Kohtulahendite kogumik

EUROOPA KOHTU OTSUS (suurkoda)

6. oktoober 2015*

Eelotsusetaotlus — Isikuandmed — Füüsiliste isikute kaitse seoses nende andmete töötlemisega — Euroopa Liidu põhiõiguste harta — Artiklid 7, 8 ja 47 — Direktiiv 95/46/EÜ — Artiklid 25 ja 28 — Isikuandmete edastamine kolmandatesse riikidesse — Otsus 2000/520/EÜ — Isikuandmete edastamine Ameerika Ühendriikidesse — Kaitse ebapiisav tase — Kehtivus — Sellise füüsilise isiku kaebus, kelle andmed edastati Euroopa Liidust Ameerika Ühendriikidesse — Liikmesriigi järelevalveasutuste volitused

Kohtuasjas C-362/14,

mille ese on ELTL artikli 267 alusel High Courti (Iirimaa) 17. juuli 2014. aasta otsusega esitatud eelotsusetaotlus, mis saabus Euroopa Kohtusse 25. juulil 2014, menetluses

Maximillian Schrems

versus

Data Protection Commissioner,

menetluses osales:

Digital Rights Ireland Ltd,

EUROOPA KOHUS (suurkoda),

koosseisus: president V. Skouris, asepresident K. Lenaerts, kodade presidendid A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (ettekandja), S. Rodin ja K. Jürimäe, kohtunikud A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. Šváby, M. Berger, F. Biltgen ja C. Lycourgos,

kohtujurist: Y. Bot,

kohtusekretär: vanemametnik L. Hewlett,

arvestades kirjalikus menetluses ja 24. märtsi 2015. aasta kohtuistungil esitatut,

arvestades seisukohti, mille esitasid:

— M. Schrems, esindajad: N. Travers, *SC*, P. O'Shea, *BL*, *solicitor* G. Rudden ja *Rechtsanwalt* H. Hofmann,

— Data Protection Commissioner, esindajad: P. McDermott, *BL*, *solicitor* S. More O'Ferrall ja *solicitor* D. Young,

* Kohtumenetluse keel: inglise.

— Digital Rights Ireland Ltd, esindajad: F. Crehan, *BL*, *solicitor* S. McGarr ja *solicitor* E. McGarr,

— Iirimaa, esindajad: A. Joyce, B. Counihan ja E. Creedon, keda abistas D. Fennelly, *BL*,

— Belgia valitsus, esindajad: J.-C. Halleux ja C. Pochet,

— Tšehhi valitsus, esindajad: M. Smolek ja J. Vláčil,

— Itaalia valitsus, esindaja: G. Palmieri, keda abistas *avvocato dello Stato* P. Gentili,

— Austria valitsus, esindajad: G. Hesse ja G. Kunnert,

— Poola valitsus, esindajad: M. Kamejsza, M. Pawlicka ja B. Majczyna,

— Sloveenia valitsus, esindajad: A. Grum ja V. Klemenc,

— Ühendkuningriigi valitsus, esindajad: L. Christie ja J. Beeko, keda abistas *barrister* J. Holmes,

— Euroopa Parlament, esindajad: D. Moore, A. Caiola ja M. Pencheva,

— Euroopa Komisjon, esindajad: B. Schima, B. Martenczuk, B. Smulders ja J. Vondung,

— Euroopa Andmekaitseinspektor, esindajad: C. Docksey, A. Buchta ja V. Pérez Asinari,

olles 23. septembri 2015. aasta kohtuistungil ära kuulanud kohtujuristi ettepaneku,

on teinud järgmise

otsuse

1 Eelotsusetaotlus käsitleb seda, kuidas Euroopa Liidu põhiõiguste harta (edaspidi „harta”) artikleid 7, 8 ja 47 arvestades tõlgendada Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivi 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EÜT L 281, lk 31; ELT eriväljaanne 13/15, lk 355) (muudetud Euroopa Parlamendi ja nõukogu 29. septembri 2003. aasta määrusega (EÜ) nr 1882/2003 (ELT L 284, lk 1; edaspidi „direktiiv 95/46”)) artikli 25 lõiget 6 ja artiklit 28, ning sisuliselt ka seda, kas on kehtiv komisjoni 26. juuli 2000. aasta otsus 2000/520/EÜ vastavalt direktiivile 95/46 piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium (EÜT L 215, lk 7; ELT eriväljaanne 16/01, lk 119).

2 Taotlus on esitatud M. Schremsi ja Data Protection Commissioneri (edaspidi „andmekaitsevolinik”) vahelises vaidluses, mis käsitleb viimase keeldumist menetleda kaebust, mille M. Schrems esitas seetõttu, et Facebook Ireland Ltd (edaspidi „Facebook Ireland”) edastab oma kasutajate isikuandmed Ameerika Ühendriikidesse ja säilitab neid selles riigis asuvates serverites.

Õiguslik raamistik

Direktiiv 95/46

3 Direktiivi 95/46 põhjendused 2, 10, 56, 57, 60, 62 ja 63 on sõnastatud järgmiselt:

„(2) andmetöötlussüsteemid on loodud selleks, et teenida inimkonda; selliseid süsteeme kasutades tuleb füüsiliste isikute kodakondsusele ja elukohale vaatamata austada nende põhiõigusi ja -vabadusi, eelkõige õigust eraelu puutumatusele, ning aidata kaasa […] üksikisikute heaolule;

[…]

(10) isikuandmete töötlemist käsitlevate õigusaktide eesmärk on kaitsta [4. novembril 1950 Roomas allakirjutatud] Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 8 ja ühenduse õiguse üldistes põhimõtetes tunnustatud põhiõigusi ja -vabadusi, eelkõige õigust eraelu puutumatusele; nimetatud põhjusel ei tohi kõnealuste õigusaktide ühtlustamise tagajärjel nendega pakutav kaitse väheneda, vaid vastupidi – ühenduses tagatava kaitstuse tase peab olema kõrgem;

[…]

(56) isikuandmete liikumine üle piiride on vajalik rahvusvahelise kaubanduse laiendamiseks; ühenduses käesoleva direktiiviga tagatud üksikisikute kaitse ei takista isikuandmete edastamist kolmandatesse riikidesse, kus on tagatud nende kaitse piisav tase; andmete kaitse taset kolmandates riikides tuleb hinnata kõiki edastamistoimingu või edastamistoimingute kogumi asjaolusid silmas pidades;

(57) samas tuleb keelata isikuandmete edastamine kolmandatesse riikidesse, kus nende kaitse tase ei ole piisav;

[…]

(60) igal juhul võib andmete edastamine kolmandatesse riikidesse toimuda ainult siis, kui täielikult järgitakse sätteid, mis liikmesriigid on vastu võtnud käesoleva direktiivi ja eelkõige selle artikli 8 põhjal;

[…]

(62) liikmesriikides täiesti sõltumatult oma tööülesandeid täitvate järelevalveasutuste loomine on oluline tegur üksikisikute kaitsmisel seoses isikuandmete töötlemisega;

(63) sellistel asutustel peavad olema oma kohustuste täitmiseks vajalikud vahendid, sealhulgas volitused tegeleda uurimisega ja sekkuda, seda eelkõige üksikisikute esitatud kaebuste puhul, ja volitused osaleda kohtumenetlustes; […]”.

4 Direktiivi 95/46 artiklites 1, 2, 25, 26, 28 ja 31 on sätestatud:

„Artikkel 1

Direktiivi eesmärk

1. Vastavalt käesolevale direktiivile kaitsevad liikmesriigid isikuandmete töötlemisel füüsiliste isikute põhiõigusi ja -vabadusi ning eelkõige nende õigust eraelu puutumatusele.

[…]

Artikkel 2

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

a) *isikuandmed* – igasugune teave tuvastatud või tuvastatava füüsilise isiku (edaspidi „andmesubjekt”) kohta. Tuvastatav isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige isikukoodi põhjal või ühe või mitme tema füüsilisele, füsioloogilisele, vaimsele, majanduslikule, kultuurilisele või sotsiaalsele identsusele omase joone põhjal;

b) *isikuandmete töötlemine* (edaspidi „töötlemine”) – iga isikuandmetega tehtav toiming või toimingute kogum, olenemata sellest, kas see on automatiseeritud või mitte, näiteks kogumine, salvestamine, korrastamine, säilitamine, kohandamine või muutmine, väljavõtete tegemine, päringu teostamine, kasutamine, üleandmine, levitamine või muul moel avaldamine, ühitamine või ühendamine, sulgemine, kustutamine või hävitamine;

[…]

d) *vastutav töötleja* – füüsiline või juriidiline isik, riigiasutus, esindused või mõni muu organ, kes määrab üksi või koos teistega kindlaks isikuandmete töötlemise eesmärgid ja vahendid; kui töötlemise eesmärgid ja vahendid on kindlaks määratud siseriiklike või ühenduse õigusnormidega, võib vastutava töötleja või tema ametissemääramise sätestada siseriiklikus või ühenduse õiguses;

[…]

Artikkel 25

Põhimõtted

1. Liikmesriigid sätestavad, et töödeldavate või pärast edastamist töötlemiseks kavandatud isikuandmete edastamine kolmandatesse riikidesse võib toimuda ainult juhul, kui kõnealune kolmas riik tagab andmekaitse piisava taseme, kui käesoleva direktiivi muude sätete kohaselt vastuvõetud siseriiklikest sätetest ei tulene teisiti.

2. Andmekaitse taset kolmandates riikides hinnatakse, pidades silmas kõiki andmete edastamise toimingute või andmete edastamise toimingute kogumi asjaolusid; tähelepanu pööratakse eelkõige andmete laadile, kavandatud töötlemistoimingu või töötlemistoimingute eesmärgile ja kestusele, päritoluriigile ja lõppsihtriigile, kõnealuses kolmandas riigis kehtivatele nii üldistele kui ka konkreetse sektori õigusnormidele ja kõnealuses riigis järgitavatele ametieeskirjadele ja turvameetmetele.

3. Liikmesriigid ja komisjon teatavad üksteisele juhtudest, mille puhul nad leiavad, et kolmas riik ei taga kaitse piisavat taset lõike 2 tähenduses.

4. Kui komisjon artikli 31 lõikes 2 ette nähtud korras leiab, et kolmas riik ei taga kaitse piisavat taset käesoleva artikli lõike 2 tähenduses, võtavad liikmesriigid vajalikke meetmeid tagamaks, et sama liiki andmeid kõnealusesse kolmandasse riiki ei edastata.

5. Sobival ajal alustab komisjon läbirääkimisi, et parandada olukorda, mis tekkis lõike 4 kohaselt tehtud avastuse tõttu.

6. Komisjon võib leida artikli 31 lõikes 2 sätestatud korras, et kolmas riik tagab kaitse piisava taseme käesoleva artikli lõike 2 tähenduses oma siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega, mis tulenevad eelkõige lõikes 5 osutatud läbirääkimistest, et kaitsta eraelu puutumatust ja üksikisikute põhivabadusi ja -õigusi.

Liikmesriigid võtavad komisjoni otsuse järgimiseks vajalikke meetmeid.

Artikkel 26

Erandid

1. Erandina artiklist 25, ja kui konkreetsete juhtude suhtes ei ole siseriiklike õigusaktidega ette nähtud teisiti, sätestavad liikmesriigid, et isikuandmete edastamine või edastamiste kogum kolmandasse riiki, mis ei taga piisavat kaitset artikli 25 lõike 2 tähenduses, võib toimuda tingimusel, et:

a) andmesubjekt on andmete kavandatud edastamiseks andnud oma ühemõttelise nõusoleku või

b) edastamine on vajalik andmesubjekti ja vastutava töötleja vahelise lepingu täitmiseks või andmesubjekti taotlusel võetud lepingueelsete meetmete rakendamiseks või

c) edastamine on vajalik andmesubjekti huvides vastutava töötleja ja kolmanda isiku vahel sõlmitud lepingu sõlmimiseks või täitmiseks või

d) edastamine on vajalik või seaduste kohaselt nõutav üldiste huvidega seotud olulistel põhjustel või õigusnõuete koostamiseks, esitamiseks või kaitsmiseks või

e) edastamine on vajalik andmesubjekti eluliste huvide kaitsmiseks või

f) edastatavad andmed on pärit registrist, mis õigusnormide kohaselt on mõeldud avalikkuse teavitamiseks ja on tutvumiseks avatud laiemale avalikkusele või kõigile õigustatud huvidega isikutele, kuivõrd konkreetsel juhul täidetakse tingimusi, mis õigusaktidega on tutvumiseks ette nähtud.

2. Ilma et see piiraks lõike 1 kohaldamist, võivad liikmesriigid lubada isikuandmete edastamist või edastamistoimingute kogumit kolmandasse riiki, mis ei taga kaitse piisavat taset artikli 25 lõike 2 tähenduses, kui vastutav töötleja esitab piisavad tagatised üksikisikute eraelu puutumatuse ning põhiõiguste ja -vabaduste kaitse ja vastavate õiguste kasutamise kohta; sellised tagatised võivad tuleneda eelkõige asjakohastest lepingutingimustest.

3. Liikmesriik informeerib komisjoni ja teisi liikmesriike lõike 2 kohaselt antud lubadest.

Kui liikmesriik või komisjon esitab põhjendatud vastuväiteid, milles viidatakse üksikisikute eraelu puutumatusele või põhiõigustele ja -vabadustele, võtab komisjon vajalikud meetmed artikli 31 lõikes 2 sätestatud korras.

Liikmesriigid võtavad komisjoni otsuse järgimiseks vajalikke meetmeid.

[…]

Artikkel 28

Järelevalveasutus

1. Iga liikmesriik näeb ette ühe või mitu riigiasutust, et teostada järelevalvet tema territooriumil käesoleva direktiivi kohaselt vastuvõetud sätete kohaldamise üle.

Kõnealused asutused tegutsevad neile usaldatud ülesannete täitmisel täiesti sõltumatult.

2. Iga liikmesriik näeb ette, et selliste haldusmeetmete võtmisel või õigusaktide koostamise käigus, mis käsitlevad üksikisikute õiguste ja vabaduste kaitset isikuandmete töötlemisel, konsulteeritakse järelevalveasutustega.

3. Igal sellisel ametiasutusel on eelkõige:

— uurimisvolitused, näiteks volitused tutvuda töödeldavate andmetega ja koguda oma järelevalvekohustuse täitmiseks vajalikku teavet,

— tõhusad sekkumisvolitused, näiteks avaldada artikli 20 kohaselt arvamust enne töötlemise alustamist ja tagada sellise arvamuse asjakohane avalikustamine, anda korraldus andmete sulgemiseks, kustutamiseks või hävitamiseks, keelata töötlemine ajutiselt või alaliselt, hoiatada vastutavat töötlejat või teha talle märkus või suunata küsimus liikmesriigi parlamenti või teistesse poliitilisse institutsioonidesse,

— volitused osaleda kohtumenetlustes, kui käesoleva direktiivi kohaselt vastuvõetud siseriiklikke sätteid on rikutud, või juhtida kõnealustele rikkumistele õigusasutuste tähelepanu.

Kui järelevalveasutuse otsustega ei olda rahul, võib need edasi kaevata kohtusse.

4. Iga järelevalveasutus vaatab läbi kõigi isikute või kõnealuseid isikuid esindava ühenduse esitatud avaldused nende õiguste ja vabaduste kaitse kohta seoses isikuandmete töötlemisega. Andmesubjektile teatatakse avalduse tagajärgedest.

Iga järelevalveasutus vaatab läbi eelkõige kõigi isikute avaldused kontrollida andmete töötlemise seaduslikkust, kui kohaldatakse käesoleva direktiivi artikli 13 kohaselt vastuvõetud siseriiklikke sätteid. Igal juhul teatatakse isikule kontrollimisest.

[…]

6. Olenemata sellest, milliseid siseriiklikke õigusi kõnealuse töötlemise suhtes kohaldatakse, on iga järelevalveasutus pädev kasutama oma liikmesriigi territooriumil talle lõikega 3 antud volitusi. Teise liikmesriigi asutused võivad igalt järelevalveasutuselt taotleda, et see kasutaks oma volitusi.

[…]

Artikkel 31

[…]

2. Kui viidatakse käesolevale artiklile, kohaldatakse [nõukogu 28. juuni 1999. aasta] otsuse 1999/468/EÜ[, millega kehtestatakse komisjoni rakendusvolituste kasutamise menetlused (EÜT L 184, lk 23; ELT eriväljaanne 01/03, lk 124)] artikleid 4 ja 7, võttes arvesse selle artikli 8 sätteid.

[…]”.

Otsus 2000/520

5 Otsuse 2000/520 on komisjon vastu võtnud direktiivi 95/46 artikli 25 lõike 6 alusel.

6 Otsuse põhjendused 2, 5 ja 8 on sõnastatud järgmiselt:

„(2) Komisjon võib jõuda järeldusele, et kolmas riik tagab kaitse piisava taseme. Sel juhul võib liikmesriikidest isikuandmeid edastada ilma lisatagatisteta.

[…]

(5) Käesoleva otsusega tunnustatav piisav kaitse andmete edastamiseks ühendusest Ameerika Ühendriikidesse peaks olema saavutatud, kui organisatsioonid järgivad liikmesriigist Ameerika Ühendriikidesse edastatavate isikuandmete kaitsel programmi Safe Harbor põhimõtteid (edaspidi „põhimõtted") ja korduma kippuvaid küsimusi (edaspidi „KKK"), milles sätestatakse juhised Ameerika Ühendriikide valitsuse poolt 21. juulil 2000. aastal välja antud põhimõtete rakendamiseks. Lisaks sellele tuleks organisatsioonidel avalikustada oma eraelu puutumatuse kaitse normid ning tunnustada Federal Trade Commission'i (FTC) pädevust seaduse Federal Trade Commission Act paragrahvi 5 raames, milles keelustatakse ärilised ja äritegevust mõjutavad kõlvatud tavad või pettus, või mõne muu täitevasutuse pädevust, mis tõhusalt tagab KKKga kooskõlas rakendatud põhimõtete järgimise.

[…]

(8) Selguse ja arusaadavuse huvides ning võimaldamaks liikmesriikide pädevatel ametiasutustel tagada üksikisikute kaitset neid puudutavate isikuandmete töötlemisel, tuleb käesolevas otsuses kindlaks määrata need erandlikud asjaolud, mille korral konkreetsete andmevoogude peatamine oleks põhjendatud olenemata sellest, et andmete kaitsetase on tunnistatud piisavaks."

7 Otsuse 2000/520 artiklites 1–4 on ette nähtud:

„Artikkel 1

1. Direktiivi 95/46/EÜ artikli 25 lõike 2 tähenduses tagavad programmi Safe Harbor põhimõtted (edaspidi „põhimõtted") käesoleva otsuse I lisas sätestatud kujul, rakendatuna kooskõlas Ameerika Ühendriikide kaubandusministeeriumi poolt 21. juulil 2000. aastal välja antud korduma kippuvate küsimustega (edaspidi „KKK") käesoleva otsuse II lisas sätestatud kujul, kõikide selle direktiivi reguleerimisalasse jäävate tegevuste suhtes piisava kaitse taseme ühendusest Ameerika Ühendriikides asuvatele organisatsioonidele edastatavatele isikuandmetele, võttes arvesse järgmisi Ameerika Ühendriikide kaubandusministeeriumi poolt välja antud dokumente:

a) III lisas toodud ülevaade programmi Safe Harbor täitmise tagamisest;

b) IV lisas toodud memorandum kahjutasu kohta eraelu puutumatuse rikkumise eest ja Ameerika Ühendriikide seadustes sätestatud otsestest volitustest;

c) V lisas toodud kiri Federal Trade Commission'ilt;

d) VI lisas toodud kiri Ameerika Ühendriikide transpordiministeeriumilt.

2. Iga andmete edastuse puhul peavad olema täidetud järgmised tingimused:

a) andmeid vastuvõttev organisatsioon on ühemõtteliselt ja avalikult teatavaks teinud, et kohustub järgima KKKdega kooskõlas rakendatavaid põhimõtteid; ja

b) organisatsioon allub käesoleva otsuse VII lisas toodud Ameerika Ühendriikide valitsusasutuse kohta seaduses sätestatud õigusele uurida kaebusi KKKdega kooskõlas rakendatavatele põhimõtetele mittevastavuste korral ja taotleda abi kõlvatute tavade või pettuse vastu ning hüvitust üksikisikutele olenemata nende elukohariigist või kodakondsusest.

3. Lõikes 2 sätestatud tingimused on täitnud iga organisatsioon, mis kinnitab, et järgib KKKdega kooskõlas rakendatud põhimõtteid alates kuupäevast, mil organisatsioon ise teatab Ameerika Ühendriikide kaubandusministeeriumile (või selle poolt määratule), et on lõike 2 punktis a nimetatud kohustuse avalikustanud ning lõike 2 punktis b nimetatud valitsusasutuse nime.

Artikkel 2

Käesolev otsus puudutab ainult KKKdega kooskõlas rakendatud põhimõtetega tagatud kaitse taseme piisavust Ameerika Ühendriikides vastavalt direktiivi 95/46/EÜ artikli 25 lõike 1 nõuetele ning ei mõjuta muude selles direktiivis isikuandmete töötlemist liikmesriikides käsitlevate sätete rakendamist, eriti selle artiklit 4.

Artikkel 3

1. Ilma et see piiraks liikmesriikide pädevate ametiasutuste volitusi võtta meetmeid selliste siseriiklike sätete järgimise tagamiseks, mis on vastu võetud muude sätete alusel peale direktiivi 95/46/EÜ artikli 25, võivad need ametiasutused järgmistel juhtudel kasutada oma volitusi ka andmete edastamise peatamiseks organisatsioonile, mis on ise kohustunud järgima KKKdega kooskõlas rakendatud põhimõtteid, et tagada üksikisikute kaitse seoses nende isikuandmete töötlemisega:

a) käesoleva otsuse VII lisas osutatud Ameerika Ühendriikide valitsusasutus või sõltumatu kaebuste käsitlemise mehhanism käesoleva otsuse I lisas sätestatud täitmise tagamise põhimõtte punkti a tähenduses on otsustanud, et organisatsioon rikub KKKdega kooskõlas rakendatud põhimõtteid; või

b) on väga tõenäoline, et põhimõtteid rikutakse; on põhjust arvata, et asjakohane täitmise tagamise mehhanism ei rakenda piisavaid ja õigeaegseid meetmeid kõnealuse olukorra lahendamiseks; edastamise jätkamisel tekiks raske kahju otsene oht andmesubjektidele; ning liikmesriigi pädevad asutused on teinud selles olukorras mõistlikke pingutusi organisatsiooni teavitamiseks ja andnud võimaluse vastata.

Peatamine lakkab niipea, kui on tagatud vastavus KKKdega kooskõlas rakendatud põhimõtetele ja ühenduse asjakohaseid pädevaid asutusi on sellest teavitatud.

2. Liikmesriigid teatavad lõike 1 alusel võetud meetmetest viivitamata komisjonile.

3. Liikmesriigid ja komisjon teatavad üksteisele ka juhtudest, mil Ameerika Ühendriikides kooskõlas KKKdega rakendatud põhimõtete järgimise tagamise eest vastutavad asutused ei suuda oma tegevuse kaudu nõuete järgimist tagada.

4. Kui lõigete 1, 2 ja 3 alusel kogutud teave annab tunnistust sellest, et Ameerika Ühendriikides kooskõlas KKKdega rakendatud põhimõtete järgimise tagamise eest vastutav asutus ei täida oma rolli tõhusalt, teavitab komisjon Ameerika Ühendriikide kaubandusministeeriumi ja vajaduse korral esitab meetmete eelnõud kooskõlas direktiivi 95/46/EÜ artiklis 31 osutatud korraga käesoleva otsuse tühistamiseks või peatamiseks või selle reguleerimissala piiramiseks.

Artikkel 4

1. Käesolevat otsust võib muuta igal ajal vastavalt selle rakendamise kogemusele ja/või kui Ameerika Ühendriikide õigusaktid jõuavad põhimõtete ja KKKdega tagatud kaitse taseme tagamiseni. Kolm aastat pärast käesoleva otsuse teatavakstegemist liikmesriikidele hindab komisjon kättesaadava teabe alusel igal juhul selle rakendamist ning esitab direktiivi 95/46/EÜ artikli 31 alusel moodustatud komiteele aruande kõigi asjakohaste järelduste kohta, sealhulgas tõendid, mis võivad mõjutada järeldust, et käesoleva otsuse artikli 1 sätetega pakutav kaitse on direktiivi 95/46/EÜ artikli 25 tähenduses piisav, ning tõendid selle kohta, et käesolevat otsust rakendatakse diskrimineerival viisil.

2. Komisjon esitab vajaduse korral meetmete eelnõud direktiivi 95/46/EÜ artiklis 31 sätestatud korras."

8 Otsuse 2000/520 I lisa on sõnastatud järgmiselt:

„Programmi Safe Harbor põhimõtted välja antud Ameerika Ühendriikide kaubandusministeeriumi poolt 21. juulil 2000 […] Ameerika Ühendriikide kaubandusministeerium [annab] välja käesoleva dokumendi ning korduma kippuvad küsimused (põhimõtted) oma seadusest tulenevate volituste piires, et aidata kaasa rahvusvahelisele kaubandusele, seda edendada ja arendada. Põhimõtted töötati välja koostöös tootjate ja üldsusega äri- ja kaubandustegevuse lihtsustamiseks Ameerika Ühendriikide ja Euroopa Liidu vahel. Nad on mõeldud kasutamiseks ainult isikuandmeid Euroopa Liidust vastu võtvate Ameerika Ühendriikide organisatsioonide poolt, et saavutada vastavus programmi Safe Harbor põhimõtetega ja seeläbi saavutada eeldatav „piisav" andmekaitse. Kuna põhimõtted on kavandatud üksnes sellel konkreetsel eesmärgil, ei pruugi nad sobida muul otstarbel kohaldamiseks. […] Organisatsioonide otsused järgida programmiga Safe Harbor ühinemiseks nõutavaid tingimusi on täiesti vabatahtlikud ja organisatsioonid võivad programmi Safe Harbor põhimõtteid järgida mitmel erineval moel. […] Nende põhimõtete järgimist võib piirata: a) riikliku julgeoleku, avaliku huvi või õiguskaitseliste vajaduste täitmiseks vajalikus ulatuses; b) statuudi, valitsuse määruse või pretsedendiõigusega, mis loovad vasturääkivaid kohustusi või annavad otseseid volitusi, tingimusel et selliste volituste kasutamisel suudab organisatsioon demonstreerida, et põhimõtete mittejärgimine tema poolt piirdub ulatusega, mis on vajalik selliste volitustega seotud ülekaaluka õigustatud huvi järgimiseks; või c) kui direktiiv või liikmesriigi seadus lubab erandeid ja kõrvalekaldeid, tingimusel et selliseid erandeid või kõrvalekaldeid rakendatakse võrreldavates tingimustes. Vastavalt eraelu puutumatuse kaitse suurendamise eesmärgile peaksid organisatsioonid püüdma neid põhimõtteid täielikult ja läbipaistvalt rakendada, sealhulgas sätestama oma eraelu puutumatuse normides, kui eespool toodud punkti b erandeid rakendatakse regulaarselt. Samal põhjusel eeldatakse, et kui on võimalik teha valik põhimõtete ja/või Ameerika Ühendriikide seaduste alusel, valivad organisatsioonid võimalusel kõrgema kaitse taseme. […]".

9 Otsuse 2000/520 II lisa on sõnastatud järgmiselt:

„Korduma kippuvad küsimused (KKK)

[…] KKK 6 – Kinnitamine

K: *Kuidas saab organisatsioon ise kinnitada, et järgib programmi Safe Harbor põhimõtteid?*

V: Programmi Safe Harbor soodustused tagatakse alates kuupäevast, mil organisatsioon ise kinnitab Ameerika Ühendriikide kaubandusministeeriumile (või selle poolt määratule) põhimõtete järgimist kooskõlas allpool esitatud juhtnööridega.

Programmi Safe Harbor osas kinnituse andmiseks võivad organisatsioonid esitada Ameerika Ühendriikide kaubandusministeeriumile (või selle poolt määratule) kirja, millele on alla kirjutanud vastutav isik programmiga Safe Harbor ühineva organisatsiooni nimel ning mis sisaldab vähemalt järgmist teavet:

1) organisatsiooni nimi, postiaadress, e-posti aadress, telefoni- ja faksinumbrid;

2) organisatsiooni tegevuse kirjeldus EList saadavate isikuandmetega seoses; ja

3) organisatsiooni puutumatusnormide kirjeldus selliste isikuandmete puhul, sealhulgas: a) kus on avalikkusel võimalik selliste puutumatusnormidega tutvuda, b) nende juurutamise kuupäev, c) kontaktandmed kaebuste, juurdepääsunõuete ning muude programmi Safe Harbor alusel tekkivate küsimuste käsitluseks; d) konkreetne täitevasutus, millel on pädevus läbi vaadata mis tahes nõudeid organisatsiooni vastu seoses võimalike kõlvatute tavade või pettusega ja puutumatusele kohaldatavate (ning põhimõtete lisas loetletud) seaduste või normide rikkumisega, e) kõikide puutumatusprogrammide nimed, mille liige organisatsioon on, f) kontrolli viis (nt sisemine, kolmas osapool), […] ja g) sõltumatu kaebuste käsitlemise mehhanism, mida saab kasutada lahendamata kaebuste uurimiseks.

Organisatsioon, mis soovib oma programmi Safe Harbor soodustusi laiendada EList töösuhte kontekstis edastatavatele töötajate isikuandmetele, võib seda teha sellise täitevasutuse olemasolul, millel on pädevus võtta vastu töötajate isikuandmetest tulenevaid nõudeid, mis on loetletud põhimõtete lisas. […]

Ministeerium (või selle poolt määratu) peab nimekirja kõikidest sellise kirja esitanud organisatsioonidest, tagades seeläbi programmi Safe Harbor soodustuste kättesaadavuse, ning uuendab seda nimekirja iga-aastaste kirjade ja teadete alusel, mida ta KKK 11 alusel vastu võtab. […]

[…] KKK 11 – Vaidluste lahendamine ja täitmise tagamine

K: *Kuidas tuleks rakendada täitmise tagamise põhimõtte vaidluste lahendamise nõudeid ja kuidas käsitletakse põhimõtete püsivat rikkumist organisatsiooni poolt?*

V: Täitmise tagamise põhimõttes sätestatakse nõuded programmi Safe Harbor täitmise tagamiseks. Põhimõtte punkti b nõuete täitmine on sätestatud kontrolli käsitlevas KKKs (KKK 7). KKK 11 käsitleb punkte a ja c, mis mõlemad nõuavad sõltumatut kaebuste käsitlemise mehhanismi. Need mehhanismid võivad võtta erineva vormi, kuid peavad vastama täitmise tagamise põhimõtte nõuetele. Organisatsioonid võivad saavutada nõuetega vastavuse järgmiselt: 1) nad järgivad erasektori poolt välja töötatud eraelu puutumatuse programme, mis toovad oma reeglitesse sisse programmi Safe Harbor põhimõtted ja mis hõlmavad täitmise tagamise põhimõttes kirjeldatud liiki tõhusaid täitmise tagamise mehhanisme; 2) nad järgivad üksikisikute kaebuste käsitlemise ja vaidluste lahendamisega tegelevate järelevalveasutuste juhiseid; või 3) nad kohustuvad tegema koostööd Euroopa Liidus asuvate andmekaitseasutustega või nende volitatud esindajatega. See loend on illustratiivne ja mittetäielik. Erasektor võib välja töötada muid täitmise tagamise mehhanisme, kui need vastavad täitmise tagamise põhimõtte ja KKKde nõuetele. Tähele tuleb panna, et täitmise tagamise põhimõtted lisanduvad põhimõtete sissejuhatuse lõikes 3 sätestatud nõuetele selle kohta, et iseregulatsioonipüüdlused peavad olema jõustatavad seaduse Federal Trade Commission Act artikli 5 või sarnase statuudi alusel.

Kaebuste käsitlemise mehhanismid

Tarbijaid tuleb julgustada esitama mis tahes kaebusi osjaomasele organisatsioonile enne siirdumist sõltumatute kaebuste käsitlemise mehhanismide juurde. […]

[…]

FTC meetmed

FTC on kohustunud prioriteetsel alusel läbi vaatama eraelu puutumatuse iseregulatsiooniorganisatsioonide, näiteks BBBOnline and TRUSTe, ja EL liikmesriikide esildised väidetavatest mittevastavustest programmi Safe Harbor põhimõtetele, et otsustada, kas on rikutud seaduse FTC Act paragrahvi 5, mis keelustab kõlvatud tavad ja pettuse äritegevuses. […] […]".

10 Otsuse 2000/520 IV lisas on ette nähtud:

„Kahjutasu eraelu puutumatuse rikkumise eest, õiguslikud volitused ning ühinemised ja ülevõtmised Ameerika Ühendriikide seaduses

Käesolev selgitus on vastuseks Euroopa Komisjoni taotlusele anda selgitusi Ameerika Ühendriikide seaduses a) eraelu puutumatuse rikkumisega seotud kahjutasu nõuete kohta, b) Ameerika Ühendriikide seaduses esitatud „otseste volituste" kohta isikuandmete kasutamiseks viisil, mis ei ole kooskõlas programmi Safe Harbor põhimõtetega, ja c) ühinemiste ja ülevõtmiste mõju kohta programmi Safe Harbor põhimõtete alusel võetud kohustustele.

[…]

B. Otsesed õiguslikud volitused Programmi Safe Harbor põhimõtted sisaldavad erandit, kui statuut, normid või pretsedendiõigus loovad või annavad „vastandlikke kohustusi või otseseid volitusi, tingimusel et mis tahes sellise volituse teostamisel suudab organisatsioon demonstreerida, et tema mittevastavus põhimõtetele on piiratud ainult sellega, mis on vajalik selliste volitustega talle pandud ülekaalukate õigustatud huvide täitmiseks." Selge on, et kui Ameerika Ühendriikide seadustes sätestatakse vastandlik kohustus, peavad Ameerika Ühendriikide organisatsioonid, sõltumata sellest, kas nad osalevad programmis Safe Harbor või mitte, seadust täitma. Mis puutub otsestesse volitustesse, siis kui programmi Safe Harbor põhimõtete eesmärgiks on ületada erinevusi Ameerika Ühendriikide ja Euroopa eraelu puutumatuse kaitse viiside vahel, peame meie austama meie valitud seadusandjate seadusandlikke prerogatiive. Rangele programmi Safe Harbor põhimõtetele vastavusele piiratud erandi tegemise eesmärgiks on tasakaalu leidmine mõlema osapoole õigustatud huvide vahel. Erand tehakse ainult otseste volituste korral. Minimaalseks eelduseks seega on, et asjakohane statuut, norm või kohtuotsus peab programmi Safe Harbor organisatsioonidele sellist tegevust kindlalt lubama. Teiste sõnadega ei kehti erand seal, kus seadus vaikib. Lisaks kehtiks erand ainult siis, kui see otsene luba satub vastuollu programmi Safe Harbor põhimõtete järgimisega. Isegi siis on erand „kehtiv ulatuses, mis on vajalik sellise loaga talle pandud ülekaalukate õigustatud huvide täitmiseks". Näiteks kui seadus lihtsalt lubab äriühingul riigiasutustele andmeid esitada, siis kõnesolev erand ei kehti. Kui aga seadus vastupidi konkreetselt lubab äriühingul esitada isikuandmeid riigiasutustele ilma üksikisiku nõusolekuta, kujutaks see endast „otsest volitust" tegutseda viisil, mis on vastuolus programmi Safe Harbor põhimõtetega. Alternatiivselt jääksid konkreetsed erandid seoses kindla nõudega teade ja nõusoleku kohta erandi raamesse (kuna võrduksid eriloaga avalikustada teave ilma teate ja kooskõlastuseta). Näiteks statuut, mis annab arstidele loa esitada patsientide meditsiinilisi andmeid tervishoiuametnikele ilma patsientide eelneva nõusolekuta, võiks lubada erandit teate ja valikuvõimaluse põhimõtetest. Kõnesolev luba ei annaks arstile õigust esitada kõnesolevaid meditsiinilisi andmeid tervishoiuorganisatsioonidele ega kommertsalustel tegutsevatele farmaatsialaboritele, mis jääksid seadusega lubatud eesmärkidest ja seega erandi reguleerimisalast välja

[…]. Kõnesolevad õiguslikud load võivad endast kujutada ühekordset luba isikuandmete konkreetseks kasutamiseks, kuid nagu allpool toodud näidetest selgub, on tõenäoliselt tegemist mõne laiema isikuandmete kogumist, kasutamist või avalikustamist keelava seaduse erandiga. […]".

Teatis COM(2013) 846 final

11 Komisjon võttis 27. novembril 2013 vastu teatise Euroopa Parlamendile ja nõukogule „Usalduse taastamine ELi ja Ameerika Ühendriikide vaheliste andmevoogude vastu" (COM(2013) 846 final; edaspidi „teatis COM(2013) 846 final"). Teatise juurde kuulus samuti 27. novembrist 2013 pärinev aruanne, mis sisaldas „Euroopa Liidu ja Ameerika Ühendriikide ajutise andmekaitse töörühma Euroopa Liidu kaasesimeeste järeldusi" („Report on the Findings by the EU Co-chairs of the *ad hoc* EU-US Working Group on Data Protection"). Nagu nähtub aruande punktist 1, koostati see koostöös Ameerika Ühendriikidega seetõttu, et ilmnes, et kõnealuses riigis on mitu jälgimisprogrammi, mis hõlmavad laiaulatuslikku isikuandmete kogumist ja töötlemist. Aruanne sisaldas muu hulgas Ameerika Ühendriikide õiguskorra üksikasjalikku analüüsi eelkõige seoses õigusliku alusega, mis lubab jälgimisprogrammidel eksisteerida ning Ameerika Ühendriikide ametiasutustel isikuandmeid koguda ja töödelda.

12 Teatise COM(2013) 846 final punktis 1 täpsustas komisjon, et „[k]aubandussuhetega seotud andmevahetust käsitletakse otsuses [2000/520]", lisades, et „[o]tsuses on sätestatud õiguslik alus isikuandmete edastamiseks EList Ameerika Ühendriikides asuvatele äriühingutele, kes järgivad programmi Safe Harbor põhimõtteid". Lisaks rõhutas komisjon punktis 1 isikuandmete voo üha tähtsamaks muutumist seoses eelkõige digitaalmajanduse arenguga, kuivõrd see on nimelt „viinud andmetöötlusega seotud toimingute arvu hüppelise kasvuni ning on paranenud nende kvaliteet, suurenenud erinevate toimingute hulk ja tehingud muutunud oma iseloomult mitmekesisemaks".

13 Teatise punktis 2 juhib komisjon tähelepanu sellele, et „[s]uurenenud on […] mure programmi Safe Harbor raames Ameerika Ühendriikidele edastatud [liidu] kodanike isikuandmete kaitsetaseme pärast" ja et „[p]rogrammi vabatahtliku ja deklaratiivse iseloomu tõttu keskendutakse põhjalikumalt selle läbipaistvusele ja nõuete järgimisele".

14 Lisaks märkis komisjon punktis 2, et „[p]rogrammi Safe Harbor raames Ameerika Ühendriikidele saadetavatele [liidu] kodanike isikuandmetele on juurdepääs Ameerika Ühendriikide ametiasutustel, kes võivad kõnealuseid andmeid töödelda ka viisil, mis ei vasta põhjustele, miks andmed [liidus] algselt koguti, ega eesmärkidele, miks need USA-le edastati", ning et „[e]namik Ameerika Ühendriikide internetiühenduse pakkujaid, keda [jälgimis]programmid otsesemalt puudutavad, on programmi Safe Harbor raames sertifitseeritud".

15 Teatise COM(2013) 846 final punktis 3.2 tõi komisjon esile teatud hulga kitsaskohti seoses otsuse 2000/520 rakendamisega. Ta viitas esiteks sellele, et Ameerika sertifitseeritud ettevõtjad ei järgi otsuse 2000/520 artikli 1 lõikes 1 nimetatud põhimõtteid (edaspidi „Safe Harbor' põhimõtted") ja et selles otsuses tuleks teha muudatusi, mis kõrvaldaksid „läbipaistvuse ja normide täitmise tagamisega seotud struktuursed probleemid, tugevdama programmi keskseid põhimõtteid ning olema suunatud riikliku julgeolekuga seotud erandi kohaldamisele". Teiseks juhtis ta tähelepanu sellele, et „[p]rogramm Safe Harbor on ühtlasi kanaliks, mille kaudu edastatakse [liidu] kodanike isikuandmeid [liidust] Ameerika Ühendriikidele äriühingute poolt, kes peavad Ameerika Ühendriikide luureandmete kogumise programmide raames edastama andmeid USA luureteenistustele".

16 Komisjon järeldas punktis 3.2, et „[p]idades silmas kindlaks tehtud puudusi, ei ole programmi Safe Harbor kohaldamist praegusel kujul võimalik jätkata[, kuid selle] tühistamisel oleks siiski kahjustav mõju programmis osalevate [liidu] ja Ameerika Ühendriikide äriühingute huvidele". Komisjon lisas lõpuks punktis 3.2, et ta „alustab Ameerika Ühendriikide ametiasutustega kiiresti koostööd, et arutada kindlaks tehtud kitsaskohti".

Teatis COM(2013) 847 final

17 Samal kuupäeval ehk 27. novembril 2013 võttis komisjon vastu Euroopa Parlamendile ja nõukogule teatise, mis käsitleb programmi Safe Harbor toimimist ELi kodanike ja ELis asutatud äriühingute seisukohast (COM(2013) 847 final; edaspidi „teatis COM(2013) 847 final"). Nagu nähtub teatise punktist 1, põhines see eelkõige Euroopa Liidu ja Ameerika Ühendriikide *ad hoc* töörühma saadud teabel ning järgnes kahele komisjoni hindamisaruandele, mis avaldati vastavalt 2002. ja 2004. aastal.

18 Teatise punktis 1 on täpsustatud, et otsuse 2000/520 toimimine „toetub sellega liitunud äriühingute võetud kohustustele ja nende vastavale kinnitusele", ning lisatud, et „[l]iitumine on vabatahtlik, kuid eeskirjad on liitunute jaoks siduvad".

19 Lisaks nähtub teatise COM(2013) 847 final punktist 2.2, et 26. septembri 2013. aasta seisuga on kinnituse andnud 3246 ettevõtjat, kes kuuluvad paljudesse majandusharudesse ja teenustesektoritesse. Need ettevõtjad osutavad teenuseid peamiselt liidu siseturul, eriti internetisektoris, ja osa neist on liidu ettevõtjad, kellel on Ameerika Ühendriikides tütarettevõtjad. Osa neist ettevõtjatest töötleb oma Euroopas töötavate töötajate andmeid, mis edastatakse Ameerika Ühendriikidesse personalijuhtimise eesmärgil.

20 Punktis 2.2 rõhutas komisjon samuti, et „[j]uhul kui USA poolel esineb mis tahes probleeme läbipaistvuse või täitmise kontrollimisega seoses, liigub vastutus selle tulemusena Euroopa andmekaitseasutustele ning programmi kasutavatele äriühingutele".

21 Teatise COM(2013) 847 final punktidest 3–5 ja 8 ilmneb muu hulgas, et suur hulk kinnituse andnud ettevõtjaid tegelikult ei järgi Safe Harbor' põhimõtteid või järgivad neid ainult osaliselt.

22 Lisaks tõi komisjon teatise punktis 7 esile, et „tundub, et kõik programmis PRISM [teabe laiaulatusliku kogumise programm] osalevad äriühingud, kes annavad USA ametiasutustele juurdepääsu salvestatud ja töödeldud andmetele, on programmi Safe Harbor raames kinnituse andnud", ning et programm Safe Harbor on seega muutunud „ühe[ks] kanali[ks], mille kaudu antakse USA luureasutustele juurdepääs algselt [liidus] töödeldud isikuandmete kogumisele". Sellega seoses tõdes komisjon teatise punktis 7.1, et „USA õiguse raames mitme õigusliku aluse olemasolu [võimaldab] USAs asuvate äriühingute poolt salvestatud või muul moel töödeldud isikuandmete ulatuslikku kogumist ja töötlemist" ja et „[k]õnealuste programmide ulatuslikkuse tulemusena võib programmi Safe Harbor raames edastatud andmetele tekkida juurdepääs USA ametiasutustel, kes saavad neid andmeid ka töödelda ulatuses, mis on suurem kui otseselt vajalik ja proportsionaalne […] otsuses [2000/520] sätestatud erandiga ette nähtud riikliku julgeoleku kaitsmise eesmärgil".

23 Teatise COM(2013) 847 final punktis 7.2 „Piirangud ja õiguskaitsevahendid" rõhutas komisjon, et „USA õigusega ette nähtud kaitsemeetmed [on] kättesaadavad peamiselt USA kodanikele või seaduslikele residentidele" ja et „[l]isaks sellele puudub nii [liidu] kui ka USA andmesubjektidel võimalus saada andmetele juurdepääsu, teha neisse parandusi või neid kustutada või kasutada halduslikke või kohtulikke õiguskaitsevahendeid seoses nende isikuandmete kogumise või töötlemisega, mis leiab aset USA jälgimisprogrammide raames".

24 Teatise COM(2013) 847 final punkti 8 kohaselt kuuluvad kinnituse andnud ettevõtjate hulka „veebifirmad[…] nagu Google, Facebook, Microsoft, Apple ja Yahoo", kellel on „Euroopas sadu miljoneid kliente" ja kes edastavad isikuandmeid nende töötlemiseks Ameerika Ühendriikidesse.

25 Komisjon järeldas punktis 8, et „luureagentuuride ulatuslik juurdepääs programmi Safe Harbor raames kinnituse andnud äriühingute poolt USAsse edastatud andmetele [tekitab] täiendavaid tõsiseid küsimusi seoses eurooplaste andmekaitseõiguste järjepidevusega nende andmete edastamisel USAsse".

Põhikohtuasi ja eelotsuse küsimused

26 Austrias elav Austria kodanik M. Schrems on sotsiaalvõrgustiku Facebook (edaspidi „Facebook”) kasutaja alates 2008. aastast.

27 Kõik liidu territooriumil elavad isikud, kes soovivad Facebooki kasutada, on kohustatud enda registreerimisel sõlmima lepingu Facebook Irelandiga, kes on Ameerika Ühendriikides asuva Facebook Inc. tütarettevõtja. Liidu territooriumil elavate Facebook Irelandi kasutajate isikuandmed edastatakse kas täielikult või osaliselt Facebook Inc. serveritesse, mis asuvad Ameerika Ühendriikide territooriumil, ja neid töödeldakse seal.

28 M. Schrems esitas 25. juunil 2013 andmekaitsevolinikule kaebuse, milles ta sisuliselt palus, et viimane oma seadusjärgset pädevust teostades keelaks Facebook Irelandil tema isikuandmeid Ameerika Ühendriikidesse edastada. Ta väitis, et selles riigis kehtiv õigus ja valitsev praktika ei taga selle territooriumil säilitatavate isikuandmete piisavat kaitset ametiasutustepoolse jälgimise eest. M. Schrems viitas sellega seoses Edward Snowdeni paljastustele Ameerika Ühendriikide luureteenistuste ja täpsemalt National Security Agency (edaspidi „NSA”) tegevuse kohta.

29 Andmekaitsevolinik leidis, et ta ei ole kohustatud uurima asjaolusid, mis M. Schrems oma kaebuses esile tõi, ja jättis kaebuse läbi vaatamata, kuna tema hinnangul oli see alusetu. Ta asus seisukohale, et puuduvad tõendid selle kohta, et NSA oleks tutvunud huvitatud isiku isikuandmetega. Andmekaitsevolinik lisas, et M. Schremsi kaebuses esitatud väited ei saa anda tulemust, kuna kõik Ameerika Ühendriikides isikuandmete kaitse piisavat taset puudutavad küsimused tuleb lahendada kooskõlas otsusega 2000/520 ja selles otsuses on komisjon tõdenud, et Ameerika Ühendriigid tagavad kaitse piisava taseme.

30 M. Schrems esitas põhikohtuasjas kõne all oleva otsuse peale High Courtile (kõrgeim kohus) kaebuse. Olles põhikohtuasja poolte esitatud tõendeid analüüsinud, tuvastas kohus, et liidust Ameerika Ühendriikidesse edastatud isikuandmete elektrooniline jälgimine ja infopüük teenib avalikes huvides vajalikke ja möödapääsmatuid eesmärke. Kohus lisas siiski, et E. Snowdeni paljastused annavad tunnistust sellest, et NSA ja teised föderaalasutused on oma pädevust „märkimisväärselt ületanud”.

31 Sama kohtu hinnangul ei ole liidu kodanikel mingit tegelikku õigust olla ära kuulatud. Järelevalvet luureteenistuste tegevuse üle teostatakse salastatud menetluses, mis ei ole võistlev. Kui isikuandmed on kord Ameerika Ühendriikidesse edastatud, võivad NSA ja ka teised föderaalasutused, nagu Federal Bureau of Investigation (FBI), nendega tutvuda valimatu ulatusliku jälgimise ning pealtkuulamise või -vaatamise käigus.

32 High Court tõdes, et Iiri õigus keelab isikuandmete edastamise väljapoole Iirimaad, välja arvatud juhul, kui asjassepuutuv kolmas riik tagab eraelu ning põhiõiguste ja -vabaduste kaitse piisava taseme. Iiri põhiseadusega tagatud õiguse eraelu ja eluaseme puutumatusele olulisus nõuab, et mis tahes sekkumine neisse õigustesse oleks proportsionaalne ja vastaks seaduses ette nähtud nõuetele.

33 Massiline ja valimatu isikuandmetega tutvumine on aga proportsionaalsuse põhimõtte ja Iiri põhiseadusega kaitstavate põhiväärtustega ilmselgelt vastuolus. Selleks et elektroonilise side pealtkuulamist või -vaatamist võiks pidada põhiseadusega kooskõlas olevaks, tuleks tõendada, et pealtkuulamine või -vaatamine on konkreetne, et teatud isikute või isikurühmade jälgimine on riikliku julgeoleku või kuritegevuse tõkestamise huvides objektiivselt põhjendatud ning et sellega kaasnevad piisavad ja kontrollitavad tagatised. Seega leiab High Court, et kui põhikohtuasja peaks lahendama ainult Iiri õiguse alusel, tuleks asuda seisukohale, et arvestades tõsiseid kahtlusi selles, kas Ameerika Ühendriigid tagavad isikuandmete kaitse piisava taseme, oleks andmekaitsevolinik pidanud M. Schremsi kaebuses esile toodud asjaolusid uurima, ning et ta jättis kaebuse ekslikult läbi vaatamata.

34 High Court leiab siiski, et kõnealune juhtum puudutab liidu õiguse kohaldamist harta artikli 51 tähenduses, mistõttu tuleb põhikohtuasjas käsitletava otsuse õiguspärasust hinnata lähtuvalt liidu õigusest. Nimetatud kohtu hinnangul ei vasta otsus 2000/520 aga ei harta artiklitest 7 ja 8 ega ka Euroopa Kohtu poolt kohtuotsuses Digital Rights Ireland jt (C-293/12 ja C-594/12, EU:C:2014:238) esile toodud põhimõtetest tulenevatele nõuetele. Harta artikliga 7 ja liikmesriikide traditsioonide ühiste põhiväärtustega tagatud õigus eraelu puutumatusele muutuks mõttetuks, kui ametiasutustel oleks lubatud tutvuda elektroonilise side teel edastatud teabega suvaliselt ja üldiselt, ilma et neil oleks selleks vaja objektiivset põhjust, mis põhineks riikliku julgeoleku kaalutlustel või konkreetsete isikutega seotud kuritegevuse ennetamise vajaduse korral, ning ilma et sellise tegevusega kaasneksid piisavad ja kontrollitavad tagatised.

35 High Court märgib lisaks, et M. Schrems vaidlustab oma kaebuses tegelikult otsusega 2000/520 kehtestatud programmi Safe Harbor õiguspärasuse, kuivõrd põhikohtuasjas käsitletav otsus lähtub sellest korrast. Seega, kuigi M. Schrems ei ole direktiivi 95/46 ega otsuse 2000/520 kehtivust formaalselt vaidlustanud, tekib nimetatud kohtu sõnul küsimus, kas tulenevalt direktiivi artikli 25 lõikest 6 oli andmekaitsevolinik seotud otsuses komisjoni tehtud järeldusega, mille kohaselt Ameerika Ühendriikides on tagatud kaitse piisav tase, või kas harta artikkel 8 lubab andmekaitsevolinikul sellest järeldusest vajaduse korral kõrvale kalduda.

36 Neil asjaoludel otsustas eelotsusetaotluse esitanud kohus menetluse peatada ja esitada Euroopa Kohtule järgmised eelotsuse küsimused:

„1. Kas harta artikleid 7, 8 ja 47 arvesse võttes ja ilma, et see piiraks direktiivi 95/46 artikli 25 lõike 6 kohaldamist, on andmekaitsealaste õigusnormide kohaldamise pädevusega sõltumatu andmekaitsevolinik, kes menetleb kaebust seoses isikuandmete edastamisega kolmandasse riiki (käesoleval juhul Ameerika Ühendriikidesse), milles kehtiv õigus ja valitsev praktika kaebuse esitaja väitel ei taga asjaomasele isikule piisavat kaitset, absoluutselt kohustatud järgima liidu vastupidist järeldust, mis sisaldub otsuses 2000/520?

2. Kas vastupidisel juhul võib või peab andmekaitsevolinik oma uurimises võtma arvesse pärast komisjoni otsuse esmakordset avaldamist toimunud faktilist arengut?”

Eelotsuse küsimuste analüüs

37 Oma eelotsuse küsimustega, mida tuleb analüüsida koos, palub eelotsusetaotluse esitanud kohus sisuliselt selgitada, kas ja millises ulatuses tuleb direktiivi 95/46 artikli 25 lõiget 6 koostoimes harta artiklitega 7, 8 ja 47 tõlgendada nii, et selle sätte alusel vastu võetud otsus, nagu seda on otsus 2000/520, milles komisjon on tuvastanud, et kolmandas riigis on tagatud kaitse piisav tase, takistab liikmesriigi järelevalveasutust direktiivi artikli 28 tähenduses läbi vaatamast isiku avaldust, mis puudutab tema õiguste ja vabaduste kaitset seoses tema selliste isikuandmete töötlemisega, mis on liikmesriigist edastatud sellesse kolmandasse riiki, kui kõnealune isik väidab, et selles riigis kehtiv õigus ja valitsev praktika ei taga kaitse piisavat taset.

Direktiivi 95/46 artikli 28 tähenduses liikmesriigi järelevalveasutuste pädevus, kui komisjon on direktiivi artikli 25 lõike 6 alusel otsuse vastu võtnud

38 Sissejuhatuseks olgu meenutatud, et kuivõrd direktiivi 95/46 sätted reguleerivad isikuandmete töötlemist, mis võib riivata põhivabadusi ja eriti õigust eraelu puutumatusele, tuleb nende tõlgendamisel tingimata lähtuda hartaga tagatud põhiõigustest (vt kohtuotsused Österreichischer Rundfunk jt, C-465/00, C-138/01 ja C-139/01, EU:C:2003:294, punkt 68; Google Spain ja Google, C-131/12, EU:C:2014:317, punkt 68, ning Ryneš, C-212/13, EU:C:2014:2428, punkt 29).

39 Direktiivi 95/46 artiklist 1 ning põhjendustest 2 ja 10 nähtub, et direktiivi eesmärk on tagada mitte ainult füüsiliste isikute põhiõiguste ja -vabaduste ning eelkõige nende õiguse eraelu puutumatusele tõhus ja täielik kaitse isikuandmete töötlemisel, vaid ka põhiõiguste ja -vabaduste kaitse kõrge tase. Seda, et nii harta artikliga 7 tagatud põhiõigus eraelu puutumatusele kui ka artikliga 8 tagatud põhiõigus isikuandmete kaitsele on olulised, on lisaks rõhutatud ka Euroopa Kohtu praktikas (vt kohtuotsused Rijkeboer, C-553/07, EU:C:2009:293, punkt 47; Digital Rights Ireland jt, C-293/12 ja C-594/12, EU:C:2014:238, punkt 53, ning Google Spain ja Google, C-131/12, EU:C:2014:317, punktid 53, 66 ja 74 ning seal viidatud kohtupraktika).

40 Mis puudutab liikmesriigi järelevalveasutuste pädevust seoses isikuandmete edastamisega kolmandatesse riikidesse, siis tuleb märkida, et direktiivi 95/46 artikli 28 lõikega 1 on liikmesriikidele pandud kohustus asutada üks või mitu ametiasutust, kes täiesti sõltumatult kontrollivad füüsiliste isikute kaitset reguleerivate liidu õigusnormide järgimist isikuandmete töötlemisel. See nõue tuleneb ka liidu esmasest õigusest, eelkõige harta artikli 8 lõikest 3 ja ELTL artikli 16 lõikest 2 (vt selle kohta kohtuotsused komisjon *vs.* Austria, C-614/10, EU:C:2012:631, punkt 36, ja komisjon *vs.* Ungari, C-288/12, EU:C:2014:237, punkt 47).

41 Liikmesriigi järelevalveasutuste sõltumatuse tagatise eesmärk on tagada isikuandmete töötlemisel füüsiliste isikute kaitset reguleerivate sätete järgimise üle teostatava kontrolli tõhusus ja usaldusväärsus ning seda tuleb tõlgendada nimetatud eesmärki arvestades. See tagatis kehtestati eesmärgiga tugevdada kaitset, mida pakutakse isikutele ja asutustele, keda järelevalveasutuste otsused puudutavad. Sõltumatute järelevalveasutuste asutamine liikmesriikides on seega oluline tegur üksikisikute kaitsmisel seoses isikuandmete töötlemisega, nagu on märgitud direktiivi 95/46 põhjenduses 62 (vt kohtuotsused komisjon *vs.* Saksamaa, C-518/07, EU:C:2010:125, punkt 25 ning komisjon *vs.* Ungari, C-288/12, EU:C:2014:237, punkt 48 ja seal viidatud kohtupraktika).

42 Kaitse tagamiseks peavad liikmesriigi järelevalveasutused eelkõige hoolitsema selle eest, et oleksid tasakaalus ühelt poolt eraelu puutumatuse kui põhiõiguse austamine ja teiselt poolt huvid, mida teenib isikuandmete vaba liikumine (vt selle kohta kohtuotsused komisjon *vs.* Saksamaa, C-518/07, EU:C:2010:125, punkt 24, ja selle kohta komisjon *vs.* Ungari, C-288/12, EU:C:2014:237, punkt 51).

43 Selleks on järelevalveasutustel lai valik volitusi, mis on direktiivi 95/46 artikli 28 lõikes 3 loetletud mitteammendavalt ja mis on nende kohustuste täitmiseks vajalikud vahendid, nagu on rõhutatud direktiivi põhjenduses 63. Nii on nendel asutustel muu hulgas uurimisvolitused, mille hulka kuulub õigus koguda oma järelevalvekohustuse täitmiseks vajalikku teavet, tõhusad sekkumisvolitused, mille hulka kuulub õigus keelata andmete töötlemine ajutiselt või alaliselt, ning volitused osaleda kohtumenetlustes.

44 Direktiivi 95/46 artikli 28 lõigetest 1 ja 6 nähtub, et liikmesriigi järelevalveasutuste pädevus puudutab isikuandmete töötlemist, mis toimub asutuse asukoha liikmesriigi territooriumil, mistõttu puudub neil artikli 28 kohaselt pädevus isikuandmete töötlemise suhtes, mis leiab aset mõne kolmanda riigi territooriumil.

45 Toiming, mis seisneb isikuandmete edastamises liikmesriigist kolmandasse riiki, on iseenesest siiski käsitatav direktiivi 95/46 artikli 2 punkti b tähenduses isikuandmete töötlemisena (vt selle kohta kohtuotsus parlament *vs.* nõukogu ja komisjon, C-317/04 ja C-318/04, EU:C:2006:346, punkt 56), mis toimub liikmesriigi territooriumil. Selles sättes on „isikuandmete töötlemine" nimelt määratletud kui „iga isikuandmetega tehtav toiming või toimingute kogum, olenemata sellest, kas see on automatiseeritud või mitte" ning näitena on toodud „üleandmine, levitamine või muul moel avaldamine".

46 Direktiivi 95/46 põhjenduses 60 on täpsustatud, et isikuandmete edastamine kolmandatesse riikidesse võib toimuda ainult siis, kui täielikult järgitakse sätteid, mis liikmesriigid on vastu võtnud direktiivi alusel. Sellega seoses on direktiivi IV peatükiga, milles sisalduvad artiklid 25 ja 26, kehtestatud kord,

mille eesmärk on tagada isikuandmete kolmandatesse riikidesse edastamise kontrollimine liikmesriikide poolt. See kord täiendab direktiivi II peatükiga kehtestatud üldist korda, milles on ette nähtud isikuandmete töötlemise seaduslikkuse üldised tingimused (vt selle kohta kohtuotsus Lindqvist, C-101/01, EU:C:2003:596, punkt 63).

47 Kuna harta artikli 8 lõike 3 ja direktiivi 95/46 artikli 28 kohaselt on liikmesriigi järelevalveasutuste ülesanne kontrollida füüsiliste isikute kaitset reguleerivate liidu õigusnormide järgimist isikuandmete töötlemisel, on igal sellisel asutusel seega pädevus kindlaks teha, kas isikuandmete edastamine asutuse asukoha liikmesriigist kolmandasse riiki vastab direktiiviga 95/46 kehtestatud nõuetele.

48 Kuigi direktiivi 95/46 põhjenduses 56 on tunnistatud, et isikuandmete edastamine liikmesriikidest kolmandatesse riikidesse on vajalik rahvusvahelise kaubanduse laiendamiseks, on artikli 25 lõikes 1 ette nähtud põhimõte, et edastamine võib toimuda ainult juhul, kui kolmas riik tagab andmekaitse piisava taseme.

49 Lisaks on direktiivi põhjenduses 57 täpsustatud, et isikuandmete edastamine liikmesriikidest kolmandatesse riikidesse, kus kaitse tase ei ole piisav, peab olema keelatud.

50 Selleks et kontrollida isikuandmete edastamist kolmandatesse riikidesse vastavalt andmekaitse tasemele igas sellises riigis, on direktiivi 95/46 artikliga 25 kehtestatud liikmesriikidele ja komisjonile hulk kohustusi. Sellest artiklist nähtub muu hulgas, et seda, kas kolmas riik pakub kaitse piisavat taset või mitte, võib tuvastada nii liikmesriik kui ka komisjon, nagu märkis kohtujurist oma ettepaneku punktis 86.

51 Komisjon võib direktiivi 95/46 artikli 25 lõike 6 alusel vastu võtta otsuse, milles ta tuvastab, et kolmas riik tagab kaitse piisava taseme. Sellise otsuse adressaadid on vastavalt selle artikli teisele lõigule liikmesriigid, kes peavad võtma otsuse järgimiseks vajalikud meetmed. ELTL artikli 288 neljanda lõigu kohaselt on see otsus kõikidele adressaatideks olevatele liikmesriikidele ja seega ka kõikidele nende organitele siduv (vt selle kohta kohtuotsused Albako Margarinefabrik, 249/85, EU:C:1987:245, punkt 17, ja Mediaset, C-69/13, EU:C:2014:71, punkt 23), niivõrd kuivõrd sellega antakse luba edastada isikuandmeid liikmesriikidest otsuses nimetatud kolmandasse riiki.

52 Seega seni, kuni Euroopa Kohus ei ole komisjoni otsust kehtetuks tunnistanud, ei tohi liikmesriigid ja nende organid, sealhulgas sõltumatud järelevalveasutused, tõepoolest võtta selle otsusega vastuolus olevaid meetmeid, nagu akte, milles siduvalt tuvastatakse, et otsuses nimetatud kolmas riik ei taga kaitse piisavat taset. Üldjuhul nimelt eeldatakse liidu institutsioonide aktide õiguspärasust ja need tekitavad seega õiguslikke tagajärgi seni, kuni neid ei ole tagasi võetud, tühistamishagi menetlemise tulemusena tühistatud ega eelotsusemenetluse tulemusel või õigusvastasuse väite alusel kehtetuks tunnistatud (kohtuotsus komisjon *vs.* Kreeka, C-475/01, EU:C:2004:585, punkt 18 ja seal viidatud kohtupraktika).

53 Direktiivi 95/46 artikli 25 lõike 6 alusel komisjoni tehtud otsus, nagu otsus 2000/520, ei saa siiski takistada isikutel, kelle isikuandmed on edastatud või võidakse edastada kolmandasse riiki, pöörduda liikmesriigi järelevalveasutuste poole direktiivi artikli 28 lõikes 4 ette nähtud avaldusega oma õiguste ja vabaduste kaitse kohta seoses isikuandmete töötlemisega. Samamoodi ei saa selline otsus – nagu kohtujurist eelkõige oma ettepaneku punktides 61, 93 ja 116 märkis – välistada ega ka vähendada liikmesriigi järelevalveasutustele harta artikli 8 lõikega 3 ja direktiivi artikliga 28 sõnaselgelt antud volitusi.

54 Ei harta artikli 8 lõikega 3 ega direktiivi 95/46 artikliga 28 ei ole liikmesriigi järelevalveasutuste pädevusvaldkonnast välja jäetud kontrolli isikuandmete edastamise üle kolmandatesse riikidesse, kelle suhtes on komisjon direktiivi artikli 25 lõike 6 alusel otsuse vastu võtnud.

55 Täpsemalt ei ole direktiivi 95/46 artikli 28 lõike 4 esimeses lõigus, milles on sätestatud, et liikmesriigi järelevalveasutustele võib esitada „kõigi isikute […] avaldused nende õiguste ja vabaduste kaitse kohta seoses isikuandmete töötlemisega", ette nähtud ühtegi erandit juhuks, kui komisjon on direktiivi artikli 25 lõike 6 alusel otsuse vastu võtnud.

56 Lisaks oleks see vastuolus direktiivis 95/46 ette nähtud süsteemiga ning artiklite 25 ja 28 eesmärgiga, kui direktiivi artikli 25 lõike 6 alusel komisjoni tehtud otsus takistaks liikmesriigi järelevalveasutusel läbi vaadata isiku avaldust tema õiguste ja vabaduste kaitse kohta seoses selliste isikuandmete töötlemisega, mis on edastatud või võidakse edastada liikmesriigist otsuses nimetatud kolmandasse riiki.

57 Vastupidi, direktiivi 95/46 artikkel 28 on oma laadilt kohaldatav isikuandmete mis tahes töötlemisele. Seega, isegi direktiivi artikli 25 lõike 6 alusel komisjoni tehtud otsuse korral peab liikmesriigi järelevalveasutustel, kellele isik on esitanud avalduse oma õiguste ja vabaduste kaitse kohta seoses tema isikuandmete töötlemisega, olema võimalik täiesti sõltumatult analüüsida, kas nende andmete edastamine vastab direktiiviga kehtestatud nõuetele.

58 Kui see oleks teisiti, jäetaks isikud, kelle isikuandmed on edastatud või võidakse edastada asjaomasesse kolmandasse riiki, ilma harta artikli 8 lõigetega 1 ja 3 tagatud õigusest esitada liikmesriigi järelevalveasutusele avaldus oma põhiõiguste kaitse kohta (vt analoogia alusel kohtuotsus Digital Rights Ireland jt, C-293/12 ja C-594/12, EU:C:2014:238, punkt 68).

59 Direktiivi 95/46 artikli 28 lõike 4 tähenduses avaldust, milles isik, kelle isikuandmed on edastatud või võidakse edastada kolmandasse riiki, väidab – nagu põhikohtuasjas –, et asjaomases riigis kehtiv õigus ja valitsev praktika ei taga kaitse piisavat taset hoolimata sellest, mida on komisjon järeldanud direktiivi artikli 25 lõike 6 alusel vastu võetud otsuses, tuleb mõista nii, et see puudutab sisuliselt kõnealuse otsuse kooskõla üksikisikute eraelu ning põhiõiguste ja -vabaduste kaitsega.

60 Sellega seoses tuleb meelde tuletada Euroopa Kohtu väljakujunenud praktikat, mille kohaselt liit on õigusel rajanev liit, milles kontrollitakse selle institutsioonide aktide kooskõla eelkõige aluslepingutega, õiguse üldpõhimõtetega ja põhiõigustega (vt selle kohta kohtuotsused komisjon jt *vs*. Kadi, C-584/10 P, C-593/10 P ja C-595/10 P, EU:C:2013:518, punkt 66; Inuit Tapiriit Kanatami jt *vs*. parlament ja nõukogu, C-583/11 P, EU:C:2013:625, punkt 91, ning Telefónica *vs*. komisjon, C-274/12 P, EU:C:2013:852, punkt 56). Direktiivi 95/46 artikli 25 lõike 6 alusel komisjoni tehtud otsused ei saa seega niisuguse kontrolli alt välja jääda.

61 Samas on Euroopa Kohtul ainsana pädevus tunnistada kehtetuks liidu õigusakt, nagu direktiivi 95/46 artikli 25 lõike 6 alusel komisjoni tehtud otsus, kusjuures sellise ainupädevuse eesmärk on tagada õiguskindlus seeläbi, et hoolitsetakse liidu õiguse ühetaolise kohaldamise eest (vt kohtuotsused Melki ja Abdeli, C-188/10 ja C-189/10, EU:C:2010:363, punkt 54, ning CIVAD, C-533/10, EU:C:2012:347, punkt 40).

62 Kuigi siseriiklikel kohtutel on küll õigus analüüsida sellise liidu õigusakti kehtivust, nagu direktiivi 95/46 artikli 25 lõike 6 alusel komisjoni tehtud otsus, puudub neil siiski pädevus seda õigusakti ise kehtetuks tunnistada (vt selle kohta kohtuotsused Foto-Frost, 314/85, EU:C:1987:452, punktid 15–20, ning IATA ja ELFAA, C-344/04, EU:C:2006:10, punkt 27). Seda enam, kui liikmesriigi järelevalveasutus vaatab läbi direktiivi artikli 28 lõike 4 tähenduses avaldust, mis käsitleb direktiivi artikli 25 lõike 6 alusel komisjoni tehtud otsuse kooskõla üksikisikute eraelu ning põhiõiguste ja -vabaduste kaitsega, ei ole tal õigust ise sellist otsust kehtetuks tunnistada.

63 Neid kaalutlusi arvestades, kui isik, kelle isikuandmed on edastatud või võidakse edastada kolmandasse riiki, mida on nimetatud direktiivi 95/46 artikli 25 lõike 6 alusel komisjoni tehtud otsuses, esitab liikmesriigi järelevalveasutusele avalduse oma õiguste ja vabaduste kaitse kohta seoses nende andmete

töötlemisega ning vaidlustab selles avalduses – nagu põhikohtuasjas – komisjoni otsuse kooskõla üksikisikute eraelu ning põhiõiguste ja -vabaduste kaitsega, on kõnealune asutus kohustatud avalduse nõutava hoolsusega läbi vaatama.

64 Kui järelevalveasutus jõuab järeldusele, et avalduse põhjendamiseks esitatud väited on alusetud, ning lükkab seetõttu avalduse tagasi, peab avalduse esitanud isikul tulenevalt direktiivi 95/46 artikli 28 lõike 3 teisest lõigust koostoimes harta artikliga 47 olema võimalik kasutada kohtulikke õiguskaitsevahendeid, mis võimaldavad tal tema huve kahjustava otsuse vaidlustada siseriiklikus kohtus. Käesoleva kohtuotsuse punktides 61 ja 62 viidatud kohtupraktikat silmas pidades peab siseriiklik kohus menetluse peatama ja kehtivuse hindamiseks esitama eelotsusetaotluse Euroopa Kohtule, kui ta leiab, et üks või mitu poolte esitatud või vajaduse korral kohtu omal algatusel tõstatatud väidet kehtetuse kohta on põhjendatud (vt selle kohta kohtuotsus T & L Sugars ja Sidul Açúcares *vs.* komisjon, C-456/13 P, EU:C:2015:284, punkt 48 ja seal viidatud kohtupraktika).

65 Vastasel juhul, kui järelevalveasutus peab põhjendatuks selle isiku esitatud väiteid, kes on tema poole pöördunud avaldusega oma õiguste ja vabaduste kaitse kohta seoses tema isikuandmete töötlemisega, peab liikmesriigi järelevalveasutusel vastavalt direktiivi 95/46 artikli 28 lõike 3 esimese lõigu kolmandale taandele koostoimes eelkõige harta artikli 8 lõikega 3 olema võimalik osaleda kohtumenetlustes. Sellega seoses on liikmesriigi seadusandja kohustatud ette nägema õiguskaitsevahendid, mis võimaldavad järelevalveasutusel esitada siseriiklikes kohtutes väiteid, mida ta peab põhjendatuks, selleks et kohtud juhul, kui neil on komisjoni otsuse kehtivuse suhtes samasugused kahtlused, esitaksid eelotsusetaotluse kõnealuse otsuse kehtivuse analüüsimiseks.

66 Eespool toodud kaalutlusi arvestades tuleb esitatud küsimustele vastata, et direktiivi 95/46 artikli 25 lõiget 6 koostoimes harta artiklitega 7, 8 ja 47 tuleb tõlgendada nii, et selle sätte alusel vastu võetud otsus, nagu seda on otsus 2000/520, milles komisjon on tuvastanud, et kolmandas riigis on tagatud kaitse piisav tase, ei takista liikmesriigi järelevalveasutust direktiivi artikli 28 tähenduses läbi vaatamast isiku avaldust, mis puudutab tema õiguste ja vabaduste kaitset seoses tema selliste isikuandmete töötlemisega, mis on liikmesriigist edastatud sellesse kolmandasse riiki, kui kõnealune isik väidab, et selles riigis kehtiv õigus ja valitsev praktika ei taga kaitse piisavat taset.

Otsuse 2000/520 kehtivus

67 Nagu nähtub eelotsusetaotluse esitanud kohtu selgitustest esitatud küsimuste kohta, väidab M. Schrems põhikohtuasjas, et Ameerika Ühendriikides kehtiv õigus ja valitsev praktika ei taga kaitse piisavat taset direktiivi 95/46 artikli 25 tähenduses. Nagu kohtujurist oma ettepaneku punktides 123 ja 124 märkis, väljendab M. Schrems kahtlusi, millega eelotsusetaotluse esitanud kohus sisuliselt ka nõustub ja mis puudutavad otsuse 2000/520 kehtivust. Niisugustel asjaoludel tuleb käesoleva kohtuotsuse punktides 60–63 tehtud järeldusi silmas pidades ja nimetatud kohtule täieliku vastuse andmiseks analüüsida, kas see otsus vastab direktiivist koostoimes hartaga tulenevatele nõuetele.

Direktiivi 95/46 artikli 25 lõikest 6 tulenevad nõuded

68 Nagu käesoleva kohtuotsuse punktides 48 ja 49 on juba märgitud, on direktiivi 95/46 artikli 25 lõike 1 kohaselt keelatud edastada isikuandmeid kolmandasse riiki, kus ei ole tagatud kaitse piisavat taset.

69 Sellise edastamise kontrollimiseks on direktiivi artikli 25 lõike 6 esimeses lõigus siiski sätestatud, et komisjon „võib leida […], et kolmas riik tagab kaitse piisava taseme [selle] artikli lõike 2 tähenduses oma siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega, […] et kaitsta eraelu puutumatust ja üksikisikute põhivabadusi ja -õigusi”.

70 Ei direktiivi 95/46 artikli 25 lõikes 2 ega ka direktiivi üheski teises sättes ei ole antud mõiste „kaitse piisav tase” määratlust. Täpsemalt on direktiivi artikli 25 lõikes 2 piirdutud sätestamisega, et kolmanda riigi pakutava kaitse taseme piisavust „hinnatakse, pidades silmas kõiki andmete edastamise toimingute või andmete edastamise toimingute kogumi asjaolusid”, ning selles on mitteammendavalt loetletud asjaolud, mida hinnangu andmisel tuleb arvesse võtta.

71 Siiski ühelt poolt, nagu nähtub direktiivi 95/46 artikli 25 lõike 6 sõnastusest endast, nõuab see säte, et kolmas riik „tagaks” kaitse piisava taseme oma siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega. Teiselt poolt – samuti selle sätte kohaselt – hinnatakse kolmanda riigi tagatava kaitse piisavust selleks, „et kaitsta eraelu puutumatust ja üksikisikute põhivabadusi ja -õigusi”.

72 Nii viiakse direktiivi 95/46 artikli 25 lõikega 6 ellu harta artikli 8 lõikes 1 ette nähtud sõnaselge isikuandmete kaitsmise kohustus ja selle eesmärk on tagada, nagu kohtujurist oma ettepaneku punktis 139 märkis, järjepidev kõrgetasemeline kaitse, kui isikuandmeid edastatakse kolmandasse riiki.

73 Direktiivi 95/46 artikli 25 lõikes 6 sisalduv sõna „piisav” tähendab, et ei saa olla nõutav, et kolmas riik tagaks kaitsetaseme, mis on liidu õiguskorras tagatuga identne. Nagu kohtujurist oma ettepaneku punktis 141 märkis, tuleb väljendit „kaitse piisav tase” siiski mõista nii, et see nõuab, et kolmas riik tõepoolest tagab oma siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega põhiõiguste ja -vabaduste kaitse taseme, mis on sisuliselt samaväärne sellega, mis on liidus tagatud vastavalt direktiivile 95/46 koostoimes hartaga. Nimelt, kui selline nõue puuduks, eirataks käesoleva kohtuotsuse eelmises punktis nimetatud eesmärki. Lisaks oleks direktiiviga 95/46 koostoimes hartaga tagatud kõrgetasemelisest kaitsest võimalik hõlpsasti mööda hiilida sel viisil, et isikuandmed edastatakse liidust kolmandatesse riikidesse, et neid seal töödelda.

74 Direktiivi 95/46 artikli 25 lõike 6 selgest sõnastusest ilmneb, et komisjoni otsuses nimetatud kolmanda riigi õiguskord peab tagama kaitse piisava taseme. Kuigi vahendid, mida kolmas riik sellega seoses niisuguse kaitsetaseme saavutamiseks kasutab, võivad olla erinevad nendest, mida liidus rakendatakse direktiivist koostoimes hartaga tulenevate nõuete järgimise tagamiseks, peavad need vahendid siiski praktikas osutuma tõhusaks, et tagada liidus kehtiva kaitsega sisuliselt samaväärne kaitse.

75 Neil asjaoludel on komisjon kolmanda riigi pakutava kaitsetaseme analüüsimisel kohustatud hindama selle riigi siseriiklikust õigusest või endale võetud rahvusvahelistest kohustustest tulenevate kohaldatavate õigusnormide sisu ning nende õigusnormide järgimise tagamise praktikat, kusjuures institutsioon peab direktiivi 95/46 artikli 25 lõike 2 kohaselt arvesse võtma kõiki isikuandmete kolmandasse riiki edastamisega seotud asjaolusid.

76 Samuti, kuna kolmanda riigi tagatav kaitsetase võib muutuda, peab komisjon pärast direktiivi 95/46 artikli 25 lõike 6 alusel otsuse tegemist regulaarselt kontrollima, kas järeldus kõnealuse kolmanda riigi tagatava kaitse piisava taseme kohta on jätkuvalt faktiliselt ja õiguslikult põhjendatud. Niisugune kontrollimine on igal juhul nõutav, kui teatud asjaolud tekitavad vastava kahtluse.

77 Lisaks, nagu kohtujurist oma ettepaneku punktides 134 ja 135 märkis, tuleb direktiivi 95/46 artikli 25 lõike 6 alusel komisjoni tehtud otsuse kehtivuse analüüsimisel arvesse võtta ka pärast selle otsuse vastuvõtmist aset leidnud asjaolusid.

78 Sellega seoses tuleb tõdeda, et arvestades esiteks olulist rolli, mis on isikuandmete kaitsel eraelu puutumatuse põhiõiguse seisukohast, ja teiseks nende isikute suurt arvu, kelle põhiõigusi võidakse rikkuda, kui isikuandmeid edastatakse kolmandasse riiki, kus ei ole tagatud kaitse piisav tase, on komisjoni kaalutlusruum kolmanda riigi tagatava kaitsetaseme piisavuse hindamisel väike, mistõttu tuleb direktiivi 95/46 artiklist 25 koostoimes hartaga tulenevaid nõudeid kontrollida rangelt (vt analoogia alusel kohtuotsus Digital Rights Ireland jt, C-293/12 ja C-594/12, EU:C:2014:238, punktid 47 ja 48).

Otsuse 2000/520 artikkel 1

79 Komisjon asus otsuse 2000/520 artikli 1 lõikes 1 seisukohale, et selle I lisas sätestatud põhimõtted rakendatuna kooskõlas otsuse II lisas sätestatud KKKga tagavad piisava kaitse taseme liidust Ameerika Ühendriikides asuvatele organisatsioonidele edastatavatele isikuandmetele. Sellest sättest nähtub, et nii need põhimõtted kui ka KKK on avaldanud Ameerika Ühendriikide kaubandusministeerium.

80 Organisatsiooni liitumine Safe Harbor' põhimõtetega toimub ise kinnituse andmise süsteemi kohaselt, nagu ilmneb otsuse artikli 1 lõigetest 2 ja 3 koostoimes otsuse II lisas sisalduva KKK 6-ga.

81 Kuigi see, kui kolmas riik kasutab ise kinnituse andmise süsteemi, ei ole iseenesest vastuolus direktiivi 95/46 artikli 25 lõikes 6 ette nähtud nõudega, et asjaomane kolmas riik peab kaitse piisava taseme tagama „siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega", põhineb sellise süsteemi usaldusväärsus seda nõuet arvestades peamiselt selliste tõhusate avastamis- ja kontrollimehhanismide sisseseadmises, mis võimaldavad põhiõiguste – eelkõige õiguse eraelu puutumatusele ja õiguse isikuandmete kaitsele – kaitset tagavate õigusnormide võimalikke rikkumisi praktikas tuvastada ja nende eest karistada.

82 Käesoleval juhul on Safe Harbor' põhimõtted otsuse 2000/520 I lisa teise lõigu kohaselt „mõeldud kasutamiseks ainult isikuandmeid Euroopa Liidust vastu võtvate Ameerika Ühendriikide organisatsioonide poolt, et saavutada vastavus programmi Safe Harbor põhimõtetega ja seeläbi saavutada eeldatav „piisav" andmekaitse". Need põhimõtted on seega kohaldatavad ainult Ameerika Ühendriikide organisatsioonidele, kes on kinnituse andnud ja saavad isikuandmeid liidust, ilma et oleks nõutav, et Ameerika Ühendriikide ametiasutused oleksid kohustatud neid põhimõtteid järgima.

83 Lisaks nähtub otsuse 2000/520 artiklist 2, et otsus „puudutab ainult KKKdega kooskõlas rakendatud [Safe Harbor'] põhimõtetega tagatud kaitse taseme piisavust Ameerika Ühendriikides vastavalt direktiivi [95/46] artikli 25 lõike 1 nõuetele", sisaldamata siiski piisavaid järeldusi meetmete kohta, millega Ameerika Ühendriigid tagavad direktiivi artikli 25 lõike 6 tähenduses kaitse piisava taseme siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega.

84 Lisaks sellele võib vastavalt otsuse 2000/520 I lisa neljandale lõigule nende põhimõtete kohaldamist piirata muu hulgas „[Ameerika Ühendriikide] riikliku julgeoleku, avaliku huvi või õiguskaitseliste vajaduste täitmiseks vajalikus ulatuses" ning „statuudi, valitsuse määruse või pretsedendiõigusega, mis loovad vasturääkivaid kohustusi või annavad otseseid volitusi, tingimusel et selliste volituste kasutamisel suudab organisatsioon demonstreerida, et põhimõtete mittejärgimine tema poolt piirdub ulatusega, mis on vajalik selliste volitustega seotud ülekaaluka õigustatud huvi järgimiseks".

85 Sellega seoses on otsuse 2000/520 IV lisa B osas Safe Harbor' põhimõtete kohaldatavuse piiride kohta rõhutatud, et „[s]elge on, et kui Ameerika Ühendriikide seadustes sätestatakse vastandlik kohustus, peavad Ameerika Ühendriikide organisatsioonid, sõltumata sellest, kas nad osalevad programmis Safe Harbor või mitte, seadust täitma".

86 Seega on otsuses 2000/520 ette nähtud „[Ameerika Ühendriikide] riikliku julgeoleku, avaliku huvi või õiguskaitseliste vajaduste täitmiseks vajalikus ulatuses" esimus Safe Harbor' põhimõtete ees ning selle esimuse kohaselt on kinnituse andnud Ameerika Ühendriikide organisatsioonid, kes saavad liidust isikuandmeid, kohustatud nendest põhimõtetest piiramatult kõrvale kalduma, kui need lähevad nimetatud vajadustega vastuollu ja on seega nendega kokkusobimatud.

87 Pidades silmas otsuse 2000/520 I lisa neljandas lõigus sisalduva erandi üldist laadi, muudab see võimalikuks Ameerika Ühendriikide riiklikku julgeolekut ja avalikku huvi puudutavatel nõuetel või selle riigi sisemisel õigusel põhinevad sekkumised nende isikute põhiõigustesse, kelle isikuandmed on edastatud või võidakse edastada liidust Ameerika Ühendriikidesse. Eraelu puutumatuse põhiõiguse

riive tuvastamisel ei ole oluline, kas edastatud isikuandmed on delikaatsed või mitte või kas asjaomased isikud on selle riive tõttu pidanud taluma mingeid ebamugavusi (kohtuotsus Digital Rights Ireland jt, C-293/12 ja C-594/12, EU:C:2014:238, punkt 33 ja seal viidatud kohtupraktika).

88 Peale selle ei sisalda otsus 2000/520 mingeid järeldusi selle kohta, et Ameerika Ühendriikides kehtiks riigi tasandil õigusnorme, mille eesmärk oleks piirata võimalikke sekkumisi nende isikute põhiõigustesse, kelle andmeid edastatakse liidust Ameerika Ühendriikidesse, kusjuures neid sekkumisi on selle riigi asutustel lubatud toime panna, kui nad taotlevad õiguspäraseid eesmärke, nagu riiklik julgeolek.

89 Sellele lisandub veel asjaolu, et otsusest 2000/520 ei ilmne, et sedalaadi sekkumiste vastu oleks olemas tõhus õiguslik kaitse. Nagu kohtujurist oma ettepaneku punktides 204–206 märkis, on eraõigusliku vahekohtu mehhanismid ja Federal Trade Commissioni läbi viidavad menetlused, sealhulgas volitused, mida on kirjeldatud eelkõige otsuse II lisas sisalduvas KKK 11-s, piiratud kaubanduslike vaidlustega, puudutavad Safe Harbor' põhimõtete järgimist Ameerika Ühendriikide ettevõtjate poolt ja neid ei saa rakendada vaidlustes, mis puudutavad küsimust, kas riiklikku päritolu meetmetest tulenev sekkumine põhiõigustesse on seaduslik.

90 Pealegi kinnitab otsuse 2000/520 kohta eespool esitatud analüüsi komisjoni enda hinnang selle otsuse rakendamisest tulenevale olukorrale. Nimelt eelkõige teatise COM(2013) 846 final punktides 2 ja 3.2 ning teatise COM(2013) 847 final punktides 7.1, 7.2 ja 8, mille sisu on ära toodud käesoleva kohtuotsuse punktides 13–16 ning 22, 23 ja 25, tõdes kõnealune institutsioon, et Ameerika Ühendriikide ametiasutused said liikmesriikidest Ameerika Ühendriikidesse edastatud isikuandmetega tutvuda ja neid andmeid töödelda viisil, mis on vastuolus eelkõige nende edastamise eesmärgiga ja mis läks kaugemale sellest, mis on rangelt vajalik ja riikliku julgeoleku kaitsega proportsionaalne. Samuti tuvastas komisjon, et asjaomaste isikute jaoks puuduvad halduslikud või kohtulikud õiguskaitsevahendid, mis võimaldaksid neil eelkõige neid puudutavate andmetega tutvuda või vajaduse korral lasta neisse parandusi teha või neid kustutada.

91 Mis puudutab põhiõiguste ja -vabaduste kaitse taset, mis on tagatud liidus, siis peab liidu õigusakt, millega kaasneb sekkumine harta artiklitega 7 ja 8 tagatud põhiõigustesse, Euroopa Kohtu väljakujunenud praktika kohaselt sisaldama selgeid ja täpseid õigusnorme, mis reguleerivad meetme ulatust ja kohaldamist ning millega on kehtestatud miinimumnõuded, nii et isikutel, kelle isikuandmed on asjassepuutuvad, on piisavad tagatised, mis võimaldavad nende andmeid tõhusalt kaitsta kuritarvitamise ohu ning ebaseadusliku juurdepääsu ja kasutamise eest. Niisuguste tagatiste olemasolu on veel vajalikum siis, kui isikuandmeid töödeldakse automaatselt ja kui esineb suur oht, et neile andmetele pääsetakse juurde ebaseaduslikult (kohtuotsus Digital Rights Ireland jt, C-293/12 ja C-594/12, EU:C:2014:238, punktid 54 ja 55 ning seal viidatud kohtupraktika).

92 Lisaks ja eelkõige nõuab eraelu puutumatuse põhiõiguse kaitsmine liidu tasandil, et isikuandmete kaitse erandid ja piirangud piirduksid rangelt vajalikuga (kohtuotsus Digital Rights Ireland jt, C-293/12 ja C-594/12, EU:C:2014:238, punkt 52 ning seal viidatud kohtupraktika).

93 Rangelt vajalikuga ei piirdu õigusakt, mis annab üldise loa säilitada kõikide selliste isikute kõik isikuandmed, kelle andmed on edastatud liidust Ameerika Ühendriikidesse, ilma et olenevalt taotletavast eesmärgist esineks eristamist, piiranguid või erandeid ning ilma, et oleks ette nähtud objektiivset kriteeriumi, mis võimaldaks piiritleda ametiasutuste juurdepääsu andmetele ja nende hilisemat kasutamist konkreetsetel rangelt piiritletud eesmärkidel, millega nii andmete tutvumise kui ka kasutamisega kaasnev sekkumine võib olla põhjendatud (vt selle kohta seoses Euroopa Parlamendi ja nõukogu 15. märtsi 2006. aasta direktiiviga 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ (ELT L 105, lk 54), kohtuotsus Digital Rights Ireland jt, C-293/12 ja C-594/12, EU:C:2014:238, punktid 57–61).

94 Täpsemalt tuleb õigusakti, mis võimaldab ametiasutustel elektroonilise side sisuga üldiselt tutvuda, pidada harta artikliga 7 tagatud eraelu puutumatuse põhiõiguse põhisisu kahjustavaks (vt selle kohta kohtuotsus Digital Rights Ireland jt, C-293/12 ja C-594/12, EU:C:2014:238, punkt 39).

95 Samuti ei järgi õigusakt, milles ei ole andmesubjektile ette nähtud mingit võimalust kasutada õiguskaitsevahendeid, et tutvuda teda puudutavate isikuandmetega või lasta neisse parandusi teha või neid kustutada, harta artiklis 47 sätestatud põhiõiguse tõhusale kohtulikule kaitsele põhisisu. Harta artikli 47 esimene lõik nõuab nimelt, et igaühel, kelle liidu õigusega tagatud õigusi või vabadusi rikutakse, on selles artiklis kehtestatud tingimuste kohaselt õigus tõhusale õiguskaitsevahendile kohtus. Juba tõhusa kohtuliku kontrolli olemasolu, mille eesmärk on tagada liidu õigusnormide järgimine, on õigusriigi olemuslik tunnus (vt selle kohta kohtuotsused Les Verts *vs*. parlament, 294/83, EU:C:1986:166, punkt 23; Johnston, 222/84, EU:C:1986:206, punktid 18 ja 19; Heylens jt, 222/86, EU:C:1987:442, punkt 14, ning UGT-Rioja jt, C-428/06–C-434/06, EU:C:2008:488, punkt 80).

96 Nagu käesoleva kohtuotsuse punktides 71, 73 ja 74 on tõdetud, nõuab direktiivi 95/46 artikli 25 lõike 6 alusel komisjoni otsuse tegemine, et see institutsioon oleks jõudnud nõuetekohaselt põhjendatud järeldusele, et asjassepuutuvas kolmandas riigis on siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega tõepoolest tagatud põhiõiguste kaitse tase, mis on sisuliselt samaväärne liidu õiguskorras tagatuga, nagu nähtub muu hulgas käesoleva kohtuotsuse eelmistest punktidest.

97 Tuleb aga märkida, et komisjon ei tõdenud otsuses 2000/520, et Ameerika Ühendriigid siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega tõepoolest „tagavad" kaitse piisava taseme.

98 Seega, ilma et oleks vaja Safe Harbor' põhimõtteid sisuliselt analüüsida, tuleb järeldada, et otsuse artikkel 1 eirab nõudeid, mis on ette nähtud direktiivi 95/46 artikli 25 lõikes 6 koostoimes hartaga, ning seetõttu on kõnealune otsus kehtetu.

Otsuse 2000/520 artikkel 3

99 Käesoleva kohtuotsuse punktides 53, 57 ja 63 esitatud kaalutlustest ilmneb, et lähtuvalt direktiivi 95/46 artiklist 28 koostoimes eelkõige harta artikliga 8 peab liikmesriigi järelevalveasutustel olema võimalik sõltumatult läbi vaadata mis tahes avaldusi isiku õiguste ja vabaduste kaitse kohta seoses tema isikuandmete töötlemisega. See on nii eelkõige juhul, kui avalduses tõstatab isik küsimusi direktiivi artikli 25 lõike 6 alusel komisjoni tehtud otsuse kooskõla kohta üksikisikute eraelu puutumatuse ning põhiõiguste ja -vabaduste kaitsega.

100 Otsuse 2000/520 artikli 3 lõike 1 esimeses lõigus on siiski ette nähtud erinormid volituste kohta, mis liikmesriigi järelevalveasutustel on järelduse suhtes, mille komisjon on teinud kaitse piisava taseme kohta direktiivi 95/46 artikli 25 tähenduses.

101 Nimelt, selle sätte kohaselt võivad need asutused „[i]lma et see piiraks [nende] volitusi võtta meetmeid selliste siseriiklike sätete järgimise tagamiseks, mis on vastu võetud muude sätete alusel peale direktiivi [95/46] artikli 25, […] kasutada oma volitusi ka andmete edastamise peatamiseks organisatsioonile, mis on ise kohustunud järgima [otsuse 2000/520] põhimõtteid", kitsastel tingimustel, millega on sekkumiseks kehtestatud kõrge künnis. Kuigi see säte ei kahjusta järelevalveasutuste pädevust võtta meetmeid selliste siseriiklike sätete järgimise tagamiseks, mis on vastu võetud direktiivi alusel, välistab see seevastu nende asutuste võimaluse võtta meetmeid direktiivi artikli 25 järgimise tagamiseks.

102 Otsuse 2000/520 artikli 3 lõike 1 esimest lõiku tuleb seega mõista nii, et see jätab liikmesriigi järelevalveasutused pädevusest, mis neil on tulenevalt direktiivi 95/46 artiklist 28, ilma juhul, kui isik selle sätte alusel esitatud avalduses toob esile asjaolud, mis võivad seada kahtluse alla selle, kas üksikisikute eraelu puutumatuse ning põhiõiguste ja -vabaduste kaitsega on kooskõlas komisjoni otsus, milles direktiivi artikli 25 lõike 6 alusel on tuvastatud, et kolmas riik tagab kaitse piisava taseme.

103 Rakenduspädevus, mille liidu seadusandja on komisjonile direktiivi 95/46 artikli 25 lõikega 6 andnud, ei omista aga sellele institutsioonile pädevust piirata liikmesriigi järelevalveasutuste volitusi, mida on nimetatud käesoleva kohtuotsuse eelmises punktis.

104 Neil asjaoludel tuleb asuda seisukohale, et otsuse 2000/520 artikli 3 vastuvõtmisega on komisjon ületanud pädevust, mis on talle antud direktiivi 95/46 artikli 25 lõike 6 koostoimes hartaga, ning seetõttu on see artikkel kehtetu.

105 Kuna otsuse 2000/520 artiklid 1 ja 3 on artiklitest 2 ja 4 ning otsuse lisadest lahutamatud, mõjutab nende kehtetus kogu otsuse kehtivust.

106 Kõiki eespool toodud kaalutlusi arvestades tuleb jõuda järeldusele, et otsus 2000/520 on kehtetu.

Kohtukulud

107 Kuna põhikohtuasja poolte jaoks on käesolev menetlus eelotsusetaotluse esitanud kohtus pooleli oleva asja üks staadium, otsustab kohtukulude jaotuse siseriiklik kohus. Euroopa Kohtule seisukohtade esitamisega seotud kulusid, välja arvatud poolte kohtukulud, ei hüvitata.

Esitatud põhjendustest lähtudes Euroopa Kohus (suurkoda) otsustab:

1. **Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivi 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (muudetud Euroopa Parlamendi ja nõukogu 29. septembri 2003. aasta määrusega (EÜ) nr 1882/2003) artikli 25 lõiget 6 koostoimes Euroopa Liidu põhiõiguste harta artiklitega 7, 8 ja 47 tuleb tõlgendada nii, et selle sätte alusel vastu võetud otsus – nagu seda on komisjoni 26. juuli 2000. aasta otsus 2000/520/EÜ vastavalt direktiivile 95/46 piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium –, milles Euroopa Komisjon on tuvastanud, et kolmandas riigis on tagatud kaitse piisav tase, ei takista liikmesriigi järelevalveasutust direktiivi (muudetud kujul) artikli 28 tähenduses läbi vaatamast isiku avaldust, mis puudutab tema õiguste ja vabaduste kaitset seoses tema selliste isikuandmete töötlemisega, mis on liikmesriigist edastatud sellesse kolmandasse riiki, kui kõnealune isik väidab, et selles riigis kehtiv õigus ja valitsev praktika ei taga kaitse piisavat taset.**

2. **Otsus 2000/520 on kehtetu.**

Allkiri