden när de nationella bestämmelser som antagits till följd av detta direktiv har överträtts eller att uppmärksamma de rättsliga myndigheterna på dessa överträdelser.

Sådana beslut av tillsynsmyndigheten som går en part emot kan överklagas till domstol.

4. Var och en kan, på egen hand eller företrädd av en organisation, vända sig till tillsynsmyndigheten med begäran om skydd för sina fri- och rättigheter med avseende på behandling av personuppgifter. Den berörda personen skall informeras om vilka följder hans begäran har fått.

Var och en kan i samband med tillämpningen av de nationella bestämmelser som har antagits med stöd av artikel 13 i detta direktiv till tillsynsmyndigheten ge in en begäran om att få kontrollera om en behandling är tillåten. Den berörda personen skall informeras om vilka följder hans begäran har fått.

...

6. En tillsynsmyndighet har, oavsett vilken nationell lagstiftning som gäller för den aktuella behandlingen, behörighet att inom sin egen medlemsstats territorium utöva de befogenheter som i enlighet med punkt 3 åligger den. Varje myndighet kan av en myndighet i en annan medlemsstat anmodas att utöva sina befogenheter.

...

Artikel 31

...

2. När det hänvisas till denna artikel skall artiklarna 4 och 7 i beslut [rådets beslut 1999/468/EG av den 28 juni 1999 om de förfaranden som skall tillämpas vid utövandet av kommissionens genomförandebefogenheter (EGT L 184, s. 23)] tillämpas, med beaktande av bestämmelserna i artikel 8 i det beslutet.

..."

Beslut 2000/520

5 Kommissionen antog beslut 2000/520 med stöd av artikel 25.6 i direktiv 95/46.

6 Skälen 2, 5 och 8 i beslut 2000/520 har följande lydelse:

"(2) Kommissionen kan konstatera att ett tredje land har en adekvat skyddsnivå. I sådana fall får personuppgifter överföras från medlemsstaterna utan att det behövs några ytterligare garantier.

...

(5) Den adekvata skyddsnivån för överföring av uppgifter från gemenskapen till Förenta staterna i enlighet med detta beslut bör anses ha uppnåtts om organisationer följer *Safe Harbor Privacy*-principerna för skydd av personuppgifter som överförs från en medlemsstat till Förenta staterna (nedan kallade principerna) och de vägledande frågorna och svaren (nedan kallade FoS) som utfärdats av Förenta staternas regering den 21 juli 2000. Organisationerna bör dessutom offentliggöra sin politik för skydd av personuppgifter och vara underställda antingen Federal Trade Commission (FTC) enligt avsnitt 5 i Federal Trade Commission Act, som förbjuder illojala eller bedrägliga handlingar eller metoder i handeln och i verksamhet som påverkar handeln, eller någon

annan tillsynsmyndighet som på ett effektivt sätt ser till att principerna, tillämpade i överensstämmelse med FoS, efterlevs.

...

- (8) För att värna om öppenhet och för att bevara förmågan hos de behöriga myndigheterna i medlemsstaterna att garantera skydd av enskilda med avseende på behandlingen av deras personuppgifter är det nödvändigt att i detta beslut specificera vilka omständigheter som i undantagsfall bör medföra att vissa dataflöden avbryts, trots att skyddsnivån befunnits vara adekvat.”

7 Artiklarna 1–4 i beslut 2000/520 har följande lydelse:

”Artikel 1

1. Med avseende på artikel 25.2 i direktiv 95/46/EG skall i fråga om all verksamhet som omfattas av det direktivet, *safe harbor*-principerna om integritetsskydd (nedan kallade principerna), se bilaga I till detta beslut, tillämpade i enlighet med den vägledning som ges i de frågor och svar (nedan kallade FoS) som utfärdats av Förenta staternas handelsministerium den 21 juli 2000, se bilaga II till detta beslut, anses utgöra en adekvat skyddsnivå för personuppgifter som överförs från gemenskapen till organisationer som är etablerade i Förenta staterna med beaktande av följande dokument som utfärdats av Förenta staternas handelsministerium:

- a) En översikt över genomförandet av *safe harbor*, bilaga III.
 - b) Ett memorandum om ersättning vid kränkning av enskildas integritet och uttryckliga behörigheter i Förenta staternas lagstiftning, bilaga IV.
 - c) En skrivelse från Federal Trade Commission, bilaga V.
 - d) En skrivelse från Förenta staternas transportministerium, bilaga VI.
2. I samband med varje överföring av uppgifter skall följande villkor vara uppfyllda:
- a) Den organisation som tar emot uppgifterna har otvetydigt och offentligt förpliktat sig att följa principerna såsom de tillämpas i enlighet med FoS, och
 - b) denna organisation omfattas av de lagstadgade befogenheter som tillkommer någon av de myndigheter i Förenta staterna som anges i bilaga VII till detta beslut och som är bemyndigade att handlägga klagomål och ge upprättelse vid användning av illojala och bedrägliga metoder och att utverka skadestånd åt enskilda, oberoende av deras bosättningsland eller nationalitet, om principerna inte följs i överensstämmelse med FoS.

3. De villkor som anges i punkt 2 skall anses vara uppfyllda för varje organisation som genom självcertifiering förbinder sig att följa principerna i överensstämmelse med FoS från den dag då organisationen underrättar Förenta staternas handelsministerium, eller det organ som ministeriet bestämmer, om offentliggörandet av den förpliktelse som avses i punkt 2 a och om namnet på den myndighet som avses i punkt 2 b.

Artikel 2

Detta beslut gäller endast frågan om den skyddsnivå är adekvat som enligt principerna och FoS erbjuds i Förenta staterna, i förhållande till de krav som ställs i artikel 25.1 i direktiv 95/46/EG, och det påverkar inte tillämpningen av andra bestämmelser i det direktivet som gäller behandling av personuppgifter inom medlemsstaterna, särskilt artikel 4 i direktivet.

Artikel 3

1. Utan att det påverkar de befogenheter behöriga myndigheter i medlemsstaterna har att vidta åtgärder för att säkra efterlevnaden av nationella bestämmelser som antagits enligt

andra bestämmelser i direktiv 95/46/EG än artikel 25, får dessa myndigheter utöva sin befogenhet att tillfälligt förbjuda överföringen av uppgifter till en organisation som genom självcertifiering förbundit sig att följa principerna i överensstämmelse med FoS, i syfte att skydda enskilda med avseende på behandling av deras personuppgifter i de fall då

- a) den myndighet i Förenta staterna som avses i bilaga VII till detta beslut eller en sådan oberoende instans för handläggning av klagomål som avses under a i avsnittet om kontroll av efterlevnaden i bilaga I till detta beslut, har funnit att organisationen agerar i strid med principerna tillämpade i överensstämmelse med FoS, eller
- b) det är i hög grad sannolikt att principerna överträds, det finns välgrundad anledning att tro att den berörda instansen för handläggning av klagomål inte vidtar och inte i rätt tid kommer att vidta de åtgärder som behövs för att lösa problemet, en fortsatt överföring av uppgifterna skulle innebära en överhängande risk för allvarlig skada för registrerade, och de behöriga myndigheterna i medlemsstaten har gjort vad som under rådande omständigheter rimligvis kan krävas för att anmärka mot organisationen och ge den tillfälle att gå i svaromål.

Förbudet skall hävas så snart det säkerställts att organisationen följer principerna i överensstämmelse med FoS och de behöriga myndigheterna i Europeiska unionen har underrättats härom.

2. Medlemsstaterna skall utan dröjsmål underrätta kommissionen om åtgärder som vidtagits med stöd av punkt 1.

3. Medlemsstaterna och kommissionen skall även underrätta varandra om varje fall där en myndighet, som är ansvarig för att principerna tillämpade i överensstämmelse med FoS följs i Förenta staterna, inte kunnat säkerställa detta.

4. Om den information som inhämtats i enlighet med punkterna 1, 2 och 3 visar att någon av de myndigheter som har ansvar för att principerna tillämpade i överensstämmelse med FoS följs i Förenta staterna inte fullgör denna uppgift på ett effektivt sätt, skall kommissionen underrätta Förenta staternas handelsministerium om detta och vid behov lägga fram förslag till bestämmelser i enlighet med det förfarande som föreskrivs i artikel 31 i direktivet i syfte att helt eller tills vidare upphäva detta beslut eller begränsa dess tillämpningsområde.

Artikel 4

1. Detta beslut kan vid vilken tidpunkt som helst ändras på grundval av erfarenheter i samband med beslutets genomförande och/eller om det i Förenta staternas lagstiftning ställs krav på minst samma skyddsnivå, som den som uppnås genom principerna och FoS. Kommissionen skall under alla omständigheter utvärdera tillämpningen av detta beslut på grundval av tillgänglig information tre år efter det att beslutet delgivits medlemsstaterna och skall underrätta den kommitté som inrättats genom artikel 31 i direktiv 95/46/EG om alla iakttagelser av betydelse, däribland omständigheter som kan påverka den gjorda bedömningen att bestämmelserna i artikel 1 i detta beslut ger ett adekvat skydd i den mening som avses i artikel 25 i direktiv 95/46/EG samt varje omständighet som tyder på att detta beslut tillämpas på ett sätt som innebär diskriminering.

2. Kommissionen skall om så behövs föreslå åtgärder i enlighet med det förfarande som föreskrivs i artikel 31 i direktivet."

8 Bilaga I till beslut 2000/520 har följande lydelse:

"PRINCIPER OM *SAFE HARBOR* OCH INTEGRITETSSKYDD

fastlagda av Amerikas förenta staters handelsministerium den 21 juli 2000

...

... [H]andelsministeriet (Department of Commerce) [fastlägger] detta dokument och frågorna och svaren (principerna) i enlighet med sitt lagstadgade bemyndigande att stödja, främja och

utveckla utrikeshandeln. Principerna har utarbetats i samråd med näringslivet och allmänheten för att underlätta handel och affärsverksamhet mellan USA och EU. De är endast avsedda att tillämpas på de organisationer i USA som tar emot personuppgifter från EU och syftet är att dessa organisationer skall uppfylla villkoren för *safe harbor* samt den presumtion om 'adekvat skyddsnivå' som därmed skapas. Eftersom principerna endast är utformade för att tjäna detta specifika ändamål skulle det vara olämpligt om de godkändes för andra ändamål. ...

Det är helt och hållet frivilligt för en organisation att besluta om den vill ansluta sig till *safe harbor*-systemet, och organisationerna kan gå tillväga på olika sätt för att tillerkännas *safe harbor*-status. ...

Efterlevnaden av principerna kan begränsas a) till vad som är nödvändigt för att uppfylla krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden eller b) av lagar, myndighetsföreskrifter eller rättspraxis som skapar motstridiga skyldigheter eller ger explicita befogenheter, förutsatt att organisationen då den utövar dessa befogenheter kan visa att avvikelser från principerna begränsar sig till vad som är nödvändigt för att de övergripande legitima intressen som är beroende av dessa befogenheter skall kunna tillgodoses, eller c) om följden av direktivet eller medlemsstaternas lagstiftning är att man tillåter undantag och avvikelser förutsatt att sådana undantag eller avvikelser tillämpas i jämförbara sammanhang. I överensstämmelse med målen om ökat integritetsskydd bör organisationerna sträva efter att genomföra dessa principer öppet och fullt ut, samt även ange i sina planer för integritetsskydd på vilka områden undantag från principerna av skäl angivna i b ovan kommer att göras regelbundet. Av samma skäl förväntas organisationerna, såvida det finns en valmöjlighet enligt principerna och/eller amerikansk lag, välja en högre skyddsnivå om det är möjligt.

..."

9 Bilaga II till beslut 2000/520 har följande lydelse:

"FRÅGOR OCH SVAR (FoS)

...

FoS 6 – Självcertifiering

F: *Hur sker en organisations självcertifiering efter det att den har anslutit sig till safe harbor-principerna?*

S: En organisation omfattas av de fördelar som *safe harbor* medför från den dag då organisationen till handelsministeriet (eller dess utsedda företrädare) anmäler att den har anslutit sig till principerna genom självcertifiering i enlighet med de riktlinjer som anges nedan.

Organisationer som vill ansluta sig till *safe harbor* genom självcertifiering kan till handelsministeriet (eller dess utsedda företrädare) sända en skrivelse, som skall vara undertecknad av en person i ansvarig ställning på den organisations vägnar som ansluter sig till *safe harbor*. Denna skrivelse skall innehålla åtminstone följande uppgifter:

- 1) Organisationens namn, postadress, e-postadress, telefon- och faxnummer.
- 2) En beskrivning av den del av organisationens verksamhet som rör personuppgifter som tas emot från EU.
- 3) En beskrivning av organisationens integritetsskyddspolicy för sådana personuppgifter, vilket skall omfatta a) uppgift om hur allmänheten kan ta del av den, b) det datum den trädde i kraft, c) en kontaktpunkt för handläggningen av klagomål, ansökningar om åtkomst och andra frågor som kan uppstå inom ramen för *safe harbor*, d) den tillsynsmyndighet som är behörig att behandla klagomål som rör organisationen och gäller eventuell förekomst av illojala eller bedrägliga metoder och brott mot gällande lagstiftning om integritetsskydd (och som förtecknas i bilagan till principerna), e) namn på eventuella program för integritetsskydd som organisationen deltar i, f) kontrollmetod (t.ex. intern eller

genom tredje man) ... och g) förfarande vid oberoende instans som kan handlägga olösta klagomål.

Om organisationen vill att de fördelar som *safe harbor* innebär skall omfatta personaluppgifter som överförs från EU för att användas inom ramen för anställningsförhållandet, kan detta tillåtas om det finns en tillsynsmyndighet som är behörig att behandla klagomål som för organisationen och gäller sådana personaluppgifter som förtecknas i bilagan till principerna. ...

Handelsministeriet (eller dess utsedda företrädare) skall hålla en förteckning över alla organisationer som insänder sådana skrivelser, varigenom fördelarna med *safe harbor* garanteras. Förteckningen skall uppdateras i överensstämmelse med de skrivelser om självcertifiering som inkommer varje år och de anmälningar som erhålls i enlighet med FoS 11. ...

...

FoS 11 - Tvistlösning, genomförande och uppföljning

F: *Hur skall kraven på tvistlösning enligt principen om genomförande och uppföljning uppfyllas och hur skall en organisations upprepade underlåtenhet att följa principen hanteras?*

S: Principen om genomförande och uppföljning anger de krav som skall ställas på metoder för genomförande och uppföljning av *safe harbor*-principerna. Hur kraven som uppställs i principens punkt b skall uppfyllas framgår av FoS om kontroll (FoS 7). Denna FoS 11 behandlar punkterna a och c som både kräver oberoende instanser för behandling av klagomål. Dessa metoder kan ha olika former men de måste uppfylla kraven enligt principen om genomförande och uppföljning. En organisation kan uppfylla kraven på något av följande sätt: 1) Den kan följa ett program för integritetsskydd som utarbetats inom den privata sektorn och i vilket *safe harbor*-principerna inlemmats. I programmet skall det ingå effektiva metoder för kontroll av efterlevnaden av det slag som beskrivs i principen om genomförande och uppföljning. 2) Den kan förbinda sig att rätta sig efter beslut från lagstadgade tillsynsmyndigheter eller andra offentliga tillsynsorgan som handlägger individuella klagomål och tillhandahåller tvistlösning. 3) Den kan förbinda sig att samarbeta med dataskyddsmyndigheter inom Europeisk gemenskapen eller deras bemyndigade ombud. Denna förteckning är inte ämnad att vara uttömmande utan snarare belysande. Den privata sektorn kan utarbeta andra metoder för genomförande och uppföljning förutsatt att de uppfyller kraven enligt principen och FoS. Observera att villkoren som uppställs i principen om genomförande och uppföljning gäller utöver de krav som uppställs i punkt 3 i inledningen till principerna om att tvistlösningsmodeller skall tillhandahålla lösningar som kan verkställas enligt avsnitt 5 i lagen om en federal konkurrensmyndighet (Federal Trade Commission Act) eller liknande regelverk.

Rättsmedel.

Konsumenterna skall uppmuntras att först inge klagomål till den berörda organisationen innan de vänder sig till oberoende instanser för behandling av klagomål. ...

...

Åtgärder från den federala konkurrensmyndighetens sida.

Den federala konkurrensmyndigheten (FTC) har förbundit sig att göra en förhandsprövning av klagomål som mottagits av organ för självreglering på integritetsskyddets område, t.ex. BBBOnline och TRUSTe, och från medlemsstater i EU vilka hävdar att *safe harbor*-principerna inte följs, i syfte att avgöra huruvida det föreligger en överträdelse av avdelning 5 i Federal Trade Commission Act, som förbjuder illojala eller bedrägliga handlingar och metoder i handeln. ..."

”Integritetsskydd och skadestånd, befogenhet i lag (Legal Authorizations) samt fusioner och övertag i amerikansk lag

Detta är ett svar på EU:s begäran om förtydliganden av amerikansk lag när det gäller a) krav på skadestånd för integritetsintrång, b) uttryckliga befogenheter i amerikansk lag att använda personuppgifter på ett sätt som inte överensstämmer med *safe harbor*-principerna samt c) verkan av fusioner och övertag på *safe harbor*-åtaganden.

...

B. Utryckliga befogenheter i lag

Safe-harbor-principerna innehåller ett undantag när lagar och andra författningar eller rättspraxis skapar ’motstridiga skyldigheter eller uttryckliga befogenheter, förutsatt att organisationen då den utövar dessa befogenheter kan visa att avvikelserna från principerna begränsas till vad som är nödvändigt för att de övergripande legitima intressen som är beroende av dessa befogenheter skall kunna tillgodoses’. Självklart måste amerikanska organisationer, om de i amerikansk lag har en motstridig skyldighet, oberoende av om de anslutit sig till *safe harbor* eller inte, följa lagen. Vad gäller uttryckliga befogenheter, så är målsättningen med *safe harbor* att överbrygga skillnaderna mellan det amerikanska och det europeiska sättet att hantera integritetsskydd, men vi måste respektera den lagstiftande makt våra valda politiska ombud har. Detta smärre undantag från strikt iakttagande av *safe harbor*-principerna är ett försök att hitta en lämplig balansgång mellan berättigade intressen på båda sidor.

Undantaget inskränker sig till att gälla när det finns uttryckliga befogenheter. Som minsta gemensam nämnare måste därför den relevanta texten (lag, annan författning eller domstolsbeslut) uttryckligen tillåta *safe harbor*-organisationer att utföra den aktuella handlingen. Med andra ord kan undantaget inte göras gällande om det inte står något i lagen. Vidare kan undantaget bara gälla om de uttryckliga befogenheterna står i strid med *safe harbor*-principerna. Även i detta fall skall undantaget begränsas ’till vad som är nödvändigt för att de övergripande legitima intressen som är beroende av dessa befogenheter skall kunna tillgodoses’. Exempelvis skulle undantaget inte gälla om lagen bara tillåter ett företag att lämna ut personuppgifter till statliga organ. Om lagen å andra sidan särskilt tillåter företaget att lämna personuppgifter till statliga organ utan den enskildes samtycke, så är detta en ’uttrycklig befogenhet’ att agera på ett sätt som strider mot *safe harbor*-principerna. Alternativt kommer särskilda undantag från uttryckliga krav på meddelande och samtycke att omfattas av undantaget (eftersom det är samma sak som en särskild tillåtelse att avslöja informationen utan meddelande och samtycke). Till exempel skulle en lagparagraf som tillåter läkare att lämna ut patientjournaler till hälsovårdsmyndigheter utan föregående samtycke från patienterna kunna motivera ett undantag från principen om meddelande och valmöjlighet. Denna tillåtelse hade inte inneburit att läkaren fått rätt att lämna ut patientjournaler till friskvårdsorganisationer eller affärsdrivande laboratorier för läkemedelsforskning, vilka hade legat utanför räckvidden för den lagstadgade tillåtelsens ändamål och därför utanför undantagets räckvidd. ... Den aktuella rättsliga grunden kan vara en ’isolerad’ tillåtelse att göra vissa saker med personuppgifter, men, vilket framgår av exemplen nedan, är förmodligen ett undantag från en bredare lag som förbjuder insamling, användning eller spridning av personuppgifter.

...”

Kommissionens meddelande COM(2013) 846 final

- 11 Den 27 november 2013 antog kommissionen meddelandet till Europaparlamentet och rådet kallat ”Återskapande av förtroendet för dataflöden mellan EU och Förenta staterna (COM(2013) 846 final) (nedan kallat meddelande COM(2013) 846 final). Meddelandet åtföljdes av en rapport, även den daterad den 27 november 2013, om ”slutsatserna från EU-ordförandena i ad hoc-arbetsgruppen EU/USA för dataskydd” (*Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection*). Av punkt 1 i rapporten framgick att den tagits fram i samarbete med Amerikas förenta stater efter att det avslöjats att det i nämnda land fanns ett flertal övervakningsprogram, vilka inbegrep storskalig insamling och behandling av personuppgifter. I denna rapport fanns bland annat en utförlig genomgång av Förenta staternas rättsordning vad särskilt gäller de rättsliga grunderna för att godkänna förekomsten

av övervakningsprogram samt amerikanska myndigheters insamling och behandling av personuppgifter.

- 12 I punkt 1 i meddelande COM(2013) 846 final angav kommissionen att "[h]andelsrelaterade frågor behandlas i beslut [2000/520]" och tillade att "[d]etta beslut ger en rättslig grund för överföringar av personuppgifter från EU till företag som är etablerade i Förenta staterna och som har anslutit sig till Safe Harbour-principerna om integritetsskydd". Vidare lyfte kommissionen i samma punkt 1 särskilt fram den allt större betydelse som flödena av personuppgifterna får, vilket bland annat hänger ihop med utvecklingen av den digitala ekonomin, vilken "lett till en exponentiell tillväxt i uppgiftsbehandlingens kvantitet, kvalitet, mångfald och natur".
- 13 I punkt 2 i meddelande COM(2013) 846 påpekade kommissionen att "farhågorna [har] ökat när det gäller nivån på skyddet av EU-medborgares personuppgifter som överförs till Förenta staterna inom ramen för Safe Harbour-systemet" och att "[d]et faktum att systemet är frivilligt och bygger på förklaringar har lett till ökat fokus på öppenhet och efterlevnad".
- 14 Kommissionen angav vidare i samma punkt 2 att "EU-medborgares personuppgifter som sänds till Förenta staterna inom ramen för Safe Harbour är åtkomliga för och kan behandlas ytterligare av amerikanska myndigheter på ett sätt som är oförenligt med de ändamål för vilka uppgifterna ursprungligen samlades in i EU och sedermera överfördes till Förenta staterna" och att "[e]n majoritet av de amerikanska internetföretag som förefaller vara mer direkt berörda av dessa [övervaknings]program är certifierade enligt Safe Harbour-systemet".
- 15 I punkt 3.2 i meddelande COM(2013) 846 final påpekade kommissionen att det fanns ett antal brister i genomförandet av beslut 2000/520. För det första angav kommissionen att de certifierade amerikanska företagen inte tillämpade principerna i artikel 1.1 i beslut 2000/520 (nedan kallad *safe harbor*-principerna) och att beslutet borde förbättras vad gällde "de strukturella bristerna rörande öppenhet och tillsyn och de materiella Safe Harbour-principerna [och] tillämpningen av det undantag som kan åberopas med hänvisning till den nationella säkerheten". För det andra påpekade kommissionen att "Safe Harbour [också] fungerar ... som en kanal för överföring av personuppgifter om EU-medborgare från [unionen] till Förenta staterna av företag som är skyldiga att överlämna uppgifter till amerikanska underrättelsetjänster inom ramen för amerikanska program för insamling av underrättelseinformation".
- 16 Kommissionen drog i nämnda punkt 3.2 slutsatsen att även om det "[m]ed tanke på de konstaterade bristerna [inte] är ... möjligt att fortsätta med den nuvarande tillämpningen av Safe Harbour-beslutet [skulle emellertid] [e]tt återkallande av beslutet ... inverka negativt på intressena för de företag i [unionen] och Förenta staterna som deltar i systemet". I samma punkt 3.2 tillade slutligen kommissionen att den "å det snaraste [kommer] att inleda en dialog med de amerikanska myndigheterna för att diskutera de konstaterade bristerna".

Kommissionens meddelande COM(2013) 847 final

- 17 Den 27 november 2013 antog kommissionen även meddelandet till Europaparlamentet och rådet om hur principerna om integritetsskydd (*safe harbor*) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU (COM(2013) 847 final) (nedan kallat meddelande COM(2013) 847 final). Såsom framgår av punkt 1 i detta meddelande byggde meddelandet bland annat på information som inhämtats inom ramen för Europeiska unionens och Förenta staternas gemensamma ad hoc-arbetsgrupp, och det följde på två utvärderingsrapporter från kommissionen som hade offentliggjorts år 2002 respektive år 2004.
- 18 I punkt 1 i meddelande COM(2013) 847 final anges att det sätt på vilket beslut 2000/520 fungerar "bygger på åtaganden och självcertifiering från de medverkande företagens sida". Det anges även att "[d]eltagande i systemet är frivilligt, men reglerna är bindande för dem som ansluter sig".
- 19 Vidare framgår det av punkt 2.2 i meddelande COM(2013) 847 final att den 26 september 2013 uppgick antalet certifierade företag till 3 246, och dessa företag tillhörde många olika industri- och tjänstesektorer. De flesta av dessa företag tillhandahöll tjänster på EU:s inre marknad,

särskilt inom internetsektorn, och några av dem var EU-företag som hade dotterbolag i Förenta staterna. Vissa av dessa företag behandlade data rörande anställda i Europa som överfördes till Förenta staterna i personalförvaltnings syfte.

- 20 I samma punkt 2.2 underströk kommissionen att "Eventuella luckor när det gäller insyn och tillsyn på den amerikanska sidan [ledde] till att ansvaret [vältrades] över till europeiska dataskyddsmyndigheter och till de företag som använder systemet".
- 21 Av bland annat punkterna 3–5 och 8 i meddelande COM(2013) 847 final framgår att ett betydande antal certifierade företag inte alls, eller endast delvis, följde *safe harbor*-principerna.
- 22 Vidare angav kommissionen i punkt 7 i samma meddelande att "[d]et verkar ... som om alla företag som deltar i Prism-programmet [omfattande program för insamling av underrättelseinformation] och som ger de amerikanska myndigheterna tillgång till uppgifter som lagras och behandlas i Förenta staterna, är *safe harbour*-certifierade" och att *safe harbour*-systemet därmed "[blivit] en av de kanaler genom vilken den amerikanska underrättelsetjänsten får möjlighet till att samla in personuppgifter som ursprungligen behandlats i [unionen]". Kommissionen konstaterade härvidlag i punkt 7.1 i meddelandet att det "finns ... ett antal rättsliga grunder enligt amerikansk lagstiftning som tillåter omfattande insamling och behandling av personuppgifter som lagras eller på annat sätt behandlas av företag som är baserade i Förenta staterna" och att "[s]torskalkigheten i dessa program kan leda till att amerikanska myndigheter får tillgång till och vidarebehandlar uppgifter som överförs inom ramen för *safe harbour* utöver vad som är absolut nödvändigt och proportionerligt för att skydda den nationella säkerheten enligt undantaget i [beslut 2000/520]".
- 23 Punkt 7.2 i meddelande COM(2013) 847 final har rubriken "Begränsningar och möjlighet till prövning". I denna punkt 7.2 underströk kommissionen att "garantierna enligt amerikansk lagstiftning [gäller] främst amerikanska medborgare eller i Förenta staterna lagligen bosatta personer" och att "[i]ngen möjlighet [finns] för registrerade personer, varken i EU eller i Förenta staterna, att få tillgång till, rätta eller radera uppgifter eller möjlighet till administrativ eller rättslig prövning med avseende på insamling och vidare behandling av personuppgifter som sker inom ramen för amerikanska övervakningsprogram".
- 24 Enligt punkt 8 i meddelande COM(2013) 847 final fanns bland de certifierade företagen "[i]nternetföretag som Google, Facebook, Microsoft, Apple och Yahoo", vilka har "hundratals miljoner användare i Europa" och överför personuppgifter till Förenta staterna för behandling.
- 25 Kommissionen angav i samma punkt 8 att "[u]nderrättelseorganens omfattande tillgång till de uppgifter som *safe harbour*-certifierade företag överför till Förenta staterna ger dessutom upphov till allvarliga frågor om kontinuiteten för européers dataskyddsrättigheter när deras uppgifter överförs till Förenta staterna".

Målet vid den nationella domstolen och tolkningsfrågorna

- 26 Maximilian Schrems är medborgare i Österrike och bosatt i den medlemsstaten. Han har använt det sociala nätverket Facebook (nedan kallat Facebook) sedan år 2008.
- 27 Alla personer med hemvist inom unionen som vill använda Facebook måste i samband med att de registrerar sig ingå ett avtal med Facebook Ireland, ett dotterbolag till moderbolaget Facebook Inc., vilket i sin tur har sitt säte i Förenta staterna. Personuppgifterna om Facebookanvändare med hemvist inom unionen överförs helt eller delvis till servrar tillhörande Facebook Inc. vilka är belägna i Förenta staterna där uppgifterna behandlas.
- 28 Maximilian Schrems gjorde den 25 juni 2013 en anmälan till ombudsmannen där han i huvudsak begärde att ombudsmannen skulle använda sin lagstadgade befogenhet och förbjuda Facebook Ireland att överföra personuppgifter till Förenta staterna. Maximilian Schrems gjorde gällande att Förenta staternas aktuella rätt och praxis inte garanterade

tillräckligt skydd för personuppgifter som lagras i Förenta staterna mot den övervakningsverksamhet som bedrevs av myndigheterna där. Maximillian Schrems hänvisade härvidlag till Edward Snowdens avslöjanden om de amerikanska underrättelsetjänsternas verksamhet, och särskilt National Security Agencys verksamhet (nedan kallat NSA).

- 29 Ombudsmannen ansåg sig inte vara skyldig att utreda de omständigheter som Maximillian Schrems hade åberopat i sin anmälan och avsåg den. Ombudsmannen ansåg att det inte fanns några bevis för att NSA hade fått åtkomst till Maximillian Schrems personuppgifter. Ombudsmannen tillade att Maximillian Schrems inte kunde ha någon framgång med de grunder som han åberopat i sin anmälan, eftersom alla frågor om huruvida skyddet av personuppgifter i Förenta staterna är adekvat ska avgöras i överensstämmelse med beslut 2000/520 och kommissionen i detta beslut konstaterat att Amerikas förenta stater säkerställer en adekvat skyddsnivå.
- 30 Maximillian Schrems överklagade ombudsmannens beslut att avslå hans anmälan till High Court. Efter att ha granskat den bevisning som hade framlagts i målet fann High Court att elektronisk övervakning och uppfångande av personuppgifter som överförs från unionen till Förenta staterna fyller nödvändiga och oundgängliga syften som ligger i allmänintresset. High Court tillade emellertid att NSA och andra federala organ har gått "mycket långt utöver" dessa syften.
- 31 Enligt High Court har unionsmedborgarna i praktiken inte någon rätt att yttra sig. Tillsynen av underrättelsetjänsternas verksamhet sker enligt ett förfarande som är hemligt och som inte är kontradiktoriskt. När personuppgifter väl har överförts till Förenta staterna, kan NSA och andra amerikanska federala organ, såsom Federal Bureau of Investigation (FBI), få åtkomst till dessa uppgifter inom ramen för ospecifika och storskaliga övervaknings- och uppfångandeåtgärder.
- 32 High Court konstaterade att irländsk rätt förbjuder överföring av personuppgifter till en annan stat, med undantag för när den främmande staten säkerställer en adekvat skyddsnivå för privatlivet och för de grundläggande fri- och rättigheterna. De grundlagsfästa rättigheterna till ett privatliv och till respekt för hemmets okränkbarhet är så betydelsefulla i irländsk rätt att varje ingrepp i dessa rättigheter måste vara proportionerligt och uppfylla de lagstadgade kraven.
- 33 Storskalig och ospecifik åtkomst till personuppgifter strider enligt High Court uppenbart mot proportionalitetsprincipen och de grundläggande värden som skyddas i den irländska grundlagen. För att ett sådant uppfångande av elektroniska kommunikationer ska kunna anses vara förenlig med grundlagen måste det bevisas att uppfångandet är målinriktat, att övervakningen av specifika personer eller grupper av personer är objektivt motiverad med hänvisning till intresset av att upprätthålla den nationella säkerheten och bekämpa brottslighet samt att det finns tillräckliga och kontrollerbara garantier. Därför anser High Court att om det nationella målet skulle prövas enbart mot bakgrund av irländsk rätt, skulle, mot bakgrund av de förevarande allvarliga tvivlen angående huruvida Amerikas förenta stater säkerställer en adekvat skyddsnivå för personuppgifter, slutsatsen bli att ombudsmannen borde ha undersökt de omständigheter som Maximillian Schrems åberopat i sin anmälan och att ombudsmannen inte hade rätt att avslå Maximillian Schrems anmälan.
- 34 High Court anser emellertid att det nationella målet rör tillämpningen av unionsrätten i den mening som avses i artikel 51 i stadgan, vilket betyder att lagenligheten av ombudsmannens beslut ska prövas mot bakgrund av unionsrätten. Enligt High Court uppfyller beslutet 2000/520 inte de krav som följer av såväl artiklarna 7 och 8 i stadgan som av de principer som domstolen angav i sin dom Digital Rights Ireland m.fl. (C-293/12 och C-594/12, EU:C:2014:238). Rätten till respekt för privatlivet, som garanteras i artikel 7 i stadgan och som följer av de grundläggande värderingar som är gemensamma för medlemsstaternas traditioner, skulle fräntas all innebörd om myndigheter hade rätt att informellt och generellt få åtkomst till elektroniska kommunikationer utan att behöva anföra sakliga skäl avseende nationell säkerhet eller brottsbekämpning med direkt koppling till de berörda individerna och helt utan tillräckliga och kontrollerbara garantier.
- 35 High Court har vidare påpekat att Maximillian Schrems genom sitt överklagande i själva verket hävdade att *safe harbor*-systemet, som infördes genom beslut 2000/520 och som ligger till

grund för det beslut som angrips i det nationella målet, är olagligt. Trots att Maximilian Schrems formellt sett inte har bestritt giltigheten av vare sig direktiv 95/46 eller beslut 2000/520, uppkommer enligt High Court frågan huruvida, mot bakgrund av artikel 25.6 i direktiv 95/46, ombudsmannen var bunden av kommissionens konstaterande i beslut 2000/520 att Amerikas förenta stater säkerställer en adekvat skyddsnivå, eller om artikel 8 i stadgan gav ombudsmannen rätt att i förekommande fall bortse från ett sådant konstaterande.

36 Mot denna bakgrund beslutade den hänskjutande domstolen att vilandeförklara målet och ställa följande frågor till domstolen:

- ”1) Är den ombudsman som ansvarar för att tillämpa dataskyddslagstiftningen, när ombudsmannen ska pröva en anmälan rörande överföring av personuppgifter till ett tredjeland (i det aktuella fallet till Förenta staterna) vars rätt och praxis enligt klaganden inte garanterar ett adekvat skydd för den berörda personen, helt bunden av det konstaterande från unionens sida med motsatt innebörd som återfinns i beslut 2000/520, mot bakgrund av artiklarna 7, 8 och 47 i stadgan och trots bestämmelserna i artikel 25.6 i direktiv 95/46?
- 2) Om så inte är fallet, får eller ska ombudsmannen göra en egen utredning och undersöka hur de faktiska omständigheterna har utvecklats sedan beslut 2000/520 först offentliggjordes?”

Prövning av tolkningsfrågorna

37 Den hänskjutande domstolen har ställt sina frågor, som ska besvaras tillsammans, för att få klarhet i huruvida, och i vilken omfattning, artikel 25.6 i direktiv 95/46, jämförd med artiklarna 7, 8 och 47 i stadgan, ska tolkas så, att ett beslut som antagits med stöd av denna bestämmelse, såsom beslut 2000/520, genom vilket kommissionen konstaterar att ett tredjeland säkerställer en adekvat skyddsnivå, utgör hinder för att en medlemsstats tillsynsmyndighet, i den mening som avses i artikel 28 i direktivet, utreder en persons begäran om skydd för sina fri- och rättigheter med avseende på behandling av personuppgifter rörande vederbörande, vilka har överförts från en medlemsstat till detta tredjeland, när denna person gör gällande att detta tredjelands rätt och praxis inte säkerställer en adekvat skyddsnivå.

Befogenheterna för de nationella tillsynsmyndigheterna, i den mening som avses i artikel 28 i direktiv 95/46, när det föreligger ett kommissionsbeslut antaget med stöd av artikel 25.6 i direktivet

38 Domstolen erinrar inledningsvis om att eftersom bestämmelserna i direktiv 95/46 reglerar behandling av personuppgifter som kan innebära intrång i de grundläggande friheterna, och då särskilt i rätten till respekt för privatlivet, måste bestämmelserna i fråga med nödvändighet tolkas mot bakgrund av de grundläggande rättigheterna, vilka garanteras i stadgan (se dom Österreichischer Rundfunk m.fl., C-465/00, C-138/01 och C-139/01, EU:C:2003:294, punkt 68, dom Google Spain och Google, C-131/12, EU:C:2014:317, punkt 68, och dom Ryneš, C-212/13, EU:C:2014:2428, punkt 29).

39 Av såväl artikel 1 som skälen 2 och 10 i direktiv 95/46 framgår att syftet med direktivet inte endast är att säkerställa ett effektivt och fullständigt skydd för fysiska personers grundläggande fri- och rättigheter, särskilt rätten till respekt för privatlivet, i samband med behandling av personuppgifter, utan även att säkerställa en hög skyddsnivå när det gäller dessa grundläggande fri- och rättigheter. Betydelsen av såväl den grundläggande rätten till respekt för privatlivet, vilken garanteras i artikel 7 i stadgan, som den grundläggande rätten till skydd för personuppgifter, vilken garanteras i artikel 8 i stadgan, har också understrukits i domstolens praxis (se dom Rijkeboer, C-553/07, EU:C:2009:293, punkt 47, dom Digital Rights Ireland m.fl., C-293/12 och C-594/12, EU:C:2014:238, punkt 53, och dom Google Spain och Google, C-131/12, EU:C:2014:317, punkterna 53, 66 och 74 och där angiven rättspraxis).

40 Vad gäller de nationella tillsynsmyndigheternas befogenhet avseende överföringen av personuppgifter till tredjeländer, följer det av artikel 28.1 i direktiv 95/46 att medlemsstaterna ska utse en eller flera tillsynsmyndigheter som fullständigt oberoende ska övervaka

efterlevnaden av unionsbestämmelserna om skydd för enskilda personer när det gäller behandling av sådana uppgifter. Detta krav framgår även av unionens primärrätt, bland annat av artikel 8.3 i stadgan och av artikel 16.2 FEUF (se, för ett liknande resonemang, dom kommissionen/Österrike, C-614/10, EU:C:2012:631, punkt 36, och dom kommissionen/Ungern, C-288/12, EU:C:2014:237, punkt 47).

- 41 Garantin för de nationella tillsynsmyndigheternas oberoende är avsedd att säkerställa en effektiv och tillförlitlig övervakning av att bestämmelserna om skydd för enskilda personer med avseende på behandling av personuppgifter följs, och den ska tolkas mot bakgrund av det syftet. Garantin har införts för att förstärka skyddet av de personer och organ som berörs av dessa myndigheters beslut. Såsom påpekas i skäl 62 i direktiv 95/46 är inrättandet av oberoende tillsynsmyndigheter i medlemsstaterna således av avgörande betydelse för skyddet av enskilda personer med avseende på behandlingen av personuppgifter (se dom kommissionen/Tyskland, C-518/07, EU:C:2010:125, punkt 25, och dom kommissionen/Ungern, C-288/12, EU:C:2014:237, punkt 48 och där angiven rättspraxis).
- 42 För att garantera detta skydd ska de nationella tillsynsmyndigheterna bland annat säkerställa en riktig avvägning mellan den grundläggande rätten till privatliv, å ena sidan, och de intressen som avser ett fritt flöde av personuppgifter, å andra sidan (se, för ett liknande resonemang, dom kommissionen/Tyskland, C-518/07, EU:C:2010:125, punkt 24, och dom kommissionen/Ungern, C-288/12, EU:C:2014:237, punkt 51).
- 43 Dessa myndigheter förfogar över en vid uppsättning befogenheter för detta ändamål. Dessa befogenheter, vilka anges på ett icke-uttömmande sätt i artikel 28.3 i direktiv 95/46, utgör nödvändiga resurser för att utöva myndigheternas uppgifter, såsom understryks i skäl 63 i direktivet. Således har dessa myndigheter bland annat undersökningsbefogenheter, såsom befogenheten att inhämta alla uppgifter som är nödvändiga för att sköta tillsynen, effektiva befogenheter att ingripa, såsom befogenheten att besluta om tillfälligt eller slutligt förbud mot behandling av uppgifter, och även befogenhet att inleda rättsliga förfaranden.
- 44 Förvisso framgår det av artikel 28.1 och 28.6 i direktiv 95/46 att de nationella tillsynsmyndigheternas befogenheter avser behandling av personuppgifter inom den medlemsstats territorium till vilken dessa myndigheter hör, varför dessa myndigheter inte har några befogenheter, med stöd av denna artikel 28, vad gäller behandling av sådana uppgifter inom ett tredjelands territorium.
- 45 Emellertid utgör åtgärden att låta överföra personuppgifter från en medlemsstat till ett tredjeland i sig en behandling av personuppgifter i den mening som avses i artikel 2 b i direktiv 95/46 (se, för ett liknande resonemang, dom parlamentet/rådet och kommissionen, C-317/04 och C-318/04, EU:C:2006:346, punkt 56) som utförs inom en medlemsstats territorium. I nämnda bestämmelse definieras nämligen "behandling av personuppgifter" som "varje åtgärd eller serie av åtgärder som vidtas beträffande personuppgifter, vare sig det sker på automatisk väg eller inte", och som ett exempel anges "utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter".
- 46 I skäl 60 i direktiv 95/46 anges att överföring av personuppgifter till tredjeland endast får utföras i enlighet med bestämmelser som medlemsstaterna antagit för genomförande av detta direktiv. Genom kapitel IV i direktiv 95/46, vari artiklarna 25 och 26 ingår, infördes en reglering som syftar till att säkerställa att medlemsstaterna har kontroll över överföringen av personuppgifter till tredjeländer. Detta system utgör ett komplement till det allmänna system som införts genom kapitel II i det nämnda direktivet, vilket kapitel avser allmänna bestämmelser om tillåten behandling av personuppgifter (se, för ett liknande resonemang, dom Lindqvist, C-101/01, EU:C:2003:596, punkt 63).
- 47 Enligt artikel 8.3 i stadgan och artikel 28 i direktiv 95/46 är de nationella tillsynsmyndigheterna ansvariga för kontrollen av efterlevnaden av unionsbestämmelserna om skyddet av enskilda personer med avseende på behandlingen av personuppgifter. Respektive tillsynsmyndighet har således befogenhet att kontrollera huruvida en överföring till ett tredjeland av personuppgifter från den medlemsstat till vilken myndigheten hör uppfyller de krav som följer av direktiv 95/46.

- 48 Även om det i skäl 56 i direktiv 95/46 medges att överföringar av personuppgifter från medlemsstaterna till tredjeländer är nödvändiga för den internationella handelns utveckling, är principen i direktiv 95/46, vilken anges i artikel 25.1, att sådana överföringar endast får ske om tredjeländerna säkerställer en adekvat skyddsnivå.
- 49 Vidare anges i skäl 57 i direktiv 95/46 att om ett tredjeland inte säkerställer en adekvat skyddsnivå ska överföring av personuppgifter till det landet förbjudas.
- 50 För att kontrollera överföringar av personuppgifter till tredjeländer beroende på den skyddsnivå som säkerställs i respektive land, åläggs medlemsstaterna och kommissionen enligt artikel 25 i direktiv 95/46 ett antal skyldigheter. Såsom generaladvokaten har påpekat i punkt 86 i sitt förslag till avgörande framgår det särskilt av denna artikel att ett konstaterande enligt vilket ett tredjeland säkerställer eller inte säkerställer en adekvat skyddsnivå kan göras antingen av medlemsstaterna eller av kommissionen.
- 51 Kommissionen får med stöd av artikel 25.6 i direktiv 95/46 anta ett beslut i vilket den konstaterar att ett tredjeland säkerställer en adekvat skyddsnivå. Av artikel 25.6 andra stycket framgår att ett sådant beslut riktar sig till medlemsstaterna, som ska vidta de åtgärder som är nödvändiga för att följa beslutet. I enlighet med artikel 288 FEUF fjärde stycket är beslutet bindande för alla de medlemsstater som det riktar sig till, och det är således bindande för alla organ i dessa stater (se, för ett liknande resonemang, dom Albako Margarinefabrik, 249/85, EU:C:1987:245, punkt 17, och dom Mediaset, C-69/13, EU:C:2014:71, punkt 23), i den utsträckning det medför tillåtelse att överföra personuppgifter från medlemsstaterna till det tredjeland som avses i beslutet.
- 52 Så länge som kommissionens beslut inte har ogiltigförklarats av domstolen kan således medlemsstaternas och deras organ, däribland deras oberoende tillsynsmyndigheter, förvisso inte vidta åtgärder som strider mot ett sådant kommissionsbeslut, såsom rättsakter i vilka det med bindande verkan konstateras att det tredjeland som avses i beslutet inte säkerställer en adekvat skyddsnivå. Unionsinstitutionernas rättsakter presumeras nämligen vara lagenliga och har rättsverkan så länge de inte har återkallats, eller förklarats vara ogiltiga efter en talan om ogiltigförklaring eller till följd av en begäran om förhandsavgörande eller invändning om rättsstridighet (dom kommissionen/Grekland, C-475/01, EU:C:2004:585, punkt 18 och där angiven rättspraxis).
- 53 Ett kommissionsbeslut som har antagits med stöd av artikel 25.6 i direktiv 95/46, såsom beslut 2000/520, kan emellertid inte hindra personer vilkas personuppgifter överförts, eller kan komma att överföras, till ett tredjeland, att vända sig till de nationella tillsynsmyndigheterna med en begäran om skydd för sina fri- och rättigheter med avseende på behandling av personuppgifter, i den mening som avses i artikel 28.4 i direktiv 95/46. Såsom generaladvokaten har påpekat i punkterna 61, 93 och 116 i sitt förslag till avgörande kan ett sådant beslut inte heller omintetgöra eller ens inskränka de befogenheter som de nationella tillsynsmyndigheterna uttryckligen ges i artikel 8.3 i stadgan och artikel 28 i direktiv 95/46.
- 54 Kontrollen av överföringar av personuppgifter till tredjeländer, vilka varit föremål för ett kommissionsbeslut i enlighet med artikel 25.6 i direktivet, är varken enligt artikel 8.3 i stadgan eller artikel 28 i direktiv 95/46 utesluten från de nationella tillsynsmyndigheternas befogenhetsområde.
- 55 I synnerhet finns det i artikel 28.4 första stycket i direktiv 95/46, i vilket det anges att "var och en [kan vända sig till de nationella tillsynsmyndigheterna] ... med begäran om skydd för sina fri- och rättigheter med avseende på behandling av personuppgifter", inte något undantag härvidlag för det fall att kommissionen har antagit ett beslut med stöd av artikel 25.6 i direktivet.
- 56 Det skulle vidare strida mot det system som införts genom direktiv 95/46 och syftet med artiklarna 25 och 28 i direktivet att ett kommissionsbeslut som har antagits med stöd av artikel 25.6 i direktiv 95/46 medför att en nationell tillsynsmyndighet hindras från att utreda en enskild persons begäran om skydd för sina fri- och rättigheter med avseende på behandling

av personuppgifter som överförs, eller kan komma att överföras, från en medlemsstat till ett tredjeland som avses i beslutet.

- 57 Tvärtom är artikel 28 i direktiv 95/46 i kraft av sin beskaffenhet tillämplig på all behandling av personuppgifter. Även när det föreligger ett kommissionsbeslut som har antagits med stöd av artikel 25.6 i direktiv 95/46, måste således de nationella tillsynsmyndigheterna, när en enskild person har inkommit med en begäran om skydd för sina fri- och rättigheter med avseende på behandling av personuppgifter rörande vederbörande, kunna genomföra en fullständigt oberoende utredning av huruvida överföringen av dessa uppgifter har skett i enlighet med de krav som uppställs i direktivet.
- 58 I annat fall skulle de personer vilkas personuppgifter har överförts, eller kan komma att överföras, till det aktuella tredjelandet berövas den rätt att lämna in en begäran till de nationella tillsynsmyndigheterna, vilken garanteras i artikel 8.1 och 8.3 i stadgan, i syfte att skydda sina grundläggande rättigheter (se, analogt, dom Digital Rights Ireland m.fl., C-293/12 och C-594/12, EU:C:2014:238, punkt 68).
- 59 En begäran i den mening som avses i artikel 28.4 i direktiv 95/46, genom vilken en person vars personuppgifter har överförts, eller kan komma att överföras, till ett tredjeland gör gällande, såsom i det nationella målet, att det aktuella tredjelandets rätt och praxis inte säkerställer en adekvat skyddsnivå, trots det som kommissionen konstaterat i ett beslut antaget med stöd av artikel 25.6 i direktivet, ska förstås som gällande i huvudsak huruvida detta beslut är förenligt med skyddet för privatlivet och enskilda personers grundläggande fri- och rättigheter.
- 60 Det ska härvid erinras om att enligt domstolens fasta praxis är unionen en rättslig union vars institutioner är underkastade prövning av om deras rättsakter står i överensstämmelse med bland annat fördragen och de allmänna rättsprinciperna samt de grundläggande rättigheterna (se, för ett liknande resonemang, dom kommissionen m.fl./Kadi, C-584/10 P, C-593/10 P och C-595/10 P, EU:C:2013:518, punkt 66, dom Inuit Tapiriit Kanatami m.fl./parlamentet och rådet, C-583/11 P, EU:C:2013:625, punkt 91, och dom Telefónica/kommissionen, C-274/12 P, EU:C:2013:852, punkt 56). De beslut som kommissionen har antagit med stöd av artikel 25.6 i direktiv 95/46 kan således inte undgå en sådan kontroll.
- 61 Det är emellertid domstolen som är exklusivt behörig att förklara en unionsrättsakt, såsom ett kommissionsbeslut som har antagits med stöd av artikel 25.6 i direktiv 95/46, ogiltig, och denna exklusiva behörighet har till syfte att upprätthålla rättssäkerheten genom att säkerställa unionsrättens enhetliga tillämpning (se dom Melki och Abdeli, C-188/10 och C-189/10, EU:C:2010:363, punkt 54, och dom CIVAD, C-533/10, EU:C:2012:347, punkt 40).
- 62 De nationella domstolarna har förvisso rätt att undersöka giltigheten av en unionsrättsakt, såsom ett kommissionsbeslut som har antagits med stöd av artikel 25.6 i direktiv 95/46. Dessa domstolar har emellertid inte befogenhet att själva ogiltigförklara en sådan rättsakt (se, för ett liknande resonemang, dom Foto-Frost, 314/85, EU:C:1987:452, punkterna 15–20, och dom IATA och ELFAA, C-344/04, EU:C:2006:10, punkt 27). Än mindre har de nationella tillsynsmyndigheterna, när de utreder en begäran i den mening som avses i artikel 28.4 i direktiv 95/46 angående huruvida ett kommissionsbeslut som har antagits med stöd av artikel 25.6 i direktiv 95/46 är förenligt med skyddet för privatlivet och enskilda personers grundläggande fri- och rättigheter, rätt att själva ogiltigförklara ett sådant beslut.
- 63 Mot bakgrund av ovanstående överväganden ankommer det på en nationell tillsynsmyndighet att med vederbörlig omsorg utreda en begäran om skydd för sina fri- och rättigheter med avseende på behandling av personuppgifter som framställts av en person vars personuppgifter överförs, eller kan komma att överföras, till ett tredjeland som varit föremål för ett kommissionsbeslut med stöd av artikel 25.6 i direktiv 95/46, och i samband med vilken vederbörande, såsom i det nationella målet, gör gällande att beslutet inte är förenligt med skyddet för privatlivet och enskilda personers grundläggande fri- och rättigheter.
- 64 För det fall att en nationell tillsynsmyndighet kommer fram till att det saknas fog för de argument som anförts till stöd för begäran och därför avslår den, följer det av artikel 28.3

andra stycket i direktiv 95/46, jämförd med artikel 47 i stadgan, att den person som inkommit med denna begäran ska ha tillgång till rättsmedel med vilka han eller hon vid nationella domstolar kan angripa det beslut som gått vederbörande emot. Mot bakgrund av den rättspraxis som redovisats i punkterna 61 och 62 i förevarande dom är dessa domstolar skyldiga att vilandeförklara målet och hänskjuta en giltighetsfråga till EU-domstolen för förhandsavgörande, för det fall att en nationell domstol bedömer att det finns fog för en eller flera av de grunder som parterna åberopar – eller som nämnda domstol i förekommande fall prövar ex officio – till stöd för att unionsakten ska anses ogiltig (se, för ett liknande resonemang, dom T & L Sugars och Sidul Açúcares/kommissionen, C-456/13 P, EU:C:2015:284, punkt 48 och där angiven rättspraxis).

65 Om den nationella tillsynsmyndigheten däremot anser att det finns fog för de invändningar som framförts av den person som inkommit med en begäran till myndigheten om skydd för vederbörandes fri- och rättigheter med avseende på behandlingen av personuppgifter, måste myndigheten, i enlighet med artikel 28.3 första stycket tredje strecksatsen i direktiv 95/46, särskild jämförd med artikel 8.3 i stadgan, ha befogenhet att inleda rättsliga förfaranden. Det ankommer härvidlag på den nationella lagstiftaren att föreskriva rättsmedel som gör det möjligt för den nationella tillsynsmyndigheten att vid nationella domstolar göra gällande de invändningar som den anser att det finns fog för, så att nationella domstolar, för det fall att de delar myndighetens tvivel angående kommissionsbeslutet giltighet, kan hänskjuta en begäran om förhandsavgörande för att pröva detta besluts giltighet.

66 Mot denna bakgrund ska de hänskjutna frågorna besvaras enligt följande. Artikel 25.6 i direktiv 95/46, jämförd med artiklarna 7, 8 och 47 i stadgan, ska tolkas så, att ett beslut som har antagits med stöd av denna bestämmelse, såsom beslut 2000/520, genom vilket kommissionen konstaterar att ett tredjeland säkerställer en adekvat skyddsnivå, inte utgör hinder för att en medlemsstats tillsynsmyndighet, i den mening som avses i artikel 28 i direktivet, prövar en persons begäran om skydd för sina fri- och rättigheter med avseende på behandling av personuppgifter rörande vederbörande, vilka har överförts från en medlemsstat till detta tredjeland, när denna person gör gällande att detta tredjelands rätt och praxis inte säkerställer en adekvat skyddsnivå.

Huruvida beslut 2000/520 är giltigt

67 Såsom framgår av de förklaringar som den hänskjutande domstolen lämnat avseende de ställda frågorna, har Maximilian Schrems i det nationella målet gjort gällande att Förenta staternas rätt och praxis inte säkerställer en adekvat skyddsnivå i den mening som avses i artikel 25 i direktiv 95/46. Såsom generaladvokaten har påpekat i punkterna 123 och 124 i sitt förslag till avgörande har Maximilian Schrems uttryckt tvivel, vilka för övrigt i huvudsak tycks delas av den hänskjutande domstolen, angående giltigheten av beslut 2000/520. Under dessa omständigheter ska mot bakgrund av de konstateranden som gjorts i punkterna 60–63 i förevarande dom, och i syfte att lämna ett fullständigt svar till den hänskjutande domstolen, det prövas huruvida detta beslut motsvarar de krav som följer av direktiv 95/46 jämfört med stadgan.

De krav som följer av artikel 25.6 i direktiv 95/46

68 Såsom redan har påpekats i punkterna 48 och 49 i förevarande dom förbjuder artikel 25.1 i direktiv 95/46 överföring av personuppgifter till ett tredjeland som inte säkerställer en adekvat skyddsnivå.

69 Emellertid föreskrivs i artikel 25.6 första stycket i direktiv 95/46 att kommissionen för att kontrollera sådana överföringar "kan ... konstatera att ett tredje land genom sin interna lagstiftning eller på grund av de internationella förpliktelser som – ... [vad] ... gäller skyddet för privatliv och enskilda personers grundläggande fri- och rättigheter – åligger landet [säkerställer] en skyddsnivå som är adekvat i den mening som avses i punkt 2 i denna artikel."

70 Förvisso finns det inte i vare sig artikel 25.2 i direktiv 95/46 eller i någon annan av direktivets bestämmelser någon definition av begreppet "adekvat skyddsnivå". I synnerhet anges i artikel 25.2 i direktivet endast att bedömningen av huruvida skyddsnivån i ett tredjeland är adekvat "skall ske på grundval av alla de förhållanden som har samband med en överföring

eller en grupp av överföringar av uppgifter”, och i bestämmelsen ges en icke-uttömmande uppräkningslista av de omständigheter som ska beaktas vid en sådan bedömning.

- 71 Emellertid framgår av själva ordalydelsen i artikel 25.6 i direktiv 95/46, att denna bestämmelse kräver att ett tredjeland genom sin interna lagstiftning eller på grund av de internationella förpliktelser som åligger landet ”säkerställer” en skyddsnivå som är adekvat. Enligt samma bestämmelse gäller vidare att frågan huruvida den skyddsnivå som säkerställs av tredjelandet är adekvat ska bedömas ”[vad] gäller skyddet för privatliv och enskilda personers grundläggande fri- och rättigheter”.
- 72 Genom artikel 25.6 i direktiv 95/46 genomförs sålunda den uttryckliga skyldigheten att skydda personuppgifter som föreskrivs i artikel 8.1 i stadgan. Såsom generaladvokaten har påpekat i punkt 139 i sitt förslag till avgörande syftar denna bestämmelse till att säkerställa att den höga skyddsnivån vidmakthålls vid överföring av personuppgifter till ett tredjeland.
- 73 Förvisso innebär ordet ”adekvat” i artikel 25.6 i direktiv 95/46 att det inte kan krävas att ett tredjeland säkerställer en skyddsnivå som är identisk med den som garanteras i unionens rättsordning. Såsom generaladvokaten har påpekat i punkt 141 i sitt förslag till avgörande ska begreppet ”adekvat skyddsnivå” förstås som att det krävs att detta tredjeland, genom sin interna lagstiftning eller på grund av de internationella förpliktelser som åligger landet, de facto säkerställer en nivå för skyddet av grundläggande fri- och rättigheter som är väsentligen likvärdig med den skyddsnivå som garanteras inom unionen enligt direktiv 95/46 jämfört med stadgan. Om ett sådant krav inte fanns skulle det syfte som nämns i föregående punkt i förevarande dom åsidosättas. Vidare skulle den höga skyddsnivå som garanteras av direktiv 95/46 jämfört med stadgan med lätthet kunna kringgå genom att personuppgifter överfördes från unionen till tredjeländer för att behandlas där.
- 74 Av den uttryckliga ordalydelsen i artikel 25.6 i direktiv 95/46 framgår att det är rättsordningen i det tredjeland som avses i kommissionsbeslutet som ska säkerställa en adekvat skyddsnivå. Även om de medel som detta tredjeland använder för att säkerställa en sådan skyddsnivå kan skilja sig från dem som används inom unionen för att säkerställa iakttagandet av de krav som följer av direktiv 95/46 jämfört med stadgan, måste dessa medel dock visa sig i praktiken kunna säkerställa ett skydd som är väsentligen likvärdigt med det skydd som garanteras inom unionen.
- 75 Vid undersökningen av den skyddsnivå som erbjuds av ett tredjeland är kommissionen mot denna bakgrund skyldig att bedöma innehållet i de regler som är tillämpliga i detta land till följd av dess interna lagstiftning eller dess internationella förpliktelser samt praxis vad gäller att säkerställa iakttagandet av dessa regler. I enlighet med artikel 25.2 i direktiv 95/46 ska kommissionen härvidlag beakta alla de förhållanden som har samband med en överföring av personuppgifter till ett tredjeland.
- 76 Mot bakgrund av omständigheterna att den skyddsnivå som säkerställs i ett tredjeland kan komma att förändras, ankommer det dessutom på kommissionen, efter det att den antagit ett beslut med stöd av artikel 25.6 i direktiv 95/46, att regelbundet kontrollera att konstaterandet att det aktuella tredjelandet säkerställer en adekvat skyddsnivå fortfarande är sakligt och rättsligt motiverat. En sådan kontroll krävs under alla förhållanden när det finns uppgifter som ger upphov till tvivel i detta hänseende.
- 77 Såsom generaladvokaten har påpekat i punkterna 134 och 135 i sitt förslag till avgörande ska vid giltighetsprövningen av ett beslut som kommissionen har antagit med stöd av artikel 25.6 i direktiv 95/46 dessutom även omständigheter som har inträffat efter antagandet av detta beslut beaktas.
- 78 Domstolen konstaterar i detta avseende att kommissionens utrymme för skönsmässig bedömning av huruvida den skyddsnivå som säkerställs i ett tredjeland är adekvat är begränsat, med hänsyn till den stora betydelse som skyddet för personuppgifter har för den grundläggande rätten till respekt för privatlivet och med hänsyn till det stora antal personer som riskerar att få sina grundläggande rättigheter kränkta vid en överföring av personuppgifter till ett tredjeland som inte säkerställer en adekvat skyddsnivå. Det ska därför göras en strikt

kontroll av de krav som följer av artikel 25 i direktiv 95/46 jämförd med stadgan (se, analogt, dom Digital Rights Ireland, C-293/12 och C-594/12, EU:C:2014:238, punkterna 47 och 48).

Artikel 1 i beslut 2000/520

- 79 Kommissionen ansåg i artikel 1.1 i beslut 2000/520 att de principer som avses i bilaga I till beslut, tillämpade i enlighet med den vägledning som ges i FoS i bilaga II till beslutet, ska anses säkerställa en adekvat skyddsnivå för personuppgifter som överförs från unionen till organisationer som är etablerade i Förenta staterna. Av detta beslut framgår att såväl principerna som FoS har utfärdats av det amerikanska handelsministeriet.
- 80 Anslutningen av ett företag till *safe harbor*-systemet sker genom ett självcertifieringssystem, såsom framgår av artikel 1.2 och 1.3 i beslutet, jämförd med FoS 6 i bilaga II till beslutet.
- 81 Även om ett tredjelands användning av ett självcertifieringssystem inte i sig strider mot kravet i artikel 25.6 i direktiv 95/46 enligt vilket det aktuella tredjelandet ska säkerställa en adekvat skyddsnivå "genom sin interna lagstiftning eller på grund av de internationella förpliktelser" som åligger detta land, bygger ett sådant systems tillförlitlighet vad gäller nämnda krav i huvudsak på införandet av effektiva spårnings- och kontrollmekanismer som gör det praktiskt möjligt att upptäcka och beivra eventuella överträdelser av de bestämmelser som säkerställer skyddet av de grundläggande rättigheterna, särskilt rätten till respekt för privatlivet och rätten till skydd för personuppgifter.
- 82 I förevarande fall är *safe harbor*-principerna, enligt andra stycket i bilaga I till beslut 2000/520, "endast avsedda att tillämpas på de organisationer i USA som tar emot personuppgifter från EU och syftet är att dessa organisationer skall uppfylla villkoren för *safe harbors* samt den presumtion om 'adekvat skyddsnivå' som därmed skapas". Dessa principer är således uteslutande tillämpliga på självcertifierade amerikanska organisationer som erhåller personuppgifter från unionen, utan att det krävs att amerikanska myndigheter ska iaktta dessa principer.
- 83 Vidare framgår det av artikel 2 i beslut 2000/520 att beslutet "[endast] gäller ... frågan om den skyddsnivå är adekvat som enligt [*safe harbor*-]principerna och FoS erbjuds i Förenta staterna, i förhållande till de krav som ställs i artikel 25.1 i direktiv [95/46]", utan att innehålla tillräckliga konstateranden beträffande de åtgärder genom vilka Amerikas förenta stater säkerställer en adekvat skyddsnivå, i den mening som avses i artikel 25.6 i direktivet, genom sin interna lagstiftning eller på grund av de internationella förpliktelser som åligger landet.
- 84 Till detta kommer att tillämpligheten av nämnda principer, enligt bilaga I fjärde stycket i beslut 2000/520, kan begränsas bland annat "a) till vad som är nödvändigt för att uppfylla krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden" och av "lagar, myndighetsföreskrifter eller rättspraxis som skapar motstridiga skyldigheter eller ger explicita befogenheter, förutsatt att organisationen då den utövar dessa befogenheter kan visa att avvikelserna från principerna begränsar sig till vad som är nödvändigt för att de övergripande legitima intressen som är beroende av dessa befogenheter skall kunna tillgodoseas".
- 85 Vad gäller gränserna för tillämpligheten av *safe harbor*-principerna understryks i bilaga IV B i beslut 2000/520 att "[s]jälvklart måste amerikanska organisationer, om de i amerikansk lag har en motstridig skyldighet, oberoende av om de anslutit sig till *safe harbor* eller inte, följa lagen".
- 86 Således ges enligt beslut 2000/520 "krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden" företräde framför *safe harbor*-principerna. Detta innebär att självcertifierade amerikanska organisationer som erhåller personuppgifter från unionen är skyldiga att utan inskränkningar frångå dessa principer när de står i konflikt med ovannämnda krav, och således visar sig vara oförenliga med kraven.
- 87 Undantaget i bilaga I fjärde stycket i beslut 2000/520 är av generell beskaffenhet och möjliggör således ingrepp – grundade på krav avseende nationell säkerhet, allmänintresset eller intern lagstiftning i Förenta staterna – i de grundläggande rättigheterna för personer vilkas personuppgifter överförs eller kan komma att överföras från unionen till Förenta staterna. För

att fastställa huruvida det föreligger ett ingrepp i den grundläggande rätten till respekt för privatlivet har det härvidlag föga betydelse huruvida de uppgifter som avser privatlivet är av känslig art eller huruvida de berörda har fått utstå eventuella olägenheter på grund av ingreppet (dom Digital Rights Ireland m.fl., C-293/12 och C-594/12, EU:C:2014:238, punkt 33 och där angiven rättspraxis).

- 88 Dessutom innehåller beslut 2000/520 inte något konstaterande beträffande förekomsten i Förenta staterna av regler som antagits av staten och som syftar till att begränsa eventuella ingrepp i de grundläggande rättigheterna för personer vilkas personuppgifter överförs från unionen till Förenta staterna, ingrepp som statliga organ kan vara tillåtna att göra när de görs i ett legitimit syfte, såsom nationell säkerhet.
- 89 Till detta kommer den omständigheten att det i beslut 2000/520 inte anges att det finns något effektivt rättsligt skydd mot denna typ av ingrepp. Såsom generaladvokaten har påpekat i punkterna 204–206 i sitt förslag till avgörande, gäller de privata skiljeförfaranden och förfarandena vid Federal Trade Commission – vars befogenheter, som bland annat beskrivs i FoS 11 i bilaga II till beslutet, är begränsade till kommersiella tvister – amerikanska företags iakttagande av *safe harbor*-principerna, och de kan inte tillämpas i för tvister angående lagenligheten av ingrepp i de grundläggande rättigheterna som uppstår på grund av statliga åtgärder.
- 90 Ovanstående analys av beslut 2000/520 finner dessutom stöd i kommissionens egen bedömning av den situation som uppstått till följd av genomförandet av detta beslut. Det framgår särskilt av punkterna 2 och 3.2 i meddelande COM(2013) 846 final och punkterna 7.1, 7.2 och 8 i meddelande COM(2013) 847 final, vilkas innehåll redovisats i punkterna 13–16, 22, 23 och 25 i förevarande dom, att kommissionen konstaterat att de amerikanska myndigheterna kunde erhålla åtkomst till personuppgifter som överförs från medlemsstaterna till Förenta staterna och behandla dessa uppgifter på ett sätt som är oförenligt med, bland annat, syftena med deras överföring och som går utöver vad som var strängt nödvändigt och proportionerligt för att skydda den nationella säkerheten. Dessutom har kommissionen konstaterat att det för de berörda personerna inte fanns några förvaltningsrättsliga rättsmedel eller rättsmedel inför domstol i syfte att bland annat erhålla tillgång till uppgifter som rör dem, eller i förekommande fall rätta eller radera dessa uppgifter.
- 91 Vad gäller den nivå för skyddet av grundläggande fri- och rättigheter som garanteras inom unionen måste en unionslagstiftning som innebär ett ingrepp i de grundläggande rättigheter som garanteras av artiklarna 7 och 8 i stadgan, enligt domstolens fasta praxis, föreskriva tydliga och precisa bestämmelser som reglerar räckvidden och tillämpligheten av en åtgärd och slår fast minimikrav, så att de personer vilkas personuppgifter berörs har tillräckliga garantier som möjliggör ett effektivt skydd av deras uppgifter mot risker för missbruk och otillåten åtkomst eller användning. Behovet av sådana garantier är av än större betydelse när personuppgifterna är föremål för automatisk behandling och risken för otillåten åtkomst till uppgifterna är stor (dom Digital Rights Ireland m.fl., C-293/12 och C-594/12, EU:C:2014:238, punkterna 54 och 55 och där angiven rättspraxis).
- 92 Vidare, och framför allt, kräver skyddet av den grundläggande rätten till respekt för privatlivet på unionsnivå att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt (dom Digital Rights Ireland m.fl., C-293/12 och C-594/12, EU:C:2014:238, punkt 52 och där angiven rättspraxis).
- 93 En lagstiftning är således inte begränsad till vad som är strängt nödvändigt när den generellt tillåter lagring av samtliga personuppgifter om alla personer vilkas uppgifter har överförts från unionen till Förenta staterna, utan att det görs några åtskillnader, begränsningar eller undantag med beaktande av det eftersträfvade syftet och utan att det föreskrivs något objektivt kriterium som gör det möjligt att avgränsa myndigheternas åtkomst till uppgifterna och att avgränsa deras senare användning till bestämda, strängt begränsade syften som kan motivera det ingrepp som såväl åtkomst som användning av uppgifterna innebär (se, för ett liknande resonemang vad gäller Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG (EUT L 105, s. 54), dom Digital Rights Ireland m.fl., C-293/12 och C-594/12, EU:C:2014:238, punkterna 57–61).

- 94 I synnerhet måste en lagstiftning som tillåter myndigheterna generell åtkomst till innehållet i elektroniska kommunikationer anses kränka det väsentliga innehållet i den grundläggande rätten till respekt för privatlivet, som garanteras i artikel 7 i stadgan (se, för ett liknande resonemang, dom Digital Rights Ireland m.fl., C-293/12 och C-594/12, EU:C:2014:238, punkt 39).
- 95 En lagstiftning i vilken det inte föreskrivs någon möjlighet för enskilda att använda rättsmedel för att erhålla tillgång till, rätta eller radera uppgifter som rör dem, respekterar inte det väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd, vilken är stadfast i artikel 47 i stadgan. I artikel 47 första stycket i stadgan föreskrivs nämligen att var och en vars unionsrättsligt garanterade fri- och rättigheter har kränkts har rätt till ett effektivt rättsmedel inför en domstol, med beaktande av de villkor som föreskrivs i den artikeln. Möjligheten till en effektiv domstolsprövning i syfte att säkerställa iakttagandet av unionsrätten är härvidlag i sig en grundförutsättning för en rättsstat (se, för ett liknande resonemang, dom Les Verts/parlamentet, 294/83, EU:C:1986:166, punkt 23, dom Johnston, 222/84, EU:C:1986:206, punkterna 18 och 19, dom Heylens m.fl., 222/86, EU:C:1987:442, punkt 14, och dom UGT-Rioja m.fl., C-428/06 – C-434/06, EU:C:2008:488, point 80).
- 96 Såsom det har konstaterats i bland annat punkterna 71, 73 och 74 i förevarande dom, krävs det för att kommissionen ska kunna anta ett beslut med stöd av artikel 25.6 i direktiv 95/46 att kommissionen har fastställt och vederbörligen motiverat att det aktuella tredjelandet, genom sin interna lagstiftning eller på grund av de internationella förpliktelser som åligger landet, de facto säkerställer en nivå för skyddet av de grundläggande rättigheterna som är väsentligen likvärdig med den nivå som garanteras i unionens rättsordning, en nivå som särskilt framgår av föregående punkter i förevarande dom.
- 97 Det finns dock anledning att påpeka att kommissionen i beslut 2000/520 inte har angett att Amerikas förenta stater de facto "säkerställer" en adekvat skyddsnivå genom sin interna lagstiftning eller på grund av de internationella förpliktelser som åligger landet.
- 98 Domstolen finner följaktligen, utan att det är nödvändigt att undersöka innehållet i *safe harbor*-principerna, att artikel 1 beslut 2000/520 åsidosatte de krav som slås fast i artikel 25.6 i direktiv 95/46 jämförd med stadgan, och att den därmed är ogiltig.
- Artikel 3 i beslut 2000/520
- 99 Av domstolens överväganden i punkterna 53, 57 och 63 i förevarande dom framgår att vad gäller artikel 28 i direktiv 95/46 särskilt jämförd med artikel 8 i stadgan, måste de nationella tillsynsmyndigheterna kunna göra en fullständig oberoende utredning av varje begäran om skydd för en persons fri- och rättigheter med avseende på behandling av personuppgifter rörande vederbörande. Detta gäller särskilt när denna person i samband med en sådan begäran gör gällande att ett kommissionsbeslut som har antagits med stöd av artikel 25.6 i direktiv 95/46 inte är förenligt med skyddet för privatlivet och enskilda personers grundläggande fri- och rättigheter.
- 100 I artikel 3.1 första stycket i beslut 2000/520 finns emellertid en särskild reglering vad gäller de nationella tillsynsmyndigheternas befogenheter avseende ett konstaterande som kommissionen gjort angående adekvat skyddsnivå i den mening som avses i artikel 25 i direktiv 95/46.
- 101 Enligt denna bestämmelse får de nationella tillsynsmyndigheterna, i enlighet med restriktiva villkor som innebär en hög tröskel för ingripande, "[u]tan att det påverkar de befogenheter behöriga myndigheter i medlemsstaterna har att vidta åtgärder för att säkra efterlevnaden av nationella bestämmelser som antagits enligt andra bestämmelser i direktiv [95/46] än artikel 25, ... tillfälligt förbjuda överföringen av uppgifter till en organisation som ... förbundit sig att följa principerna [i beslut 2000/520]". Även om denna bestämmelse inte påverkar de nationella tillsynsmyndigheternas befogenheter att vidta åtgärder för att säkra efterlevnaden av nationella bestämmelser som antagits enligt detta direktiv, utesluter den däremot möjligheten för dessa myndigheter att vidta åtgärder för att säkra efterlevnaden av artikel 25 i direktivet.

- 102 Artikel 3.1 första stycket i beslut 2000/520 ska således förstås så, att den berövar de nationella tillsynsmyndigheterna de befogenheter de har i enlighet med artikel 28 i direktiv 95/46, när en person i samband med en begäran i enlighet med denna bestämmelse anför omständigheter som innebär att det kan ifrågasättas huruvida ett beslut i vilket kommissionen med stöd av artikel 25.6 i direktivet konstaterat att ett tredjeland säkerställer en adekvat skyddsnivå, är förenligt med skyddet för privatlivet och enskilda personers grundläggande fri- och rättigheter.
- 103 De genomförandebefogenheter som unionslagstiftaren gett kommissionen i artikel 25.6 i direktiv 95/46 ger emellertid inte denna institution befogenheten att inskränka de befogenheter för de nationella tillsynsmyndigheterna som det hänvisats till i föregående punkt i förevarande dom.
- 104 Mot denna bakgrund konstaterar domstolen att kommissionen genom att anta artikel 3 i beslut 2000/520 överskridit den befogenhet som kommissionen tilldelas i artikel 25.6 i direktiv 95/46 jämförd med stadgan, och att denna artikel därmed är ogiltig.
- 105 Eftersom artiklarna 1 och 3 i beslut 2000/520 inte kan avskiljas från artiklarna 2 och 4 i beslutet, eller från bilagorna till beslutet, påverkar ogiltigheten av artiklarna 1 och 3 giltigheten för beslutet i dess helhet.
- 106 Mot bakgrund av det ovan anförda finner domstolen att beslut 2000/520 är ogiltigt.

Rättegångskostnader

- 107 Eftersom förfarandet i förhållande till parterna i det nationella målet utgör ett led i beredningen av samma mål, ankommer det på den hänskjutande domstolen att besluta om rättegångskostnaderna. De kostnader för att avge yttrande till domstolen som andra än nämnda parter har haft är inte ersättningsgilla.

Mot denna bakgrund beslutar domstolen (stora avdelningen) följande:

- 1) **Artikel 25.6 i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, i dess lydelse enligt Europaparlamentets och rådets förordning (EG) nr 1882/2003 av den 29 september 2003, jämförd med artiklarna 7, 8 och 47 i Europeiska unionens stadga om de grundläggande rättigheterna, ska tolkas så, att ett beslut som har antagits med stöd av denna bestämmelse, såsom kommissionens beslut 2000/520/EG av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (*Safe Harbor Privacy Principles*) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat, genom vilket Europeiska kommissionen konstaterar att ett tredjeland säkerställer en adekvat skyddsnivå, inte utgör hinder för att en medlemsstats tillsynsmyndighet, i den mening som avses i artikel 28 i direktivet, i dess ändrade lydelse, prövar en persons begäran om skydd för sina fri- och rättigheter med avseende på behandling av personuppgifter rörande vederbörande, vilka har överförts från en medlemsstat till detta tredjeland, när denna person gör gällande att detta tredjelands rätt och praxis inte säkerställer en adekvat skyddsnivå.**
- 2) **Beslut 2000/520 är ogiltigt.**

Underskrifter

