Kohtulahendite kogumik

EUROOPA KOHTU OTSUS (suurkoda)

16. juuli 2020*

Eelotsusetaotlus – Füüsiliste isikute kaitse isikuandmete töötlemisel – Euroopa Liidu põhiõiguste harta – Artiklid 7, 8 ja 47 – Määrus (EL) 2016/679 – Artikli 2 lõige 2 – Kohaldamisala – Isikuandmete edastamine kolmandatesse riikidesse ärilisel eesmärgil – Artikkel 45 – Komisjoni otsus kaitse piisavuse kohta – Artikkel 46 – Edastamine asjakohaste kaitsemeetmete kohaldamisel – Artikkel 58 – Järelevalveasutuste volitused – Edastatud andmete töötlemine kolmanda riigi avaliku võimu asutuste poolt riikliku julgeoleku eesmärgil – Kolmandas riigis tagatud kaitse taseme piisavuse hindamine – Otsus 2010/87/EL – Andmekaitse tüüptingimused isikuandmete edastamiseks kolmandatesse riikidesse – Vastutava töötleja pakutavad asjakohased kaitsemeetmed – Kehtivus – Rakendusotsus (EL) 2016/1250 – ELi-USA andmekaitseraamistikuga Privacy Shield tagatud kaitse piisavus – Kehtivus – Kaebus, mille on esitanud füüsiline isik, kelle andmeid on edastatud Euroopa Liidust Ameerika Ühendriikidesse

Kohtuasjas C-311/18,

mille ese on ELTL artikli 267 alusel High Courti (kõrge kohus, Iirimaa) 4. mai 2018. aasta otsusega esitatud eelotsusetaotlus, mis saabus Euroopa Kohtusse 9. mail 2018, menetluses

Data Protection Commissioner

versus

Facebook Ireland Ltd,

Maximillian Schrems,

menetluses osalesid:

The United States of America,

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

EUROOPA KOHUS (suurkoda),

koosseisus: president K. Lenaerts, asepresident R. Silva de Lapuerta, kodade presidendid A. Arabadjiev, A. Prechal, M. Vilaras, M. Safjan, S. Rodin, P. G. Xuereb, L. S. Rossi ja I. Jarukaitis ning kohtunikud M. Ilešič, T. von Danwitz (ettekandja) ja D. Šváby,

* Kohtumenetluse keel: inglise.

kohtujurist: H. Saugmandsgaard Øe,

kohtusekretär: ametnik C. Strömholm,

arvestades kirjalikku menetlust ja 9. juuli 2019. aasta kohtuistungil esitatut,

arvestades seisukohti, mille esitasid:

– Data Protection Commissioner, esindajad: *solicitor* D. Young, B. Murray, *SC*, M. Collins, *SC*, ja C. Donnelly, *BL*,

– Facebook Ireland Ltd, esindajad: P. Gallagher, *SC*, N. Hyland, *SC*, A. Mulligan, *BL*, F. Kieran, *BL* ning *solicitors* P. Nolan, C. Monaghan, C. O'Neill ja R. Woulfe,

– M. Schrems, esindajad: *Rechtsanwalt* H. Hofmann, E. McCullough, *SC*, J. Doherty, *SC*, S. O'Sullivan, *SC*, ja *solicitor* G. Rudden,

– The United States of America, esindajad: E. Barrington, *SC*, S. Kingston, *BL*, ning *solicitors* S. Barton ja B. Walsh,

– Electronic Privacy Information Centre, esindajad: *solicitor* S. Lucey, G. Gilmore, *BL*, A. Butler, *BL*, ja C. O'Dwyer, *SC*,

– BSA Business Software Alliance Inc., esindajad: *advocaten* B. Van Vooren ja K. Van Quathem,

– Digitaleurope, esindajad: *barrister* N. Cahill, *solicitor* J. Cahir ja M. Cush, *SC*,

– Iirimaa, esindajad: A. Joyce ja M. Browne, keda abistas D. Fennelly, *BL*,

– Belgia valitsus, esindajad: J.-C. Halleux ja P. Cottin,

– Tšehhi valitsus, esindajad: M. Smolek, J. Vláčil, O. Serdula ja A. Kasalická,

– Saksamaa valitsus, esindajad: J. Möller, D. Klebs ja T. Henze,

– Prantsuse valitsus, esindaja: A.-L. Desjonquères,

– Madalmaade valitsus, esindajad: C. S. Schillemans, K. Bulterman ja M. Noort,

– Austria valitsus, esindajad: J. Schmoll ja G. Kunnert,

– Poola valitsus, esindaja: B. Majczyna,

– Portugali valitsus, esindajad: L. Inez Fernandes, A. Pimenta ja C. Vieira Guerra,

– Ühendkuningriigi valitsus, esindaja: S. Brandon, keda abistasid J. Holmes, *QC*, ja *barrister* C. Knight,

– Euroopa Parlament, esindajad: M. J. Martínez Iglesias ja A. Caiola,

– Euroopa Komisjon, esindajad: D. Nardi, H. Krämer ja H. Kranenborg,

– Euroopa Andmekaitsenõukogu, esindajad: A. Jelinek ja K. Behn,

olles 19. detsembri 2019. aasta kohtuistungil ära kuulanud kohtujuristi ettepaneku,

on teinud järgmise

otsuse

1 Eelotsusetaotlus puudutab sisuliselt

– Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivi 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EÜT 1995, L 281, lk 31; ELT eriväljaanne 13/15, lk 355) artikli 3 lõike 2 esimese taande, artiklite 25 ja 26 ning artikli 28 lõike 3 tõlgendamist lähtuvalt ELL artikli 4 lõikest 2 ja Euroopa Liidu põhiõiguste harta (edaspidi „harta“) artiklitest 7, 8 ja 47,

– komisjoni 5. veebruari 2010. aasta otsuse 2010/87/EL kolmandates riikides asuvatele volitatud töötlejatele isikuandmete edastamise lepingu tüüptingimuste kohta […] direktiivi 95/46 alusel (ELT 2010, L 39, lk 5) (muudetud komisjoni 16. detsembri 2016. aasta rakendusotsusega (EL) 2016/2297 (ELT 2016, L 344, lk 100) (edaspidi „tüüptingimuste otsus“) tõlgendamist ja kehtivust, ning

– komisjoni 12. juuli 2016. aasta rakendusotsuse (EL) 2016/1250 isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield vastavalt […] direktiivile 95/46 (ELT 2016, L 207, lk 1; edaspidi „Privacy Shieldi otsus“) tõlgendamist ja kehtivust.

2 Taotlus on esitatud ühelt poolt Data Protection Commissioneri (Iirimaa andmekaitsevolinik) (edaspidi „andmekaitsevolinik“) ning teiselt poolt Facebook Ireland Ltd ja Maximillian Schremsi vahelises kohtuvaidluses, mis puudutab M. Schremsi esitatud kaebust selle kohta, et Facebook Ireland edastab tema isikuandmeid Facebook Inc-le USAs.

Õiguslik raamistik

Direktiiv 95/46

3 Direktiivi 95/46 artikli 3 „Reguleerimisala“ lõikes 2 oli sätestatud:

„Käesolevat direktiivi ei kohaldata isikuandmete töötlemise suhtes:

– kui see toimub sellise tegevuse käigus, mis jääb väljapoole ühenduse õigust, nagu näiteks Euroopa Liidu lepingu V ja VI jaotises osutatud tegevused, ja igal juhul sellise töötlemise suhtes, mis on seotud avaliku korra, riigikaitse, riigi julgeoleku (sealhulgas riigi majanduslik heaolu, kui töötlemine on seotud riigi julgeoleku küsimustega) ja riigi toimingutega kriminaalõiguse valdkonnas,

[…]“.

4 Selle direktiivi artiklis 25 oli sätestatud:

„1. Liikmesriigid sätestavad, et töödeldavate […] 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; […]

[…]

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."

5 Direktiivi artikli 26 lõigetes 2 ja 4 oli sätestatud:

„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.

[…]

4. Kui komisjon otsustab artikli 31 lõikes 2 osutatud korras, et teatavad lepingu tüüptingimused pakuvad piisavaid lõikega 2 nõutavaid tagatisi, võtavad liikmesriigid komisjoni otsuse järgimiseks vajalikke meetmeid."

6 Sama direktiivi artikli 28 lõike 3 kohaselt:

„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."

[…]".

Isikuandmete kaitse üldmäärus

7 Direktiiv 95/46 tunnistati kehtetuks ja asendati Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrusega (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46 kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT 2016, L 119, lk 1; parandus ELT 2018, L 127, lk 3).

8 Isikuandmete kaitse üldmäärus põhjendustes 6, 10, 101, 103, 104, 107–109, 114, 116 ja 141 on märgitud:

„(6) Kiire tehnoloogiline areng ja üleilmastumine on tekitanud isikuandmete kaitsel uusi väljakutseid. Isikuandmete kogumise ja jagamise ulatus on märkimisväärselt suurenenud. Tehnoloogia võimaldab nii era- kui ka avaliku sektori asutustel kasutada isikuandmeid oma tegevuses enneolematus ulatuses. Füüsilised isikud avaldavad isikuandmeid üha avalikumalt ja

ülemaailmsemalt. Tehnoloogia on põhjalikult muutnud nii majandust kui ka ühiskondlikku elu ja peaks täiendavalt hõlbustama liidusisest andmete vaba liikumist ning nende kolmandatesse riikidesse ja rahvusvahelistele organisatsioonidele edastamist, tagades samal ajal isikuandmete kõrgetasemelise kaitse.

[…]

(10) Selleks et tagada füüsiliste isikute järjekindel ja kõrgetasemeline kaitse ning kõrvaldada takistused isikuandmete liikumisel liidus, peaks füüsiliste isikute õiguste ja vabaduste kaitse selliste andmete töötlemisel olema kõigis liikmesriikides samal tasemel. Isikuandmete töötlemisel tuleks tagada füüsiliste isikute põhiõiguste ja -vabaduste kaitse eeskirjade järjekindel ja ühtne kohaldamine kogu liidus. Seoses isikuandmete töötlemisega juriidilise kohustuse täitmiseks, avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks peaks liikmesriikidel olema lubatud säilitada või kehtestada õigusnormid käesoleva määruse eeskirjade kohaldamise täpsustamiseks. Koostoimes andmekaitset käsitlevate üldiste ja horisontaalsete õigusaktidega, millega rakendatakse direktiivi 95/46/EÜ, on liikmesriikidel mitmeid sektoripõhiseid õigusakte valdkondades, mis vajavad spetsiifilisemaid sätteid. Samuti nähakse käesoleva määrusega liikmesriikidele ette manööverdamisruum oma eeskirjade, sealhulgas isikuandmete eriliikide töötlemise eeskirjade täpsustamiseks. Sellega seoses ei välista käesolev määrus sellist liikmesriigi õigust, millega määratletakse konkreetsete töötlemisjuhtude asjaolud, sealhulgas määratakse täpsemalt kindlaks tingimused, mille alusel isikuandmete töötlemine on seaduslik.

[…]

(101) Isikuandmete piiriülene liikumine liitu mitte kuuluvatesse riikidesse ja rahvusvahelistele organisatsioonidele ning nendest riikidest ja organisatsioonidest liitu on vajalik rahvusvahelise kaubanduse ja koostöö laiendamiseks. Nimetatud voogude suurenemine on laiendanud isikuandmete kaitsega seonduvate probleemide ringi. Isikuandmete edastamisel liidust vastutavatele töötlejatele, volitatud töötlejatele või muudele vastuvõtjatele kolmandates riikides või rahvusvahelistele organisatsioonidele ei tohiks aga kahjustada liidus käesoleva määrusega tagatud füüsiliste isikute kaitse taset, sealhulgas juhtudel, kui kolmandast riigist või rahvusvahelisest organisatsioonist saadud isikuandmed saadetakse edasi vastutavatele töötlejatele või volitatud töötlejatele samas või muus kolmandas riigis või rahvusvahelises organisatsioonis. Igal juhul tohib andmeid kolmandatele riikidele ja rahvusvahelistele organisatsioonidele edastada ainult käesolevat määrust täielikult järgides. Andmeid tohiks edastada ainult siis, kui vastutav töötleja ja volitatud töötleja täidavad käesolevas määruses sätestatud tingimusi isikuandmete edastamise kohta, arvestades muid käesoleva määruse sätteid.

[…]

(103) Komisjon võib kogu liidu osas otsustada, et kolmas riik, territoorium või kindlaksmääratud sektor või rahvusvaheline organisatsioon pakuvad isikuandmete kaitset piisaval tasemel, tagades seega kogu liidus selle kolmanda riigi ja rahvusvahelise organisatsiooni osas õiguskindluse ja ühtsuse, mille puhul loetakse, et nad tagavad isikuandmete kaitse piisaval tasemel. Sellisel juhul võib isikuandmete edastamine kõnealusesse riiki või kõnealusele rahvusvahelisele organisatsioonile toimuda ilma, et oleks vaja saada täiendav luba. Komisjon võib samuti otsustada sellise otsuse tagasi võtta, teavitades sellest kolmandat riiki või rahvusvahelist organisatsiooni ja esitades talle täieliku põhjenduse.

(104) Kooskõlas põhiväärtustega, millele liit on rajatud, eelkõige inimõiguste kaitsmisega, peaks komisjon kolmanda riigi või territooriumi või kindlaksmääratud sektori hindamisel arvesse võtma seda, kuidas konkreetne kolmas riik peab kinni õigusriigi ja õiguskaitse kättesaadavuse põhimõtetest ning rahvusvahelistest inimõiguste normidest ja standarditest ning oma üldistest ja valdkondlikest õigusaktidest, sealhulgas õigusaktidest, mis käsitlevad avalikku julgeolekut,

riigikaitset ja riiklikku julgeolekut, samuti avalikku korda ja kriminaalõigust. Võttes vastu kaitse piisavuse otsust seoses territooriumi või kindlaksmääratud sektoriga kolmandas riigis, tuleks arvesse võtta selgeid ja objektiivseid kriteeriume, näiteks konkreetseid isikuandmete töötlemise toiminguid ja kohaldatavate õigusnormide kohaldamisala ning kolmandas riigis kehtivaid õigusakte. Kolmas riik peaks võtma kohustusi, millega tagatakse piisav kaitse tase, mis sisuliselt vastab liidus tagatava kaitse tasemele, eelkõige juhul, kui isikuandmeid töödeldakse ühes või mitmes konkreetses sektoris. Eelkõige peaks kolmas riik tagama andmete kaitse tõhusa ja sõltumatu järelevalve ja nägema ette liikmesriikide andmekaitseasutustega tehtava koostöö mehhanismid, samuti tuleks andmesubjektidele tagada tõhusad ja kohtulikult kaitstavad õigused ning tõhus haldus- ja õiguskaitse.

[…]

(107) Komisjon võib tunnistada, et kolmandas riigis, territooriumil või kindlaksmääratud sektoris või rahvusvahelises organisatsioonis ei tagata enam piisaval tasemel andmekaitset. Sellest tulenevalt tuleks isikuandmete edastamine kõnealusele kolmandale riigile või rahvusvahelisele organisatsioonile keelata, välja arvatud juhul, kui täidetakse käesoleva määruse nõudeid, mis on seotud edastamisega asjaomaste kaitsemeetmete abil, sealhulgas siduvad kontsernisisesed eeskirjad ja erandid konkreetsetes olukordades. Sellisel juhul tuleks ette näha komisjoni ja sellise kolmanda riigi või rahvusvahelise organisatsiooni konsultatsioonid. Komisjon peaks kolmandat riiki või rahvusvahelist organisatsiooni õigeaegselt põhjustest teavitama ja alustama nendega konsultatsioone, et olukorda parandada.

(108) Kaitse piisavuse otsuse puudumise korral peaks vastutav töötleja või volitatud töötleja võtma meetmed, et korvata kolmanda riigi andmekaitse puudulik tase asjakohaste andmesubjekti kaitsmise meetmetega. Sellised asjakohased kaitsemeetmed võivad hõlmata järgneva kasutamist: siduvad kontsernisisesed eeskirjad, komisjoni vastu võetud standardsed andmekaitseklauslid, järelevalveasutuse vastu võetud standardsed andmekaitseklauslid või järelevalveasutuse heaks kiidetud lepingu tüüptingimused. Need kaitsemeetmed peaksid tagama liidu siseseks töötlemiseks asjakohaste andmekaitsenõuete täitmise ja andmesubjektide õiguste kaitse, sealhulgas andmesubjektide kohtulikult kaitstavate õiguste ja tõhusate õiguskaitsevahendite kättesaadavuse, kaasa arvatud õiguse saada tõhusat haldus- või õiguskaitset ja nõuda hüvitist liidus või kolmandas riigis. Kaitsemeetmed peaksid olema eelkõige seotud vastavusega üldistele isikuandmete töötlemise põhimõtetele ning lõimitud andmekaitse ja vaikimisi andmekaitse põhimõtetele. […]

(109) Vastutavale töötlejale või volitatud töötlejale antud võimalus kasutada komisjoni või järelevalveasutuse vastu võetud standardseid andmekaitseklausleid ei tohiks takistada vastutavat töötlejat või volitatud töötlejat lisamast standardsed andmekaitseklauslid laiemasse lepingusse, nagu näiteks kahe volitatud töötleja vahelisse lepingusse, ega lisamast muid klausleid või täiendavaid kaitsemeetmeid, tingimusel et need ei lähe otseselt ega kaudselt vastuollu komisjoni või järelevalveasutuse vastu võetud lepingu tüüptingimustega ega piira andmesubjektide põhiõigusi ja -vabadusi. Vastutavaid töötlejaid ja volitatud töötlejaid tuleks ergutada nägema ette täiendavaid kaitsemeetmeid lepinguliste kohustuste abil, mis täiendavad standardseid kaitseklausleid.

[…]

(114) Igal juhul, kui komisjon ei ole teinud otsust kolmanda riigi andmekaitse taseme piisavuse kohta, peaks vastutav töötleja või volitatud töötleja kasutama lahendusi, millega antakse andmesubjektidele neid puudutava töötlemise korral liidus kohtulikult kaitstavad ja tõhusad õigused pärast selliste andmete edastamist, mistõttu neil on jätkuvalt samad põhiõigused ja nende suhtes kohaldatakse samu kaitsemeetmeid.

[…]

(116) Isikuandmete liikumine üle piiride liidust välja võib raskendada füüsiliste isikute võimalusi kasutada õigust andmete kaitsele, eelkõige kaitsta end sellise teabe ebaseadusliku kasutamise ja avaldamise eest. Samal ajal võib järelevalveasutus sattuda olukorda, milles ta leiab, et ei suuda käsitleda kaebusi ega teostada uurimist väljapoole oma riigi piire jäävates küsimustes. Nende piiriülese koostöö püüdlusi võivad takistada ka tõkestamiseks ja kaitsemeetmete kehtestamiseks ebapiisavad volitused, ebaühtlane õiguskord ja praktilised tõkked, nagu piiratud vahendid. […]

[…]

(141) Igal andmesubjektil peaks olema õigus esitada kaebus ühele järelevalveasutusele, eelkõige liikmesriigis, kus on tema alaline elukoht, ja õigus tõhusale õiguskaitsevahendile kooskõlas harta artikliga 47, kui andmesubjekt on seisukohal, et tema käesoleva määruse kohaseid õigusi on rikutud või kui järelevalveasutus ei reageeri kaebusele, lükkab kaebuse osaliselt või täielikult tagasi või ei võta meetmeid juhul, kui need on vajalikud andmesubjekti õiguste kaitsmiseks. […]“.

9 Selle määruse artikli 2 lõigetes 1 ja 2 on ette nähtud:

„1. Käesolevat määrust kohaldatakse isikuandmete täielikult või osaliselt automatiseeritud töötlemise suhtes ja isikuandmete automatiseerimata töötlemise suhtes, kui kõnealused isikuandmed kuuluvad andmete kogumisse või kui need kavatsetakse andmete kogumisse kanda.

2. Käesolevat määrust ei kohaldata, kui:

a) isikuandmeid töödeldakse muu kui liidu õiguse kohaldamisalasse kuuluva tegevuse käigus;

b) liikmesriigid töötlevad isikuandmeid sellise tegevuse käigus, mis kuulub ELi lepingu V jaotise 2. peatüki kohaldamisalasse;

c) isikuandmeid töötleb füüsiline isik eranditult isiklike või koduste tegevuste käigus;

d) isikuandmeid töötlevad pädevad asutused süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil.“

10 Kõnealuse määruse artiklis 4 on sätestatud:

„Käesolevas määruses kasutatakse järgmisi mõisteid:

[…]

2) „isikuandmete töötlemine“ – isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine;

[…]

7) „vastutav töötleja“ – füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes üksi või koos teistega määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid; kui sellise töötlemise eesmärgid ja vahendid on kindlaks määratud liidu või liikmesriigi õigusega, võib vastutava töötleja või tema määramise konkreetsed kriteeriumid sätestada liidu või liikmesriigi õiguses;

8) „volitatud töötleja“ – füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes töötleb isikuandmeid vastutava töötleja nimel;

9) „vastuvõtja“ – füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kellele isikuandmed avaldatakse, olenemata sellest, kas tegemist on kolmanda isikuga või mitte. Vastuvõtjateks ei peeta siiski avaliku sektori asutusi, kes võivad kooskõlas liidu või liikmesriigi õigusega saada isikuandmeid seoses konkreetse päringuga; nimetatud avaliku sektori asutused töötlevad kõnealuseid isikuandmeid kooskõlas asjaomaste andmekaitsenormidega vastavalt töötlemise eesmärkidele;

[…]“.

11 Sama määruse artiklis 23 on kirjas:

„1. Vastutava töötleja või volitatud töötleja suhtes kohaldatavas liidu või liikmesriigi õiguses võib seadusandliku meetmega piirata artiklites 12–22 ja artiklis 34, samuti artiklis 5 sätestatud kohustuste ja õiguste ulatust, kuivõrd selle sätted vastavad artiklites 12–22 sätestatud õigustele ja kohustustele, kui selline piirang austab põhiõiguste ja -vabaduste olemust ning on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede, et tagada

a) riigi julgeolek;

b) riigikaitse;

c) avalik julgeolek;

d) süütegude tõkestamine, uurimine, avastamine ja nende eest vastutusele võtmine või kriminaalkaristuste täitmisele pööramine, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmine ja nende ennetamine;

[…]

2. Eelkõige peab lõikes 1 osutatud seadusandlik meede sisaldama asjakohasel juhul konkreetseid sätteid vähemalt järgmise kohta:

a) töötlemise või selle kategooriate eesmärgid;

b) isikuandmete liigid;

c) kehtestatud piirangute ulatus;

d) kuritarvitamist või ebaseaduslikku andmetega tutvumist või nende edastamist tõkestavad kaitsemeetmed;

e) vastutava töötleja või vastutavate töötlejate kategooriate määratlus;

f) säilitamise ajavahemikud ja kohaldatavad kaitsemeetmed, võttes arvesse töötlemise või selle kategooriate laadi, ulatust ja eesmärki;

g) andmesubjektide õigusi ja vabadusi ähvardavad ohud ning

h) andmesubjektide õigus olla piirangust teavitatud, välja arvatud juhul, kui see võib mõjutada piirangu eesmärki.“

12 Isikuandmete kaitse üldmääruse V peatükk „Isikuandmete edastamine kolmandatele riikidele ja rahvusvahelistele organisatsioonidele“ hõlmab selle määruse artikleid 44–50. Määruse artiklis 44 „Edastamise üldpõhimõtted“ on sätestatud:

„Töödeldavate või pärast kolmandale riigile või rahvusvahelisele organisatsioonile edastamist töötlemiseks ette nähtud isikuandmete edastamine toimub ainult juhul, kui vastutav töötleja ja volitatud töötleja on täitnud kooskõlas käesoleva määruse teiste sätetega käesolevas peatükis sätestatud tingimused, sealhulgas juhul, kui kolmas riik või rahvusvaheline organisatsioon saadab isikuandmed edasi muule kolmandale riigile või rahvusvahelisele organisatsioonile. Kõiki käesoleva peatüki sätteid kohaldatakse selleks, et tagada, et käesoleva määrusega tagatud füüsiliste isikute kaitse taset ei kahjustata.“

13 Määruse artikli 45 „Edastamine kaitse piisavuse otsuse alusel“ lõigetes 1–3 on ette nähtud:

„1. Isikuandmeid võib kolmandale riigile või rahvusvahelisele organisatsioonile edastada siis, kui komisjon on teinud otsuse, et asjaomane kolmas riik või asjaomase kolmanda riigi territoorium või kõnealuse kolmanda riigi üks või mitu kindlaksmääratud sektorit või rahvusvaheline organisatsioon tagab isikuandmete kaitse piisava taseme. Selliseks edastamiseks ei ole vaja eriluba.

2. Isikuandmete kaitse taseme piisavuse hindamisel võtab komisjon eelkõige arvesse järgmisi asjaolusid:

a) õigusriigi põhimõte, inimõiguste ja põhivabaduste austamine, asjaomased õigusaktid, nii üldised kui ka valdkondlikud, sealhulgas õigusaktid, mis käsitlevad avalikku julgeolekut, kaitset, riiklikku julgeolekut, karistusõigust ja riigiasutuste juurdepääsu isikuandmetele, ning selliste õigusaktide, andmekaitsenormide, ametieeskirjade ja turvameetmete (sealhulgas eeskirjad isikuandmete edasisaatmise kohta teisele kolmandale riigile või rahvusvahelisele organisatsioonile, mida kõnealune kolmas riik või rahvusvaheline organisatsioon täidab) rakendamine, kohtupraktikast tulenevad nõuded ning andmesubjektide tõhusate ja kohtulikult kaitstavate õiguste ja tõhusa haldus- ja õiguskaitse olemasolu andmesubjektide jaoks, kelle isikuandmeid edastatakse;

b) ühe või mitme sellise sõltumatu järelevalveasutuse olemasolu ja tõhus toimimine asjaomases kolmandas riigis või kellele rahvusvaheline organisatsioon allub, kes vastutab andmekaitsenormide järgimise ja nende täitmise tagamise eest, sealhulgas piisavate täitmise tagamise volituste eest, andmesubjektide abistamise ja nõustamise eest nende õiguste teostamisel ning liikmesriikide järelevalveasutustega tehtava koostöö eest, ning

c) asjaomase kolmanda riigi või rahvusvahelise organisatsiooni rahvusvahelised kohustused või muud kohustused, mis tulenevad õiguslikult siduvatest konventsioonidest või õigusaktidest või selle kolmanda riigi või rahvusvahelise organisatsiooni osalemisest mitmepoolsetes või piirkondlikes süsteemides, eelkõige seoses isikuandmete kaitsega.

3. Komisjon võib pärast kaitse taseme piisavuse hindamist võtta rakendusaktiga vastu otsuse, et kolmas riik või kolmanda riigi territoorium või kolmanda riigi üks või mitu kindlaksmääratud sektorit või rahvusvaheline organisatsioon tagab isikuandmete kaitse piisava taseme käesoleva artikli lõike 2 tähenduses. Rakendusaktis nähakse ette korrapärase, vähemalt iga nelja aasta tagant toimuva läbivaatamise mehhanism, milles võetakse arvesse kõiki asjaomaseid suundumusi kolmandas riigis või rahvusvahelises organisatsioonis. Rakendusaktis määratakse kindlaks selle territoriaalne ja valdkondlik

kohaldatavus ning vajaduse korral käesoleva artikli lõike 2 punktis b osutatud järelevalveasutus või -asutused. Kõnealune rakendusakt võetakse vastu kooskõlas artikli 93 lõikes 2 osutatud kontrollimenetlusega.“

14 Sama määruse artikli 46 „Edastamine asjakohaste kaitsemeetmete kohaldamisel“ lõigetes 1–3 on sätestatud:

„1. Artikli 45 lõike 3 kohase otsuse puudumisel võib vastutav töötleja või volitatud töötleja edastada isikuandmeid kolmandale riigile või rahvusvahelisele organisatsioonile üksnes juhul, kui vastutav töötleja või volitatud töötleja on sätestanud asjakohased kaitsemeetmed ning tingimusel, et andmesubjektide kohtulikult kaitstavad õigused ja tõhusad õiguskaitsevahendid on kättesaadavad.

2. Lõikes 1 osutatud asjakohased kaitsemeetmed võib ilma järelevalveasutuselt mingit eriluba taotlemata ette näha:

a) õiguslikult siduva ja täitmisele pööratava dokumendiga avaliku sektori asutuste või organite vahel;

b) siduvate kontsernisiseste eeskirjadega vastavalt artiklile 47;

c) komisjoni poolt artikli 93 lõikes 2 osutatud kontrollimenetluse kohaselt vastu võetud standardsete andmekaitseklauslitega;

d) järelevalveasutuse poolt vastu võetud ja komisjoni poolt artikli 93 lõikes 2 osutatud kontrollimenetluse kohaselt heaks kiidetud standardsete andmekaitseklauslitega;

e) artikli 40 kohase heakskiidetud toimimisjuhendiga, koos kolmanda riigi vastutava töötleja või volitatud töötleja siduvate ja täitmisele pööratavate kohustustega kehtestada asjakohased kaitsemeetmed, sealhulgas andmesubjekti õiguste osas, või

f) artikli 42 kohase heakskiidetud sertifitseerimismehhanismiga, koos kolmanda riigi vastutava töötleja või volitatud töötleja siduvate ja täitmisele pööratavate kohustustega kehtestada asjakohased kaitsemeetmed, sealhulgas andmesubjekti õiguste osas.

3. Pädeva järelevalveasutuse loal võib lõikes 1 osutatud asjakohased kaitsemeetmed sätestada ka eelkõige

a) vastutava töötleja või volitatud töötleja ning kolmanda riigi või rahvusvahelise organisatsiooni vastutava töötleja või volitatud töötleja või isikuandmete vastuvõtja vaheliste lepingutingimustega või

b) sätetega, mis tuleb lisada avaliku sektori asutuste või organite vahelistesse halduskokkulepetesse ning mis hõlmavad andmesubjektide kohtulikult kaitstavaid ja tõhusaid õigusi.“

15 Sama määruse artiklis 49 „Erandid konkreetsetes olukordades“ on sätestatud:

„1. Artikli 45 lõike 3 kohase kaitse piisavuse otsuse või artikli 46 kohaste asjakohaste kaitsemeetmete, sealhulgas siduvate kontsernisiseste eeskirjade puudumise korral võib kolmandale riigile või rahvusvahelisele organisatsioonile isikuandmete ühekordne või korduv edastamine olla lubatud ainult ühel järgmistest tingimustest:

a) andmesubjekt on edastamiseks andnud selgesõnalise nõusoleku pärast seda, kui teda teavitati sellise edastamisega tema jaoks kaasnevatest võimalikest ohtudest, mis tulenevad kaitse piisavuse otsuse ja asjaomaste kaitsemeetmete puudumisest;

b) edastamine on vajalik andmesubjekti ja vastutava töötleja vahelise lepingu täitmiseks või andmesubjekti taotluse alusel võetavate lepingueelsete meetmete rakendamiseks;

c) edastamine on vajalik, et andmesubjekti huvides sõlmida vastutava töötleja ja muu füüsilise või juriidilise isiku vahel leping või seda lepingut täita;

d) edastamine on vajalik avalikust huvist tulenevatel kaalukatel põhjustel;

e) edastamine on vajalik õigusnõuete koostamiseks, esitamiseks või kaitsmiseks;

f) edastamine on vajalik, et kaitsta andmesubjekti või muude isikute olulisi huve, kui andmesubjekt on füüsiliselt või õiguslikult võimetu nõusolekut andma;

g) edastamine tehakse registrist, mis liidu või liikmesriigi õiguse kohaselt on mõeldud avalikkuse teavitamiseks ja on tutvumiseks avatud kas laiemale avalikkusele või kõigile, kes suudavad tõendada õigustatud huvi, kuid ainult sellisel määral, nagu konkreetsel juhul on täidetud tutvumist käsitlevad tingimused, mis on liidu või liikmesriigi õigusega ette nähtud.

Kui edastamise aluseks ei saa olla artikli 45 või 46 sätted, sealhulgas siduvaid kontsernisiseseid eeskirju käsitlevad sätted, ning kui ükski käesoleva lõike esimese lõigu kohane konkreetseks olukorraks ette nähtud erand ei ole kohaldatav, võib kolmandale riigile või rahvusvahelisele organisatsioonile andmeid edastada üksnes juhul, kui edastamine ei ole korduv, puudutab ainult piiratud arvu andmesubjekte, on vajalik, et kaitsta vastutava töötleja õigustatud huve, mille suhtes andmesubjekti huvid, õigused või vabadused ei ole ülekaalus ning kui vastutav töötleja on hinnanud kõiki andmete edastamisega seotud asjaolusid ja kehtestanud selle hinnangu põhjal sobivad kaitsemeetmed isikuandmete kaitseks. Vastutav töötleja teatab edastamisest järelevalveasutusele. Lisaks artiklites 13 ja 14 osutatud teabele teavitab vastutav töötleja andmesubjekte edastamisest ja vastutava töötleja poolt kaitstavatest õigustatud huvidest.

2. Lõike 1 esimese lõigu punkti g kohane edastamine ei hõlma kõiki registris sisalduvaid isikuandmeid ega kõiki isikuandmete liike. Kui register on ette nähtud tutvumiseks õigustatud huviga isikutele, toimub edastamine vaid nende isikute taotlusel või juhul, kui nemad on vastuvõtjad.

3. Lõike 1 esimese lõigu punkte a, b ja c ning lõike 1 teist lõiku ei kohaldata avalikku võimu teostavate riigiasutuste toimingute suhtes.

4. Lõike 1 esimese lõigu punktis d osutatud avalik huvi on tunnustatud liidu õiguses või selle liikmesriigi õiguses, mida vastutava töötaja suhtes kohaldatakse.

5. Kaitse piisavuse otsuse puudumise korral võib avalikust huvist tulenevatel kaalukatel põhjustel liidu või liikmesriigi õigusega selgesõnaliselt seada piirangud eri liiki isikuandmete edastamiseks kolmandale riigile või rahvusvahelisele organisatsioonile. Liikmesriigid teatavad sellistest sätetest komisjonile.

6. Vastutav töötleja või volitatud töötleja kannab artiklis 30 osutatud registrisse hindamise ja käesoleva artikli lõike 1 teises lõigus osutatud sobivad kaitsemeetmed.“

16 Isikuandmete kaitse üldmääruse artikli 51 lõige 1 on sõnastatud järgmiselt:

„Liikmesriik näeb ette ühe või mitu sõltumatut riigiasutust, kes vastutavad käesoleva määruse kohaldamise järelevalve eest, et kaitsta füüsiliste isikute põhiõigusi ja -vabadusi seoses nende isikuandmete töötlemisega ning hõlbustada isikuandmete vaba liikumist liidus („järelevalveasutus“).“

17 Määruse artikli 55 lõikes 1 on kirjas, et „[j]ärelevalveasutus on oma liikmesriigi territooriumil pädev täitma ülesandeid ja kasutama volitusi, mis on talle kooskõlas käesoleva määrusega antud“.

18 Määruse artikli 57 lõikes 1 on ette nähtud:

„Ilma et see piiraks muude käesoleva määrusega sätestatud ülesannete täitmist, teeb järelevalveasutus oma territooriumil järgmist:

a) jälgib käesoleva määruse kohaldamist ja tagab selle kohaldamise;

[…]

f) käsitleb andmesubjekti […] esitatud kaebusi, uurib asjakohasel määral kaebuste sisu ning teavitab kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest, eelkõige juhul, kui on vajalik täiendav uurimine või kooskõlastamine teise järelevalveasutusega;

[…]“.

19 Sama määruse artikli 58 lõigetes 2 ja 4 on sätestatud:

„2. Järelevalveasutusel on järgmised parandusvolitused:

[…]

f) kehtestada ajutine või alaline isikuandmete töötlemise piirang, sealhulgas töötlemiskeeld;

[…]

j) anda korraldus peatada kolmandas riigis asuvale vastuvõtjale või rahvusvahelisele organisatsioonile suunatud andmevoog.

[…]

4. Järelevalveasutusele käesoleva artikli kohaselt antud volituste kasutamisele kohaldatakse asjakohaseid kaitsemeetmeid, sealhulgas tõhusat õiguskaitsevahendit ja nõuetekohast menetlust, mis on sätestatud liidu ja liikmesriigi õiguses kooskõlas hartaga.“

20 Isikuandmete kaitse üldmääruse artikli 64 lõikes 2 on sätestatud:

„Pädev järelevalveasutus, [Euroopa] andmekaitsenõukogu eesistuja või komisjon võib taotleda mis tahes üldkohaldatava või rohkem kui ühes liikmesriigis mõju avaldava küsimuse puhul, et seda käsitleks arvamuse esitamiseks andmekaitsenõukogu, eelkõige juhul, kui pädev järelevalveasutus ei täida vastastikuse abi kohustust vastavalt artiklile 61 või ühisoperatsioonide kohustust vastavalt artiklile 62.“

21 Määruse artikli 65 lõige 1 on järgmine:

„Selleks et tagada käesoleva määruse nõuetekohane ja järjepidev kohaldamine üksikjuhtudel, võtab andmekaitsenõukogu vastu siduva otsuse järgmistel juhtudel:

[…]

c) kui pädev järelevalveasutus ei taotle andmekaitsenõukogu arvamust käesoleva artikli 64 lõikes 1 osutatud juhtudel või ei järgi andmekaitsenõukogu artikli 64 kohaselt esitatud arvamust. Sellisel juhul võib asjaomane järelevalveasutus või komisjon edastada küsimuse andmekaitsenõukogule.“

22 Nimetatud määruse artiklis 77 „Õigus esitada järelevalveasutusele kaebus“ on ette nähtud:

„1. Ilma et see piiraks muude halduslike või õiguslike kaitsevahendite kohaldamist, on igal andmesubjektil õigus esitada kaebus järelevalveasutusele, eelkõige liikmesriigis, kus on tema alaline elukoht, töökoht või väidetava rikkumise toimumiskoht, kui andmesubjekt on seisukohal, et teda puudutavate isikuandmete töötlemine rikub käesolevat määrust.

2. Järelevalveasutus, kellele kaebus esitatakse, teavitab kaebuse esitajat kaebuse menetlemise käigust ja tulemusest, sealhulgas artikli 78 kohasest õiguskaitsevahendi kasutamise võimalusest.“

23 Sama määruse artikli 78 „Õigus tõhusale õiguskaitsevahendile järelevalveasutuse vastu“ lõigetes 1 ja 2 on ette nähtud:

„1. Ilma et see piiraks muude halduslike kaitsevahendite või kohtuväliste heastamisvahendite kohaldamist, on igal füüsilisel või juriidilisel isikul õigus kasutada tõhusat õiguskaitsevahendit järelevalveasutuse õiguslikult siduva otsuse vastu, mis teda puudutab.

2. Ilma et see piiraks muude halduslike kaitsevahendite või kohtuväliste heastamisvahendite kohaldamist, on igal andmesubjektil õigus kasutada tõhusat õiguskaitsevahendit, kui artiklite 55 ja 56 kohaselt pädev järelevalveasutus ei käsitle kaebust või ei teavita andmesubjekti kolme kuu jooksul artikli 77 kohaselt esitatud kaebuse menetlemise käigust või tulemustest.“

24 Isikuandmete kaitse üldmääruse artiklis 94 on sätestatud:

„1. Direktiiv [95/46] tunnistatakse kehtetuks alates 25. maist 2018.

2. Viiteid kehtetuks tunnistatud direktiivile käsitatakse viidetena käesolevale määrusele. Viiteid direktiivi [95/46] artikli 29 alusel loodud töörühmale üksikisikute kaitseks seoses isikuandmete töötlemisega käsitatakse viidetena käesoleva määrusega loodud Euroopa Andmekaitsenõukogule.“

25 Kõnealuse määruse artiklis 99 on sätestatud:

„1. Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

2. Seda kohaldatakse alates 25. maist 2018.“

Tüüptingimuste otsus

26 Tüüptingimuste otsuse põhjendus 11 on sõnastatud järgmiselt:

„Liikmesriikide järelevalveasutused mängivad käesolevas lepingumehhanismis võtmerolli, et tagada isikuandmete piisav kaitse pärast edastamist. Erandjuhtumitel, kui andmeeksportijad keelduvad andmeimportijat korralikult juhendamast või ei saa seda teha, millega kaasneb ähvardav oht tõsise kahju tekkimiseks andmesubjektidele, peaksid lepingu tüüptingimused lubama järelevalveasutustel andmeimportijaid ja alamtöötlejaid kontrollida ning vajaduse korral andmeimportijatele ja alamtöötlejatele siduvaid otsuseid vastu võtta. Järelevalveasutustel peaks olema õigus keelata või peatada lepingu tüüptingimustel põhinev andmete edastamine või edastamistoimingute kogum sellisel erandjuhul, kui on kindlaks tehtud, et lepinguline edastamine võib tõenäoliselt omada olulist ebasoodsat mõju tagatistele ja kohustustele, mis sätestavad andmesubjekti piisava kaitse.“

27 Selle otsuse artiklis 1 on sätestatud:

„Lisas sätestatud lepingu tüüptingimusi käsitletakse piisavate tagatistena üksikisikute eraelu puutumatuse ning põhiõiguste ja -vabaduste kaitseks ning vastavate õiguste teostamiseks, nagu on nõutud direktiivi [95/46] artikli 26 lõikes 2.“

28 Selle otsuse artikli 2 teise lõigu kohaselt kehtib otsus „isikuandmete edastamise kohta Euroopa Liidus asuvatelt vastutavatelt töötlejatelt väljaspool Euroopa Liidu territooriumi asuvatele vastuvõtjatele, kes tegutsevad üksnes volitatud töötlejatena“.

29 Sama otsuse artiklis 3 on ette nähtud:

„Käesolevas otsuses kasutatakse järgmisi mõisteid:

[…]

c) andmeeksportija – vastutav töötleja, kes edastab isikuandmeid;

d) andmeimportija – kolmandas riigis asuv volitatud töötleja, kes nõustub võtma andmeeksportijalt vastu isikuandmeid, mis on mõeldud töötlemiseks pärast edastamist andmeeksportija nimel ja kooskõlas tema juhiste ja käesoleva otsuse tingimustega ning kelle kohta ei kehti piisavat kaitset tagav kolmanda riigi süsteem direktiivi [95/46] artikli 25 lõike 1 tähenduses;

[…]

f) kohaldatav andmekaitseseadus – õigusakt, mis kaitseb üksikisikute põhiõigusi ja -vabadusi ning eriti nende eraelu puutumatuse õigust seoses isikuandmete töötlemisega ning mis on kohaldatav vastutava andmetöötleja suhtes liikmesriigis, kus andmeeksportija asub;

[…]“.

30 Tüüptingimuste otsuse artikkel 4 nägi enne rakendusotsuse 2016/2297 jõustumist kehtinud algses redaktsioonis ette:

„1. Ilma et see piiraks nende volitusi võtta meetmeid tagamaks vastavust siseriiklikele õigusnormidele, mis on vastu võetud direktiivi [95/46] II, III, V ja VI peatüki kohaselt, võivad liikmesriikide pädevad organid kasutada neil olemasolevaid volitusi keelata või peatada andmete liikumine kolmandatesse riikidesse, et kaitsta üksikisikuid seoses nende isikuandmete töötlemisega juhul, kui:

a) on kindlaks tehtud, et andmeimportija või alamtöötleja kohta kehtiv seadus kehtestab talle nõudeid kalduda kõrvale kohaldatavast andmekaitseseadusest, et kõnealused nõuded lähevad kaugemale direktiivi [95/46] artiklis 13 sätestatud demokraatlikus ühiskonnas vajalikest piirangutest ja et need nõuded võivad tõenäoliselt omada olulist ebasoodsat mõju kohaldatava andmekaitseseaduse ja lepingu tüüptingimustega ettenähtud tagatistele või

b) pädev organ on kindlaks teinud, et andmeimportija või alamtöötleja ei ole järginud lisas sätestatud lepingu tüüptingimusi või

c) on olemas oluline tõenäosus, et lisas esitatud lepingu tüüptingimusi ei järgita ning et jätkuv edastamine looks ähvardava ohu tõsise kahju tekkimiseks andmesubjektidele.

2. Keelamine või peatamine vastavalt lõikele 1 tühistatakse kohe, kui keelamise või peatamise põhjusi enam pole.

3. Kui liikmesriigid võtavad meetmeid vastavalt lõikele 1 ja 2, peavad nad neist meetmetest viivitamata teatama komisjonile, kes edastab saadud teabe teistele liikmesriikidele.“

31 6. oktoobri 2015. aasta kohtuotsuse Schrems (C-362/14, EU:C:2015:650) kuulutamise järel vastu võetud rakendusotsuse 2016/2297 põhjendus 5 on sõnastatud järgmiselt:

„Vastavalt direktiivi [95/46] artikli 26 lõikele 4 vastu võetud komisjoni otsus on *mutatis mutandis* siduv kõikide otsuse adressaadiks olevate liikmesriikide organitele, kaasa arvatud nende sõltumatutele järelevalveasutustele, kui sellega tunnistatakse, et kõnealuses artiklis sätestatud lepingu tüüptingimuste alusel tehtavad ülekanded pakuvad piisavat kaitset kõnealuse direktiivi artikli 26 lõike 2 tähenduses. See ei takista riiklikul järelevalveasutusel oma volituste teostamist, et jälgida andmevooge, kaasa arvatud õigust peatada või keelustada isikuandmete edastamine, kui viimane otsustab, et edastamine viiakse läbi ELi või riikliku andmekaitse seadust rikkudes, nagu näiteks juhul, kui andmete importija ei täida lepingu tüüptingimusi.“

32 Tüüptingimuste otsuse artikkel 4 on rakendusotsusega 2016/2297 muutmise järel nüüd sõnastatud järgmiselt:

„Kui liikmesriikide pädevad ametiasutused kasutavad [direktiivi 95/46] artikli 28 lõike 3 kohaseid volitusi, mille tulemusena katkestatakse ajutiselt või alaliselt andmevoogude edastamine kolmandatele riikidele, et tagada üksikisikute kaitse seoses nende isikuandmete töötlemisega, teavitab asjaomane liikmesriik sellest viivitamatult komisjoni, kes edastab teabe teistele liikmesriikidele.“

33 Tüüptingimuste otsuse lisas pealkirjaga „Lepingu tüüptingimused (töötlejad)“ on 12 tüüptingimust. 3. tingimus „Soodustatud kolmandat isikut käsitlev tingimus“ on järgmine:

„1. Andmesubjekt saab soodustatud kolmanda isikuna andmeeksportija vastu jõustada käesolevat tingimust, 4. tingimuse punkte b–i, 5. tingimuse punkte a–e ja g–j, 6. tingimuse lõikeid 1 ja 2, 7. tingimust, 8. tingimuse lõiget 2 ning 9.–12. tingimust.

2. Andmesubjekt saab andmeeksportija vastu jõustada käesolevat tingimust, 5. tingimuse punkte a–e ja g, 6. tingimust, 7. tingimust, 8. tingimuse lõiget 2 ning 9.–12. tingimust juhul, kui andmeeksportija on teadaolevalt kadunud või on oma seadusjärgse tegevuse lõpetanud, ning välja arvatud juhul, kui õigusjärglane on andmeeksportija kõik juriidilised kohustused üle võtnud lepingu või õigustoimingu alusel, mille tulemusel ta hakkab täitma andmeeksportija õigusi ja kohustusi, mistõttu võib andmesubjekt eespool loetletud tingimusi jõustada nimetatud õigusjärglase vastu.

[…]“.

34 Vastavalt selle lisa 4. tingimusele „Andmeeksportija kohustused“:

„Andmeeksportija nõustub järgnevaga ja kinnitab, et:

a) isikuandmete töötlemine, sealhulgas edastamine, on toimunud ja toimub ka tulevikus kooskõlas kohaldatava andmekaitseseaduse asjaomaste sätetega (ja et vajaduse korral on sellest teavitatud asjaomaseid asutusi liikmesriigis, kus andmeeksportija asub) ega riku asjaomase riigi vastavaid sätteid;

b) ta on juhtinud ja juhib kogu isikuandmete töötlemise teenuse osutamise kestel andmeimportija tähelepanu sellele, et viimati nimetatud töötleks edastatud isikuandmeid üksnes andmeeksportija nimel ja kooskõlas kohaldatava andmekaitseseaduse ja käesolevate tingimustega;

[…]

f) kui edastatakse eriliiki kuuluvaid andmeid, on andmesubjekti teavitatud või seda tehakse kas enne või võimalikult kiiresti pärast edastamist asjaolust, et tema andmed võidakse edastada kolmandasse riiki, milles ei kehti piisavat kaitset tagav süsteem direktiivi [95/46] tähenduses;

g) et ta edastab vastavalt 5. tingimuse punktile b ja 8. tingimuse lõikele 3 kõik andmeimportijalt ja kõigilt alamtöötlejatelt saadud teated andmekaitseasutusele, kui andmeeksportija otsustab edastamist jätkata või tühistada andmete edastamise peatamise;

[…]“.

35 Nimetatud lisa 5. tingimuses „Andmeimportija kohustused“ on ette nähtud:

„Andmeimportija nõustub järgnevaga ja kinnitab, et:

a) ta töötleb isikuandmeid üksnes andmeeksportija nimel ning kooskõlas tema juhiste ja tingimustega. Kui ta ei suuda sellist kooskõla ükskõik millistel põhjustel tagada, nõustub ta sellest viivitamata teatama andmeeksportijale, kellel on sellisel juhul õigus andmete edastamine peatada ja/või leping lõpetada;

b) tal ei ole põhjust uskuda, et tema suhtes kohaldatav õigus takistaks tal täita andmeeksportijalt saadud suuniseid ja importijale lepingust tulenevaid kohustusi ning et asjaomastes õigusaktides tehtavate selliste muudatuste korral, mis tõenäoliselt mõjutavad tingimustest tulenevaid tagatisi ja kohustusi negatiivselt, teatab ta muudatustest teada saades neist viivitamata andmeeksportijale, kellel on sellisel juhul õigus andmete edastamine peatada ja/või leping lõpetada;

[…]

d) ta teatab andmeeksportijale viivitamata järgmistest asjaoludest:
   i) õiguskaitseorganite õiguslikult siduvad taotlused isikuandmete avaldamiseks, välja arvatud taotluste avaldamise keelu korral, mis tuleneb näiteks kriminaalõigusest ja mille eesmärk on kaitsta õiguskaitsealase uurimistoimingu konfidentsiaalsust;
   ii) juhusliku ja volitamata juurdepääsu juhtumid ning
   iii) otse andmesubjektidelt saadud taotlused, millele ta ei vasta, välja arvatud juhul, kui talle on antud õigus sellistele taotlustele vastata;

[…]“.

36 Joonealuses märkuses, millele 5. tingimuse pealkirjas on viidatud, on märgitud:

„Andmeimportija kohta kehtivate siseriiklike õigusaktide kohustuslikud nõuded, mis ei lähe kaugemale demokraatlikus ühiskonnas vajalikest eranditest ja piirangutest direktiivi [95/46] artikli 13 lõikes 1 loetletud huvide alusel, ei ole lepingu tüüptingimustega vastuolus, kui nad sätestavad vajaliku meetme, et tagada riigi julgeolek ja riigikaitse, avalik kord, kuritegude või reguleeritud kutsealade ametieetika rikkumiste ennetamine, uurimine, avastamine ja nende eest vastutusele võtmine, riigi oluline majanduslik või rahanduslik huvi või andmesubjekti kaitse või teiste isikute vabaduste ja õiguste kaitse. […]“.

37 Tüüptingimuste otsuse lisa 6. tingimuses „Vastutus“ on ette nähtud:

„1. Pooled lepivad kokku, et kõigil andmesubjektidel, kes on kandnud kahju ükskõik millise poole või alamtöötleja poolt toimepandud 3. või 11. tingimuse mis tahes rikkumise tulemusena, on õigus saada kantud kahju eest hüvitist andmeeksportijalt.

2. Kui andmesubjektil ei ole võimalik nõuda andmeimportija või tema alamtöötleja poolt toimepandud 3. või 11. tingimuses viidatud kohustuste mis tahes rikkumisega seotud ja käesoleva tingimuse lõikes 1 nimetatud hüvitist andmeeksportijalt, kuna andmeeksportija on teadaolevalt kadunud või on oma seadusjärgse tegevuse lõpetanud või on maksejõuetuks muutunud, nõustub andmeimportija, et andmesubjekt võib nõuda hüvitist temalt kui andmeeksportija asendajalt […].

[…]“.

38 Selle lisa 8. tingimuse „Koostöö järelevalveasutustega“ lõikes 2 on sätestatud:

„Pooled lepivad kokku, et järelevalveasutusel on õigus andmeimportijat ja kõiki alamtöötlejaid auditeerida samas ulatuses ja samadel tingimustel, kui tal on kohaldatava andmekaitseseaduse alusel õigus auditeerida andmeeksportijat.“

39 Nimetatud lisa 9. tingimuses „Kohaldatav õigus“ on sätestatud, et tingimusi reguleeritakse selle liikmesriigi õigusega, kus andmeeksportija asub.

40 Sama lisa 11. tingimuses „Alamtöötlemine“ on ette nähtud:

„1. Andmeimportija ei anna andmeeksportija nimel vastavalt käesolevatele tingimustele teostatavaid töötlustoiminguid edasi andmeeksportija eelneva kirjaliku nõusolekuta. Kui andmeimportija annab andmeeksportija nõusolekul oma käesolevatest tingimustest tulenevad kohustused edasi, teeb ta seda ainult alamtöötlejaga sõlmitava kirjaliku lepinguga, millega pannakse alamtöötlejale samad kohustused, mis on käesolevate tingimustega pandud andmeimportijale. […]

2. Eelnevasse andmeimportija ja alamtöötleja kirjalikku lepingusse lisatakse ka 3. tingimuses käsitletud soodustatud kolmanda isiku säte juhuks, kui andmesubjektil ei ole võimalik 6. tingimuse lõikes 1 nimetatud hüvitist nõuda andmeeksportijalt või andmeimportijalt, kuna nad on teadaolevalt kadunud või on oma seadusjärgse tegevuse lõpetanud või on maksejõuetuks muutunud ja kui ükski õigusjärglane ei ole andmeeksportija ega andmeimportija kõiki juriidilisi kohustusi üle võtnud lepingu või õigustoimingu alusel. Alamtöötleja vastutus kolmanda isiku ees on piiratud käesolevates tingimustes sätestatud töötlustoimingutega.

[…]“.

41 Tüüptingimuste otsuse lisa 12. tingimuse „Isikuandmete töötlusteenuste lõpetamise järgsed kohustused“ lõikes 1 on sätestatud:

„Pooled lepivad kokku, et andmetöötlusteenuste pakkumise lõpetamisel tagastavad andmeimportija ja alamtöötleja andmeeksportija soovil viimati nimetatule kõik edastatud isikuandmed ja nendest tehtud koopiad või hävitavad kõik isikuandmed ja kinnitavad andmeeksportijale kirjalikult, et nad on seda teinud, välja arvatud juhul, kui andmeimportija suhtes kohaldatavad õigusaktid takistavad tal kõiki edastatud isikuandmeid või osa neist tagastada või hävitada. […]“.

Privacy Shieldi otsus

42 Euroopa Kohus tunnistas 6. oktoobri 2015. aasta otsusega Schrems (C-362/14, EU:C:2015:650) kehtetuks komisjoni 26. juuli 2000. aasta otsuse 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 (ELT 2000, L 215, lk 7), milles komisjon oli tuvastanud, et nimetatud kolmas riik tagab piisava kaitse taseme.

43 Selle kohtuotsuse kuulutamise järel võttis komisjon vastu Privacy Shieldi otsuse, olles enne selle otsuse vastuvõtmist ette valmistades hinnanud USA õigusakte, nagu on mainitud selle otsuse põhjenduses 65:

„Euroopa Komisjon on hinnanud piiranguid ja kaitsemeetmeid, mis on sätestatud USA õiguses seoses ELi-USA andmekaitseraamistiku Privacy Shield alusel edastatud isikuandmetele juurdepääsu ja nende kasutamisega USA avaliku sektori asutuste poolt riikliku julgeoleku, õiguskaitse ja muu avaliku huvi eesmärgil. Lisaks on USA valitsus esitanud riigi luuredirektori büroo (Office of the Director of National Intelligence, edaspidi „ODNI“) […] kaudu Euroopa Komisjonile üksikasjalikud kinnitused ja kohustused, mis on ära toodud käesoleva otsuse VI lisas. USA välisministri allkirjaga kirjas, mis on esitatud otsuse III lisas, on USA valitsus võtnud ka kohustuse luua uus riikliku julgeolekuga seotud sekkumiste järelevalve mehhanism, nimelt andmekaitseraamistiku Privacy Shield ombudsman, kes on USA luureühendusest sõltumatu. Lõpuks on USA justiitsministeeriumi kinnituses, mis on esitatud käesoleva otsuse VII lisas, kirjeldatud piiranguid ja kaitsemeetmeid seoses isikuandmetele juurdepääsu ja nende kasutamisega avaliku sektori asutuste poolt õiguskaitse ja muudel avaliku huvi eesmärkidel. Läbipaistvuse suurendamiseks ja nimetatud kohustuste õigusliku siduvuse väljendamiseks avaldatakse kõik need eespool loetletud ja käesolevale otsusele lisatud dokumendid USA ametlikus teatajas *Federal Register*.“

44 Komisjoni analüüs nende piirangute ja kaitsemeetmete kohta on kokku võetud Privacy Shieldi otsuse põhjendustes 67–135, samas kui komisjoni järeldus ELi-USA andmekaitseraamistikuga Privacy Shield tagatud kaitse taseme piisavuse kohta on toodud selle otsuse põhjendustes 136–141.

45 Täpsemalt on selle otsuse põhjendustes 68, 69, 76, 77, 109, 112–116, 120, 136 ja 140 märgitud:

„(68) Vastavalt USA konstitutsioonile kuulub riikliku julgeoleku tagamine presidendi pädevusse, kes on relvajõudude ülemjuhataja, täitevvõimu juht ja kes korraldab USA välissuhtlust välisluure valdkonnas […]. Kuigi kongressi pädevuses on kehtestada piiranguid ja ta on seda mitmes aspektis ka teinud, saab president nimetatud piires juhtida USA luureühenduse tööd, kasutades selleks eelkõige korraldusi või presidendi suuniseid. […] Selle valdkonna kaks keskset õigusakti on praegu korraldus (Executive Order) 12333 (edaspidi „E.O. 12333“) […] ja presidendi poliitikasuunis (Presidential Policy Directive) nr 28.

(69) Presidendi 17. jaanuari 2014. aasta poliitikasuunisega nr 28 (edaspidi „PPD-28“) on kehtestatud mitmed nn signaaliluurega seotud piirangud […]. See presidendi suunis on USA luureasutustele siduv […] ja jääb kehtima kuni USA valitsuse vahetumiseni […]. PPD-28 on eriti oluline USA-välist päritolu isikutele, sealhulgas ELi andmesubjektidele. […]

[…]

(76) Kuigi [suunises PPD-28] kasutatavad juriidilised mõisted on erinevad, vastavad need põhimõtted sisuliselt vajalikkuse ja proportsionaalsuse põhimõtetele. […]

(77) Kuna suunise on välja andnud president kui täitevvõimu juht, on need nõuded siduvad kogu luureühendusele ning neid on hiljem rakendatud asutusesiseste eeskirjade ja menetlustega, millega on üldpõhimõtted teisendatud konkreetseteks igapäevatöö juhisteks. […]

[…]

(109) Seevastu [Foreign Intelligence Surveillance Act'i (FISA)] paragrahvi 702 puhul ei anna [United States Foreign Intelligence Surveillance Court (FISC) (USA välisluure jälgimise kohus)] luba üksikuteks jälgimismeetmeteks; selle asemel annab ta load jälgimisprogrammide jaoks (nt PRISM, UPSTREAM) vastavalt iga-aastastele vastavuskinnitustele, mille koostavad [United States Attorney General (USA peaprokurör)] ja [Director of National Intelligence (DNI) (riigi luuredirektor)]. […] Nagu märgitud, ei sisalda FISC heakskiidetavad kinnitused teavet

sihtmärgiks võetavate konkreetsete isikute kohta, vaid neis määratletakse pigem välisluureinfo kategooriad […]. Kuigi FISC ei hinda (ei eeldatava põhjuse järgi ega mõnel muul alusel) seda, kas isikud on välisluureinfo kogumise sihtmärgiks valitud õigesti, […] on tal õigus kontrollida tingimust, et „kogumise oluliseks eesmärgiks on saada välisluureinfot“. […]

[…]

(112) Esiteks pakub [FISA] mitmeid USA-välistele isikutele kättesaadavaid õiguskaitsevahendeid ebaseaduslikku elektroonilise jälgimise vaidlustamiseks […]. Muu hulgas on üksikisikutel võimalik esitada Ameerika Ühendriikide vastu tsiviilhagi, kui nende kohta käivaid andmeid on ebaseaduslikult ja tahtlikult kasutatud või avaldatud, […] esitada (ametivolituste ületamise sätete alusel) rahalisi kahjunõudeid otse USA riigiametnike vastu […] ja vaidlustada jälgimise õiguspärasus (ning otsida võimalusi andmeid mitte avalikustada), kui USA valitsus kavatseb isiku elektroonilise jälgimise käigus kogutud andmeid või neist tuletatud teavet kasutada või avaldada USA kohtu- või haldusmenetluses […].

(113) Teiseks andis USA valitsus komisjonile viited mitmele muule võimalusele, mida ELi andmesubjektid saavad kasutada õiguskaitse hankimiseks riigiametnike vastu, juhul kui valitsusel on tema isikuandmetele juurdepääs või neid kavatsetakse kasutada ebaseaduslikult, sealhulgas väidetavalt riikliku julgeoleku huvides […].

(114) Peale selle on USA valitsus osutanud, et USA-välised isikud saavad [teabevabaduse seaduse (Freedom of Information Act (FOIA)] alusel taotleda juurdepääsu föderaalasutuste registritele, sealhulgas konkreetse isiku isikuandmeid sisaldavatele registritele […]. FOIA eesmärki arvestades ei paku see võimalust saada individuaalset õiguskaitset isikuandmete käsitlemise kui sellise vastu, ent võimaldab üksikisikutel põhimõtteliselt saada juurdepääsu riiklikes luureasutustes hoitavale asjakohasele teabele. […]

(115) Kuigi isikutele, sealhulgas ELi andmesubjektidele, keda on riikliku julgeoleku huvides ebaseaduslikult (elektrooniliselt) jälgitud, on saadaval erinevaid õiguskaitsevõimalusi, on samas selge, et vähemalt mõnesid USA luureametkondade kasutatavaid õiguslikke aluseid (nt korraldust E.O. 12333) need ei hõlma. Isegi kui kohtuliku kaitse võimalused USA-välistele isikutele on põhimõtteliselt olemas, näiteks FISA alusel toimuva jälgimise puhul, on õiguskaitsevahendite kasutamine piiratud […] ning üksikisikute (sh USA isikute) esitatavaid nõudeid ei võeta menetlusse, kui nad ei suuda tõendada „õigustatud huvi“, […] mistõttu tavakohtutele juurdepääs on piiratud […].

(116) Et luua veel üks kõikidele ELi andmesubjektidele kättesaadav õiguskaitsevõimalus, on USA valitsus otsustanud luua uue, ombudsmani mehhanismi, nagu on märgitud USA välisministri kirjas komisjonile, mis sisaldub käesoleva otsuse III lisas. See mehhanism põhineb PPD-28 kohasel välisministeeriumi juhtivkoordinaatori (asekantsleri tase) määramisel, kes on välisriikide valitsustele kontaktpunktiks USA signaaliluuretegevusega seotud probleemide tõstatamisel, kuid mehhanism pakub algsest kavandist tunduvalt rohkem lisavõimalusi.

[…]

(120) Teiseks kohustub USA valitsus tagama, et oma ametiülesannete täitmisel on raamistik Privacy Shield ombudsmanil võimalik toetuda koostööle muude USA seadusega ette nähtud järelevalve- ja nõuetele vastavuse mehhanismidele. […] Kui mõni neist järelevalveorganitest tuvastab nõuetele mittevastavuse, peab asjaomane luureühenduse liige (st luureasutus) mittevastavuse heastama, kuna ainult sellisel juhul on ombudsmanil võimalik anda üksikisikule „positiivne“ vastus (st mittevastavus on kõrvaldatud), milleks USA valitsus on kohustuse võtnud. […]

[…]

(136) Neid järeldusi arvestades leiab komisjon, et Ameerika Ühendriigid tagavad ELi-USA andmekaitseraamistiku Privacy Shield alusel piisava kaitsetaseme isikuandmetele, mis edastatakse liidust põhimõtete järgimist kinnitanud organisatsioonidele Ameerika Ühendriikides.

[…]

(140) Lisaks leiab komisjon USA õigussüsteemi kohta saada oleva teabe, sealhulgas USA valitsuse kinnituste ja kohustuste põhjal, et selliste isikute põhiõiguste riivamine Ameerika Ühendriikides riikliku julgeoleku, õiguskaitse või muu avaliku huvi eesmärgil, kelle isikuandmeid edastatakse liidust Ameerika Ühendriikidesse, ja põhimõtete järgimist kinnitanud organisatsioonidele sellest tulenevalt kehtivad piirangud eraelu puutumatuse põhimõtete järgimisel, piirduvad asjaomase seadusliku eesmärgi saavutamiseks rangelt vajalikuga ning tagatud on tõhus õiguskaitse selliste riive vastu.“

46 Privacy Shieldi otsuse artikkel 1 on sõnastatud järgmiselt:

„1. Ameerika Ühendriigid tagavad ELi-USA andmekaitseraamistiku Privacy Shield alusel direktiivi [95/46] artikli 25 lõike 2 tähenduses piisava kaitsetaseme isikuandmetele, mis edastatakse liidust Ameerika Ühendriikides asuvatele organisatsioonidele.

2. ELi-USA andmekaitseraamistik Privacy Shield koosneb 7. juulil 2016 Ameerika Ühendriikide kaubandusministeeriumi poolt välja antud põhimõtetest, mis on esitatud II lisas, ning ametlikest kinnitustest ja kohustustest, mis on esitatud I ja III–VII lisas loetletud dokumentides.

3. Lõike 1 kohaldamisel edastatakse isikuandmed ELi-USA andmekaitseraamistiku Privacy Shield raames juhul, kui need edastatakse liidust Ameerika Ühendriikides asuvatele organisatsioonidele, mis kuuluvad Privacy Shieldi nimekirja, mida haldab ja mille teeb avalikkusele kättesaadavaks Ameerika Ühendriikide kaubandusministeerium kooskõlas II lisas esitatud põhimõtete I ja III jaoga.“

47 Privacy Shieldi otsuse II lisa „[Ameerika Ühendriikide kaubandusministeeriumi poolt välja antud] ELi-USA andmekaitseraamistiku Privacy Shield põhimõtted […]“ punktis I.5. on ette nähtud, et nende põhimõtete järgimist võib piirata „riikliku julgeoleku, avaliku huvi või õiguskaitseliste vajaduste täitmiseks“.

48 Selle otsuse III lisas on USA toonase Secretary of State (riigisekretär) John Kerry 7. juuli 2016. aasta kiri Euroopa Komisjoni õigus- ja tarbijaküsimuste ning soolise võrdõiguslikkuse volinikule, millele A lisana on lisatud memorandum „ELi-USA andmekaitseraamistiku Privacy Shield ombudsmani mehhanism signaaliluure kohta“, milles on järgmine lõik:

„Tunnustades ELi-USA andmekaitseraamistiku Privacy Shield tähtsust, käivitab käesolev memorandum protsessi uue, dokumendiga „Presidential Policy Directive 28“ (PPD-28) kooskõlas oleva signaaliluure mehhanismi rakendamise.

[…] President Obama andis teada uue presidendi poliitikasuunise PPD-28 väljaandmisest, mille eesmärgiks on „näha selgelt ette, mida me teeme ja mida ei tee, kui asi puudutab meie luuretegevust ookeani taga.“

PPD-28 jagu 4(d) kohustab riigisekretäri määrama rahvusvahelise infotehnoloogiaalase diplomaatia vanemkoordinaatori (vanemkoordinaator) „kes … oleks kontaktisikuks välisriikide valitsuste jaoks, kes soovivad väljendada muret USA signaaliluurealase tegevuse kohta“.

[…]

1. [Vanemkoordinaator] hakkab täitma andmekaitseraamistiku Privacy Shield ombudsmani kohustusi ning […] hakkab tööle tihedas koostöös asjakohaste ametnikega teistest ministeeriumitest ja asutustest, kelle ülesandeks on taotluste menetlemine kooskõlas kohaldatava Ameerika Ühendriikide õiguse ja normidega. Ombudsman on luureühendusest sõltumatu. Ombudsman allub otse riigisekretärile, kes tagab, et ombudsman täidab oma kohustusi objektiivselt ning väärmõjudeta, mis võiksid tema antavaid otsuseid mõjutada.

[…]“.

49 Privacy Shieldi otsuse VI lisas on Office of the Director of National Intelligence (USA riigi luuredirektori büroo) 21. juuni 2016. aasta kiri USA kaubandusministeeriumile ja väliskaubandusametile, milles on selgitatud, et suunis PPD-28 võimaldab teabe laiaulatuslikku kogumist, st „suhteliselt suure koguse signaaliluure teel kogutava teabe või andmete omandamist tingimustel, kus luureühendusel ei ole võimalik otsingu täpsustamiseks kasutada midagi, mille abil identifitseerida konkreetseid objekte“.

Põhikohtuasi ja eelotsuse küsimused

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

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

52 M. Schrems esitas 25. juunil 2013 andmekaitsevolinikule kaebuse, milles ta sisuliselt palus, et viimane keelaks Facebook Irelandil tema isikuandmeid Ameerika Ühendriikidesse edastada, põhjendades oma palvet väitega, et selles riigis kehtiv õigus ja valitsev praktika ei taga selle territooriumil säilitatavate isikuandmete piisavat kaitset sealsete avaliku võimu asutuste jälgimise eest. See kaebus jäeti rahuldamata eelkõige põhjendusega, et komisjon oli otsuses 2000/520 tõdenud, et USA tagab kaitse piisava taseme.

53 High Court (kõrge kohus, Iirimaa), kuhu M. Schrems kaebuse rahuldamata jätmise otsuse edasikaebamiseks pöördus, esitas Euroopa Kohtule eelotsusetaotluse otsuse 2000/520 tõlgendamise ja kehtivuse kohta. Euroopa Kohus tunnistas 6. oktoobri 2015. aasta otsusega Schrems (C-362/14, EU:C:2015:650) selle otsuse kehtetuks.

54 Sellest kohtuotsusest lähtudes tühistas eelotsusetaotluse esitanud kohus M. Schremsi kaebuse rahuldamata jätmise otsuse ning saatis kaebuse andmekaitsevolinikule tagasi. Andmekaitsevoliniku alustatud menetluses selgitas Facebook Ireland, et suur osa isikuandmeid edastatakse Facebook Inc-le tüüptingimuste otsuse lisas olevate andmekaitse tüüptingimuste alusel. Neid asjaolusid arvestades palus andmekaitsevolinik M. Schremsil oma kaebus ümber sõnastada.

55 Vastavalt ümbersõnastatud kaebuses, mis esitati 1. detsembril 2015, väitis M. Schrems eelkõige, et USA õiguse kohaselt on Facebook Inc-l kohustus teha talle edastatud isikuandmed kättesaadavaks USA asutustele nagu National Security Agency (NSA) ja Federal Bureau of Investigation (FBI). Ta väitis, et kuna neid andmeid kasutatakse eri jälgimisprogrammides viisil, mis ei ole kooskõlas harta artiklitega 7, 8 ja 47, ei saa tüüptingimuste otsus õigustada kõnealuste andmete USAsse edastamist. Neil asjaoludel palus M. Schrems andmekaitsevolinikult, et viimane keelaks või peataks tema isikuandmete edastamise Facebook Inc-le.

56 Andmekaitsevolinik avaldas 24. mail 2016 otsuse eelnõu, milles võttis kokku uurimise esialgsed järeldused. Selles eelnõus väljendas ta esialgset seisukohta, et liidu kodanike isikuandmete USAsse edastamisel on oht, et USA asutused tutvuvad nendega ja töötlevad neid viisil, mis on vastuolus harta artiklitega 7 ja 8, ning USA õigus ei paku neile liidu kodanikele harta artikliga 47 kooskõlas olevaid õiguskaitsevahendeid. Andmekaitsevolinik leidis, et tüüptingimuste otsuse lisas sisalduvad andmekaitse tüüptingimused ei ole sobivad seda lünka täitma, sest need ei ole siduvad Ameerika asutustele, vaid annavad andmesubjektidele üksnes lepingust tulenevad õigused andmeeksportija ja/või -importija vastu.

57 Kuna andmekaitsevolinik leidis, et neil asjaoludel tõstatab M. Schremsi ümbersõnastatud kaebus tüüptingimuste otsuse kehtivuse küsimuse, pöördus ta 6. oktoobri 2015. aasta kohtuotsusest Schrems (C-362/14, EU:C:2015:650, punkt 65) tulenevale kohtupraktikale tuginedes 31. mail 2016 High Courti (kõrge kohus), et viimane esitaks selle küsimuse Euroopa Kohtule. High Court (kõrge kohus) esitas 4. mai 2018. aasta otsusega Euroopa Kohtule eelotsusetaotluse käesolevas asjas.

58 Eelotsusetaotlusele lisas High Court (kõrge kohus) 3. oktoobri 2017. aasta kohtuotsuse, millesse ta oli talletanud talle riigisiseses kohtumenetluses – milles osales ka USA valitsus – esitatud tõendite hindamise tulemused.

59 Selles kohtuotsuses, millele eelotsusetaotluses on mitu korda viidatud, tõi eelotsusetaotluse esitanud kohus esile, et põhimõtteliselt ei ole tal mitte ainult õigus, vaid ka kohustus hinnata kõiki talle esitatud faktilisi asjaolusid ja argumente kogumis, selleks et ta saaks nende põhjal otsustada, kas eelotsust on vaja taotleda või mitte. Igal juhul peab ta arvesse võtma muudatusi, mis õigusaktidesse võib olla tehtud kaebuse esitamise ja tema korraldatud kohtuistungi toimumise vahelisel ajal. Nimetatud kohus täpsustas, et põhikohtuasja menetluses ei ole tema hinnang piiratud andmekaitsevoliniku esitatud väidetega kehtetuse kohta, vaid ta võib omal algatusel tõstatada kehtetuse kohta ka muid väiteid ja nende põhjal esitada eelotsusetaotluse.

60 Nimetatud kohtuotsuses on tuvastatud, et USAsse edastatud isikuandmete puhul on USA asutuste luuretegevuse aluseks eelkõige FISA artikkel 702 ja korraldus E.O. 12333.

61 FISA artikli 702 kohta täpsustab eelotsusetaotluse esitanud kohus samas kohtuotsuses, et see artikkel võimaldab peaprokuröril ja riigi luuredirektoril anda ühiselt, pärast FISC-lt heakskiidu saamist, „välisluureteabe“ hankimise eesmärgil loa jälgida isikuid, kes ei ole USA kodanikud ja kes viibivad väljaspool USA territooriumi, ning täpsemalt on see artikkel jälgimisprogrammide PRISM ja UPSTREAM aluseks. Eelotsusetaotluse esitanud kohus on tuvastanud, et programmi PRISM raames peavad internetiteenuse osutajad tegema NSA-le kättesaadavaks kõik nn selektori saadetud ja vastuvõetud sõnumid, millest osa edastatakse FBI-le ja Central Intelligence Agencyle (CIA) (Luure Keskagentuur).

62 Programmi UPSTREAM kohta tuvastas eelotsusetaotluse esitanud kohus, et selle programmi raames on interneti tuumvõrku – ehk kaablite, kommutaatorite ja ruuterite võrku – käitavad elektroonilise side ettevõtjad kohustatud võimaldama NSA-l kopeerida ja filtreerida interneti liiklusvoogusid selleks, et saada kätte nn selektori poolt välja valitud USA-välise kodaniku saadetud või vastu võetud või seda kodanikku puudutavad sõnumid. Eelotsusetaotluse esitanud kohtu tuvastatu kohaselt on NSA-l selle programmi raames juurdepääs nii sõnumite metaandmetele kui ka sisule.

63 Korralduse E.O. 12333 kohta tuvastas eelotsusetaotluse esitanud kohus, et see võimaldab NSA-l pääseda Atlandi ookeani põhjas olevate merealuste kaablite kaudu juurde USAsse liikuvatele andmetele ning koguda ja salvestada neid andmeid enne, kui need jõuavad USAsse, kus nende suhtes kuuluvad kohaldamisele FISA sätted. Ta täpsustab, et korralduse E.O. 12333 alusel toimuv tegevus ei ole seadusega reguleeritud.

64 Luureteabe kogumise toimingutele seatud piiride kohta rõhutab eelotsusetaotluse esitanud kohus, et USA-väliste isikute suhtes on kohaldatav ainult suunis PPD-28, mis piirdub sätestamisega, et teabe kogumise toimingud peavad olema „võimalikult täpselt määratletud“ (*as tailored as feasible*). Nende tuvastatud asjaolude pinnalt leiab nimetatud kohus, et USA tegeleb andmete masstöötlusega, tagamata seejuures kaitset, mis oleks sisuliselt samaväärne harta artiklitega 7 ja 8 tagatud kaitsega.

65 Kohtuliku kaitse kohta märgib nimetatud kohus, et liidu kodanikel ei ole võimalik kasutada USA kodanikega samu õiguskaitsevahendeid, juhul kui USA asutused nende isikuandmeid töötlevad, sest USA õiguse kõige olulisem õigusvastase jälgimise vastane kaitsemeede, st USA põhiseaduse (Constitution of the United States) neljas parandus, ei ole kohaldatav liidu kodanike suhtes. Eelotsusetaotluse esitanud kohus täpsustab sellega seoses, et liidu kodanikele jäävate õiguskaitsevahendite kasutamine võib olla seotud märkimisväärsete takistuste ületamisega, näiteks on neil enda kaebeõiguse tõendamise kohustus, mis nimetatud kohtu hinnangul on liiga raskesti täidetav. Lisaks sellele on eelotsusetaotluse esitanud kohus tuvastanud, et korralduse E.O. 12333 alusel toimuva NSA tegevuse üle ei toimu mingisugust kohtulikku eelkontrolli ja selle peale ei saa kohtule kaebust esitada. Viimaks leiab nimetatud kohus, et kuna tema hinnangul ei ole andmekaitseraamistiku Privacy Shield ombudsman käsitatav kohtuna harta artikli 47 tähenduses, ei taga Ameerika õigus liidu kodanikele kaitse taset, mis oleks sisuliselt samaväärne selle artikliga tagatud põhiõigusest tuleneva kaitsega.

66 Eelotsusetaotluse esitanud kohus täpsustab eelotsusetaotluses veel, et põhikohtuasja pooled on eri meelt muu hulgas küsimuses, kas liidu õigus on kohaldatav olukorras, kus isikuandmeid edastatakse kolmandasse riiki, kus selle riigi ametiasutused võivad neid töödelda eelkõige riikliku julgeolekuga seotud eesmärkidel, ning samuti küsimuses, milliseid asjaolusid tuleb arvesse võtta, et hinnata, kas selle riigi tagatud kaitse tase on piisav. Täpsemalt märgib nimetatud kohus, et Facebook Ireland on seisukohal, et kui komisjon on Privacy Shieldi otsuses tuvastanud, et kolmanda riigi pakutava kaitse tase on piisav, on tema tuvastatu järelevalveasutustele siduv ka juhul, kui tegemist on isikuandmete edastamisega tüüptingimuste otsuse lisas sisalduvate andmekaitse tüüptingimuste alusel.

67 Andmekaitse tüüptingimustega seoses on eelotsusetaotluse esitanud kohtul tekkinud küsimus, kas tüüptingimuste otsust saab lugeda kehtivaks, samas kui – sama kohtu hinnangul – need tingimused ei ole kõnealuse kolmanda riigi riigiasutuste jaoks siduvad ega saa seega korvata asjaolu, et selles riigis ei ole kaitse tase piisav. Sellega seoses leiab ta, et rakendusotsuse 2016/2297 jõustumisele eelnenud redaktsioonis kehtinud tüüptingimuste otsuse artikli 4 lõike 1 punktis a liikmesriikide pädevatele asutustele antud võimalus keelata isikuandmete edastamine sellisesse kolmandasse riiki, kes paneb importijale tüüptingimustes sisalduvate tagatistega vastuolus olevad kohustused, annab tunnistustust sellest, et kolmandas riigis valitsev õiguslik olukord võib olla põhjuseks, miks keelata andmete edastamine isegi juhul, kui see toimub tüüptingimuste otsuse lisas sisalduvate andmekaitse tüüptingimuste alusel, ja toob ilmsiks, et nendest tingimustest võib piisava kaitse tagamiseks väheks jääda. Samas on eelotsusetaotluse esitanud kohtul küsimus selle kohta, kui ulatuslik on andmekaitsevoliniku pädevus keelata nende tüüptingimuste alusel toimuv andmete edastamine, ning ta leiab, et kaalutlusõigusest ei tarvitse küllaldase kaitse tagamiseks piisata.

68 Neil asjaoludel otsustas High Court (kõrge kohus) menetluse peatada ja esitada Euroopa Kohtule järgmised eelotsuse küsimused:

„1. Kas olukorras, kus eraõiguslik äriühing edastab kooskõlas [tüüptingimuste otsusega] [liidu] liikmesriigist ärilisel eesmärgil isikuandmeid eraõiguslikule äriühingule kolmandas riigis ja neid andmeid võivad selles kolmandas riigis edaspidi töödelda selle riigi ametiasutused nii riikliku julgeolekuga kui ka avaliku korra tagamise ja selle kolmanda riigi välisasjade ajamisega seotud eesmärkidel, on liidu õigusnormid, sealhulgas harta, selle andmete edastamise suhtes kohaldatavad, olenemata ELL artikli 4 lõike 2 sätetest, mis käsitlevad riigi julgeolekut, ja [direktiivi 95/46] artikli 3 lõike 2 esimese taande sätetest, mis käsitlevad avalikku korda, riigikaitset ja riigi julgeolekut?

2. a) Kas selleks, et tuvastada, kas üksikisiku õigusi on rikutud [tüüptingimuste otsuse] kohaselt andmete edastamisega liidust kolmandasse riiki, kus neid võidakse edaspidi töödelda riikliku julgeolekuga seotud eesmärkidel, on direktiivi [95/46] kohaldamisel asjakohane võrdlusalus:
   i) harta, EL leping, EL toimimise leping, direktiiv [95/46], [Roomas 4. novembril 1950 allkirjastatud Euroopa inimõiguste ja põhivabaduste kaitse konventsioon] (või muu [liidu] õiguse säte) või
   ii) ühe või mitme liikmesriigi riigisisesed õigusaktid?
   b) Kas juhul, kui asjakohane võrdlusalus on punkt ii, tuleb võrdlusalusesse arvata ka riikliku julgeolekuga seotud tegevus ühes või mitmes liikmesriigis?

3. Kas selleks, et hinnata, kas kolmas riik tagab sellesse riiki edastatud isikuandmete liidu õigusega nõutava kaitse taseme direktiivi [95/46] artikli 26 tähenduses, tuleb lähtuda:
   a) selles kolmandas riigis kohaldatavatest normidest, mis tulenevad tema riigisisesest õigusest või rahvusvahelistest kohustustest ja praktikast, mille eesmärk on tagada nende normide järgimine, sealhulgas erialastest normidest ja turvameetmetest, mida selles kolmandas riigis täidetakse

   või
   b) punktis a viidatud normidest koostoimes selles kolmandas riigis sisse seatud haldus-, reguleerimis- ja täitmispraktikaga ning kohtuväliste kaitsemeetmete, menetluste, protokollide, järelevalvemehhanismide ja õiguskaitsevahenditega?

4. Kas High Courti (kõrge kohus) poolt USA õiguse kohta tuvastatud faktilisi asjaolusid arvestades rikutakse liidust [tüüptingimuste otsuse] kohaselt USAsse isikuandmete edastamise korral isikutele harta artiklitest 7 ja/või 8 tulenevaid õigusi?

5. Kas arvestades faktilisi asjaolusid, mis High Court (kõrge kohus) on USA õiguse kohta tuvastanud, kui liidust edastatakse tüüptingimuste otsuse kohaselt USAsse isikuandmeid,
   a) on USAs võimaldatava kaitse tase kooskõlas isikule harta artikliga 47 tagatud õiguse pöörduda kohtusse olemusega, kui on rikutud tema õigust andmete konfidentsiaalsusele?

   Juhul, kui vastus viienda küsimuse punktile a on jaatav:
   b) kas USA riikliku julgeoleku kontekstis on USA õiguses kehtestatud piirangud isiku õigusele kohtusse pöörduda harta artikli 52 tähenduses proportsionaalsed ega lähe kaugemale, kui on demokraatlikus ühiskonnas riikliku julgeoleku eesmärgil vajalik?

6. a) Millisel tasemel tuleb kaitsta isikuandmeid, mis edastatakse kolmandasse riiki vastavalt lepingu tüüptingimustele, mis on vastu võetud kooskõlas komisjoni otsusega [direktiivi 95/46] artikli 26 lõike 4 alusel, arvestades [direktiivi 95/46] sätteid ja eeskätt artikleid 25 ja 26, tõlgendatuna lähtuvalt hartast?
   b) Milliseid asjaolusid tuleb arvesse võtta selle hindamisel, kas kolmandasse riiki tüüptingimuste otsuse kohaselt edastatavate andmete kaitse tase vastab direktiivi [95/46] ja harta nõuetele?

7. Kas asjaolu, et andmeeksportija ja andmeimportija vahel kehtivad lepingu tüüptingimused ei ole siduvad kolmanda riigi ametiasutustele, kes võivad kohustada andmeimportijat avaldama [tüüptingimuste otsuses] ette nähtud tingimuste kohaselt edastatud isikuandmeid oma julgeolekuteenistustele edasiseks töötlemiseks, välistab selle, et need tingimused pakuvad selliseid piisavaid kaitsemeetmeid, mis on ette nähtud direktiivi [95/46] artikli 26 lõikes 2?

8. Kas juhul, kui kolmandas riigis asuva andmeimportija suhtes kehtivad järelevalveseadused on andmekaitseasutuse arvates vastuolus tüüptingimuste otsuse lisas sisalduvate tüüptingimustega või direktiivi [95/46] artikliga 25 või 26 ja/või hartaga, on andmekaitseasutus kohustatud kasutama direktiivi [95/46] artikli 28 lõikest 3 tulenevaid sekkumisvolitusi andmevoogude peatamiseks või

on nende volituste kasutamine piiratud üksnes erandjuhtudega, võttes arvesse [tüüptingimuste otsuse] põhjendust 11, või saab andmekaitseasutus oma kaalutlusõiguse alusel otsustada jätta andmevood peatamata?

9. a) Kas [Privacy Shieldi] otsus kujutab endast üldkehtivat, liikmesriikide andmekaitseasutustele ja kohtutele direktiivi [95/46] artikli 25 lõike 6 tähenduses siduvat järeldust, et USA tagab oma riigisisese õiguse või võetud rahvusvaheliste kohustuste kaudu kaitse piisava taseme direktiivi [95/46] artikli 25 lõike 2 mõttes?
   b) Kui ta seda ei taga, siis kuidas on [Privacy Shieldi] otsus, kui üldse, asjakohane hinnangu andmisel USAsse tüüptingimuste otsuse kohaselt edastatud andmete suhtes võetud kaitsemeetmete piisavuse kohta?

10. Kui võtta arvesse High Courti (kõrge kohus) järeldusi seoses USA õigusega, siis kas [Privacy Shieldi] otsuse III lisasse kuuluva A lisa kohaselt andmekaitseraamistiku Privacy Shield ombudsmani määramine koostoimes USAs kehtiva korraga tagab selle, et USA võimaldab isikutele, kelle isikuandmeid [tüüptingimuste otsuse] kohaselt USAsse edastatakse, harta artiklile 47 vastava õiguskaitsevahendi?

11. Kas [tüüptingimuste otsus] rikub harta artikleid 7, 8 ja/või 47?“

Eelotsusetaotluse vastuvõetavus

69 Facebook Ireland ning Saksamaa ja Ühendkuningriigi valitsus väidavad, et eelotsusetaotlus on vastuvõetamatu.

70 Facebook Irelandi esitatud vastuvõetamatuse vastuväite kohaselt tunnistati need direktiivi 95/46 sätted, millel eelotsuse küsimused põhinevad, isikuandmete kaitse üldmäärusega kehtetuks.

71 Sellega seoses olgu märgitud, et kuigi on tõsi, et direktiiv 95/46 tunnistati isikuandmete kaitse üldmääruse artikli 94 lõikega 1 alates 25. maist 2018 kehtetuks, oli see käesoleva eelotsusetaotluse vormistamise ajal 4. mail 2018 ja Euroopa Kohtusse saabumise ajal 9. mail 2018 endiselt jõus. Peale selle on direktiivi 95/46 artikli 3 lõike 2 esimene taane, artiklid 25 ja 26 ning artikli 28 lõige 3, millele eelotsuse küsimustes viidatakse, sisuliselt üle võetud isikuandmete kaitse üldmääruse vastavatesse artiklitesse: artikli 2 lõikesse 2 ning artiklitesse 45, 46 ja 58. Lisaks tuleb märkida, et Euroopa Kohtu ülesanne on tõlgendada kõiki liidu õiguse sätteid, mida liikmesriigi kohtud vajavad oma menetluses olevate kohtuasjade lahendamiseks, isegi kui need kohtud ei ole selliseid sätteid Euroopa Kohtule esitatud küsimustes otseselt maininud (2. aprilli 2020. aasta kohtuotsus Ruska Federacija, C-897/19 PPU, EU:C:2020:262, punkt 43 ja seal viidatud kohtupraktika). Neil põhjustel ei saa asjaolu, et eelotsusetaotluse esitanud kohus on eelotsuse küsimuste sõnastamisel viidanud ainult direktiivi 95/46 sätetele, tuua kaasa käesoleva eelotsusetaotluse vastuvõetamatust.

72 Saksamaa valitsus omalt poolt põhjendab oma vastuvõetamatuse vastuväidet asjaoluga, et esiteks on andmekaitsevolinik väljendanud ainult kahtlusi, kuid mitte lõplikku arvamust tüüptingimuste otsuse kehtivuse küsimuses, ja teiseks on eelotsusetaotluse esitanud kohus jätnud kontrollimata, kas M. Schrems on vaieldamatult andnud põhikohtuasjas kõne all olevaks andmeedastuseks oma nõusoleku, mis juhul oleks sellele küsimusele vastamine tarbetu. Viimaks väidab Ühendkuningriigi valitsus, et eelotsuse küsimused on hüpoteetilised, sest see kohus ei ole tuvastanud, et need isikuandmed tegelikult selle otsuse alusel edastati.

73 Euroopa Kohtu väljakujunenud praktika järgi on üksnes asja menetleva ja selle lahendamise eest vastutava liikmesriigi kohtu ülesanne kohtuasja eripära arvesse võttes hinnata nii eelotsusetaotluse vajalikkust asjas otsuse langetamiseks kui ka Euroopa Kohtule esitatavate küsimuste asjakohasust. Seega, kui küsimused on esitatud liidu õigusnormi tõlgendamise või kehtivuse kohta, on Euroopa

Kohus üldjuhul kohustatud vastama. Sellest järeldub, et eeldatakse, et liidu õigust puudutavad küsimused on asjakohased. Liikmesriigi kohtu esitatud eelotsusetaotluse võib Euroopa Kohus jätta läbi vaatamata vaid siis, kui ilmneb, et tõlgendamine, mida liikmesriigi kohus palub, ei ole mingil viisil seotud põhikohtuasja faktiliste asjaolude või esemega, või ka juhul, kui probleem on hüpoteetiline või kui Euroopa Kohtule ei ole teada faktilised või õiguslikud asjaolud, mis on vajalikud esitatud küsimustele tarviliku vastuse andmiseks (16. juuni 2015. aasta kohtuotsus Gauweiler jt, C-62/14, EU:C:2015:400, punktid 24 ja 25; 2. oktoobri 2018. aasta kohtuotsus Ministerio Fiscal, C-207/16, EU:C:2018:788, punkt 45, ning 19. detsembri 2019. aasta kohtuotsus Dobersberger, C-16/18, EU:C:2019:1110, punktid 18 ja 19).

74 Käesoleval juhul sisaldab eelotsusetaotlus piisavaid faktilisi ja õiguslikke asjaolusid, et eelotsuse küsimuste ulatus oleks mõistetav. Peale selle tuleb märkida, et ennekõike ei võimalda ükski Euroopa Kohtu käsutuses olevas toimikus sisalduv asjaolu järeldada, et liidu õiguse tõlgendamine, mida palutakse, ei ole seotud põhikohtuasja faktiliste asjaolude või esemega või on hüpoteetiline näiteks põhjusel, et põhikohtuasjas vaidluse all olev isikuandmete edastamine põhineb andmesubjekti sõnaselgel nõusolekul, mitte tüüptingimuste otsusel. Eelotsusetaotluses esitatud selgituste kohaselt on Facebook Ireland nimelt möönnud, et ta edastab liidus elavate kasutajate isikuandmed Facebook Inc-le ja suur osa nendest – M. Schremsi väitel õigusvastastest – edastamistest toimub tüüptingimuste otsuse lisas sisalduvate andmekaitse tüüptingimuste alusel.

75 Käesoleva eelotsusetaotluse vastuvõetavuse seisukohalt ei ole tähtsust ka asjaolul, et andmekaitsevolinik ei ole selle otsuse kehtivuse kohta esitanud oma lõplikku arvamust, sest eelotsusetaotluse esitanud kohus on seisukohal, et vastus liidu õigusnormide tõlgendamist ja kehtivust puudutavatele eelotsuse küsimustele on põhikohtuasjas toimuva vaidluse lahendamiseks vajalik.

76 Sellest järeldub, et eelotsusetaotlus on vastuvõetav.

Eelotsuse küsimuste analüüs

77 Sissejuhatuseks tuleb märkida, et käesolev eelotsusetaotlus sai alguse kaebusest, milles M. Schrems palus andmekaitsevolinikul kohustada Facebook Irelandi peatama tema isikuandmete edastamine Facebook Inc-le või keelata tal edaspidi neid andmeid edastada. Olgugi et eelotsuse küsimused viitavad direktiivi 95/46 sätetele, on teada, et hetkeks, mil see direktiiv isikuandmete kaitse üldmäärusega alates 25. maist 2018 kehtetuks tunnistati ja asendati, ei olnud andmekaitsevolinik selle kaebuse kohta veel lõplikku otsust teinud.

78 See riigisisese otsuse puudumine eristab põhikohtuasjas käsitletavat olukorda olukordadest, milles tehti 24. septembri 2019. aasta kohtuotsus Google (linkide eemaldamise territoriaalne ulatus) (C-507/17, EU:C:2019:772) ja 1. oktoobri 2019. aasta kohtuotsus Planet49 (C-673/17, EU:C:2019:801), milles olid kõne all enne selle direktiivi kehtetuks tunnistamist vastu võetud otsused.

79 Seega tuleb eelotsuse küsimustele vastata isikuandmete kaitse üldmääruse, mitte direktiivi 95/46 sätete alusel.

Esimene küsimus

80 Esimese küsimusega palub eelotsusetaotluse esitanud kohus sisuliselt selgitada, kas isikuandmete kaitse üldmääruse artikli 2 lõiget 1 ning artikli 2 lõike 2 punkte a, b ja d koostoimes ELL artikli 4 lõikega 2 tuleb tõlgendada nii, et üldmääruse kohaldamisalasse kuulub olukord, kus liikmesriigis asuv äriühing edastab isikuandmeid kolmandas riigis asuvale teisele äriühingule ja edastamise käigus või järel võivad neid andmeid selles kolmandas riigis töödelda selle riigi ametiasutused avaliku korra, riigikaitse ja riikliku julgeoleku eesmärkidel.

81 Selle kohta tuleb kõigepealt märkida, et ELL artikli 4 lõikes 2 sisalduv säte, mille kohaselt liidus jääb riigi julgeolek iga liikmesriigi ainuvastutusse, puudutab ainult liidu liikmesriike. Järelikult ei ole käesoleval juhul see säte isikuandmete kaitse üldmääruse artikli 2 lõike 1 ja artikli 2 lõike 2 punktide a, b ja d tõlgendamisel asjakohane.

82 Isikuandmete kaitse üldmääruse artikli 2 lõike 1 kohaselt kohaldatakse seda määrust isikuandmete täielikult või osaliselt automatiseeritud töötlemise suhtes ja isikuandmete automatiseerimata töötlemise suhtes, kui kõnealused isikuandmed kuuluvad kataloogi või kui need kavatsetakse sellesse kanda. Selle määruse artikli 4 punktis 2 on mõiste „isikuandmete töötlemine“ määratletud kui „isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum“ ning näitena on toodud „edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine“, ilma et vahet oleks tehtud sellel, kas need toimingud tehakse liidu sees või on need seotud kolmanda riigiga. Lisaks on selles määruses juhuks, kui isikuandmeid edastatakse kolmandatele riikidele, kehtestatud erinormid, mis on koondatud V peatükki „Isikuandmete edastamine kolmandatele riikidele ja rahvusvahelistele organisatsioonidele“, ja sellega seoses on järelevalveasutustele sama määruse artikli 58 lõike 2 punktis j antud erivolitused.

83 Sellest järeldub, et toiming, mis seisneb isikuandmete edastamises liikmesriigist kolmandasse riiki, on juba iseenesest isikuandmete kaitse üldmääruse artikli 4 punkti 2 tähenduses isikuandmete töötlemine, mis toimub liikmesriigi territooriumil ja millele see määrus on tulenevalt selle artikli 2 lõikest 1 kohaldatav (vt analoogia alusel direktiivi 95/46 artikli 2 punkti b ja artikli 3 lõike 1 kohta 6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, EU:C:2015:650, punkt 45 ja seal viidatud kohtupraktika).

84 Seoses küsimusega, kas sellist toimingut saab tulenevalt isikuandmete kaitse üldmääruse artikli 2 lõikest 2 pidada selle määruse kohaldamisalast välja jäävaks, tuleb märkida, et see säte näeb ette erandid, mis ei kuulu selle määruse kohaldamisalasse, mis on määratletud selle määruse artikli 2 lõikes 1, ja neid erandeid tuleb tõlgendada kitsalt (vt analoogia alusel direktiivi 95/46 artikli 3 lõike 2 kohta 10. juuli 2018. aasta kohtuotsus Jehovan todistajat, C-25/17, EU:C:2018:551, punkt 37 ja seal viidatud kohtupraktika).

85 Kuna käesoleval juhul toimub põhikohtuasjas kõne all olev isikuandmete edastamine Facebook Irelandilt Facebook Inc-le, st kahe juriidilise isiku vahel, ei kuulu see edastamine isikuandmete kaitse üldmääruse artikli 2 lõike 2 punkti c alla, mis reguleerib isikuandmete töötlemist füüsilise isiku poolt eranditult isiklike või koduste tegevuste käigus. See edastamine ei ole hõlmatud ka määruse artikli 2 lõike 2 punktides a, b ja d loetletud eranditega, sest nendes punktides näitena mainitud tegevused kujutavad endast igal juhul toiminguid, mis on omased riigile või riigiasutustele ega ole omased eraõiguslike isikute tegevusvaldkondadele (vt analoogia alusel direktiivi 95/46 artikli 3 lõike 2 kohta 10. juuli 2018. aasta kohtuotsus Jehovan todistajat, C-25/17, EU:C:2018:551, punkt 38 ja seal viidatud kohtupraktika).

86 Samas ei saa võimalus, et kahe äriühingu vahel ärilisel eesmärgil edastatavaid isikuandmeid töötlevad edastamise käigus või järel kolmanda riigi ametiasutused avaliku korra, riigikaitse ja riikliku julgeoleku eesmärkidel, seda edastamist isikuandmete kaitse üldmääruse kohaldamisalast välja jätta.

87 Juba selle määruse artikli 45 lõike 2 punkti a sõnastusest, mis paneb komisjonile sõnaselgelt kohustuse võtta kolmandas riigis tagatud kaitse taseme piisavuse hindamisel eelkõige arvesse selliseid asjaolusid nagu „asjaomased õigusaktid, nii üldised kui ka valdkondlikud, sealhulgas õigusaktid, mis käsitlevad avalikku julgeolekut, kaitset, riiklikku julgeolekut, karistusõigust ja riigiasutuste juurdepääsu isikuandmetele, ning selliste õigusaktide […] rakendamine“, ilmneb, et asjaolu, et kolmandas riigis võidakse kõnealuseid andmeid töödelda avaliku korra, riigikaitse ja riikliku julgeolekuga seotud eesmärkidel, ei sea kahtluse alla selle määruse kohaldatavust kõnealusele edastamisele.

88 Sellest järeldub, et selline edastamine ei tohiks isikuandmete kaitse üldmääruse kohaldamisalast välja jääda põhjusel, et edastamise käigus või järel võivad kõnealuseid andmeid töödelda asjaomase kolmanda riigi ametiasutused avaliku korra, riigikaitse ja riikliku julgeolekuga seotud eesmärkidel.

89 Seetõttu tuleb esimesele küsimusele vastata, et isikuandmete kaitse üldmääruse artikli 2 lõikeid 1 ja 2 tuleb tõlgendada nii, et üldmääruse kohaldamisalasse kuulub olukord, kus liikmesriigis asuv äriühing edastab ärilisel eesmärgil isikuandmeid kolmandas riigis asuvale teisele äriühingule, olenemata asjaolust, et edastamise käigus või järel võivad kõnealuseid andmeid töödelda asjaomase kolmanda riigi ametiasutused avaliku korra, riigikaitse ja riikliku julgeolekuga seotud eesmärkidel.

Teine, kolmas ja kuues küsimus

90 Teise, kolmanda ja kuuenda küsimusega palub eelotsusetaotluse esitanud kohus Euroopa Kohtul sisuliselt selgitada, milline kaitse tase on isikuandmete kaitse üldmääruse artikli 46 lõike 1 ja artikli 46 lõike 2 punkti c kohaselt nõutav juhul, kui isikuandmeid edastatakse kolmandasse riiki andmekaitse tüüptingimuste alusel. Täpsemalt palub see kohus Euroopa Kohtul selgitada, milliseid asjaolusid tuleb arvesse võtta, et teha kindlaks, kas see kaitse tase on sellise edastamise korral tagatud.

91 Kaitse taseme kohta tuleneb nende sätete koostoimest, et selle määruse artikli 45 lõike 3 kohase kaitse piisavuse otsuse puudumisel võib vastutav töötleja või volitatud töötleja edastada isikuandmeid kolmandasse riiki või rahvusvahelisele organisatsioonile üksnes juhul, kui ta on ette näinud „asjakohased kaitsemeetmed“, ning tingimusel, et andmesubjektidele on kättesaadavad „kohtulikult kaitstavad õigused ja tõhusad õiguskaitsevahendid“, mis muu hulgas võivad olla ette nähtud komisjoni vastu võetud andmekaitse tüüptingimustega.

92 Kuigi isikuandmete kaitse üldmääruse artiklis 46 ei ole täpsustatud, millised nõuded tulenevad selles sättes mainitud „asjakohastest kaitsemeetmetest“, „kohtulikult kaitstavatest õigustest“ ja „tõhusatest õiguskaitsevahenditest“, tuleb silmas pidada, et see artikkel paikneb määruse V peatükis ja seetõttu tuleb seda artiklit tõlgendada lähtuvalt nimetatud määruse artiklist 44 „Edastamise üldpõhimõtted“, milles on sätestatud, et „[k]õiki [selle] peatüki sätteid kohaldatakse selleks, et tagada, et [sama] määrusega tagatud füüsiliste isikute kaitse taset ei kahjustata“. Kaitse tase peab seega olema tagatud olenemata sellest, millise selles peatükis sisalduva sätte alusel isikuandmeid kolmandasse riiki edastatakse.

93 Nagu tõi esile kohtujurist oma ettepaneku punktis 117, soovitakse isikuandmete kaitse üldmääruse V peatüki sätetega vastavalt selle määruse põhjenduses 6 osutatud eesmärgile nimelt kindlustada isikuandmete kõrgetasemelise kaitse järjepidevus andmete edastamise korral kolmandasse riiki.

94 Isikuandmete kaitse üldmääruse artikli 45 lõike 1 esimeses lauses on ette nähtud, et loa isikuandmete edastamiseks kolmandasse riiki võib anda komisjoni otsusega, milles leitakse, et asjaomane kolmas riik või asjaomase kolmanda riigi territoorium või kõnealuse kolmanda riigi üks või mitu kindlaksmääratud sektorit tagab isikuandmete kaitse piisava taseme. Siinkohal olgu märgitud, et nõutud ei ole, et asjaomane kolmas riik tagaks liidu õiguskorras tagatud kaitsega võrdsel tasemel kaitse, vaid väljendit „kaitse piisav tase“ tuleb selle määruse põhjenduse 104 põhjal mõista nii, et see nõuab, et kolmas riik tõepoolest tagaks oma riigisisese õigusega või endale võetud rahvusvaheliste kohustustega põhiõiguste ja -vabaduste kaitse taseme, mis on sisuliselt samaväärne sellega, mis on liidus selle määrusega tagatud, tõlgendatuna lähtuvalt hartast. Sellise nõude puudumisel eirataks nimelt eelmises punktis mainitud eesmärki (vt analoogia alusel direktiivi 95/46 artikli 25 lõike 6 kohta 6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, EU:C:2015:650, punkt 73).

95 Selles kontekstis olgu märgitud, et isikuandmete kaitse üldmääruse põhjenduses 107 on kirjas, et kui „kolmandas riigis, territooriumil või kindlaksmääratud sektoris […] ei tagata enam piisaval tasemel andmekaitset, […] tuleks isikuandmete edastamine kõnealusele kolmandale riigile […] keelata, välja

arvatud juhul, kui täidetakse [selle] määruse nõudeid, mis on seotud edastamisega asjaomaste kaitsemeetmete abil“. Sellega seoses on nimetatud määruse põhjenduses 108 täpsustatud, et kaitse piisavuse otsuse puudumise korral peaks vastutav töötleja või volitatud töötleja võtma asjakohased kaitsemeetmed vastavalt määruse artikli 46 lõikele 1, et „korvata kolmanda riigi andmekaitse puudulik tase“, selleks et „taga[d]a liidu siseseks töötlemiseks asjakohaste andmekaitsenõuete täitmi[n]e ja andmesubjektide õiguste kaitse“.

96 Nagu märkis kohtujurist oma ettepaneku punktis 115, tuleneb sellest, et need asjakohased kaitsemeetmed peavad tagama selle, et isikule, kelle andmeid edastatakse kolmandasse riiki andmekaitse tüüptingimuste alusel, oleks sama moodi nagu andmete edastamise korral kaitse piisavuse otsuse alusel tagatud selline õiguste kaitse tase, mis on sisuliselt samaväärne liidus tagatuga.

97 Eelotsusetaotluse esitanud kohtul on ka küsimus, kas liidus tagatud kaitsega sisuliselt samaväärse kaitse taseme kindlaksmääramisel tuleb lähtuda liidu õigusest, eelkõige hartaga kaitstud õigustest, ja/või Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga (edaspidi „EIÕK“) tunnustatud põhiõigustest või hoopis liikmesriikide riigisisesest õigusest.

98 Sellega seoses tuleb märkida, et kuigi EIÕKga tunnustatud põhiõigused on liidu õiguse üldpõhimõtted, nagu kinnitab ELL artikli 6 lõige 3, ning kuigi harta artikli 52 lõikes 3 on sätestatud, et hartas sisalduvate selliste õiguste tähendus ja ulatus, mis vastavad EIÕKga tagatud õigustele, on samad, mis neile nimetatud konventsiooniga ette on nähtud, ei kujuta viimane endast formaalselt liidu õiguskorda kuuluvat õigusinstrumenti, seni kuni liit ei ole konventsiooniga ametlikult ühinenud (26. veebruari 2013. aasta kohtuotsus Åkerberg Fransson, C-617/10, EU:C:2013:105, punkt 44 ja seal viidatud kohtupraktika, ning 20. märtsi 2018. aasta kohtuotsus Menci, C-524/15, EU:C:2018:197, punkt 22).

99 Neil asjaoludel on Euroopa Kohus otsustanud, et liidu õiguse tõlgendamisel ning liidu õigusaktide kehtivuse hindamisel tuleb lähtuda hartaga tagatud põhiõigustest (vt analoogia alusel 20. märtsi 2018. aasta kohtuotsus Menci, C-524/15, EU:C:2018:197, punkt 24).

100 Peale selle tuleneb väljakujunenud kohtupraktikast, et liidu õigusnormide kehtivuse hindamisel – ja juhul, kui need normid ei viita otseselt liikmesriikide õigusele, siis ka nende tõlgendamisel – ei saa lähtuda liikmesriikide õigusest ega isegi mitte liikmesriikide põhiseadusliku tasandi õigusnormidest ehk täpsemalt sellest, kuidas on põhiõigused sõnastatud nende riikide põhiseadustes (vt selle kohta 17. detsembri 1970. aasta kohtuotsus Internationale Handelsgesellschaft, 11/70, EU:C:1970:114, punkt 3; 13. detsembri 1979. aasta kohtuotsus Hauer, 44/79, EU:C:1979:290 punkt 14, ning 18. oktoobri 2016. aasta kohtuotsus Nikiforidis, C-135/15, EU:C:2016:774, punkt 28 ja seal viidatud kohtupraktika).

101 Sellest järeldub, et kuna esiteks kuulub selline isikuandmete edastamine, mis on kõne all põhikohtuasjas ja mille raames edastab liikmesriigis asuv äriühing ärilisel eesmärgil isikuandmeid kolmandas riigis asuvale teisele äriühingule, isikuandmete kaitse üldmääruse kohaldamisalasse, nagu nähtub vastusest esimesele küsimusele, ja kuna teiseks on selle määruse eesmärk, nagu selgub selle põhjendusest 10, eelkõige tagada liidus füüsiliste isikute järjekindel ja kõrgetasemeline kaitse ning tagada selleks liidus füüsiliste isikute põhiõiguste ja -vabaduste kaitse eeskirjade järjekindel ja ühtne kohaldamine isikuandmete töötlemisel, tuleb selle määruse artikli 46 lõikes 1 nõutav isikuandmete kaitse tase kindlaks määrata sama määruse sätete alusel, tõlgendatuna lähtuvalt hartaga kaitstud põhiõigustest.

102 Eelotsusetaotluse esitanud kohus palub veel selgitada, milliseid asjaolusid tuleb arvesse võtta, kui kaitse taseme piisavus tuleb kindlaks määrata olukorras, kus isikuandmeid edastatakse kolmandasse riiki isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkti c alusel vastu võetud andmekaitse tüüptingimustele tuginedes.

103 Selle kohta tuleb märkida, et kuigi viidatud sättes ei ole loetletud asjaolusid, mida tuleb arvesse võtta hindamaks, milline kaitse tase on sellise edastamise puhul piisav, on määruse artikli 46 lõikes 1 täpsustatud, et andmesubjektidele peavad olema tagatud asjakohased kaitsemeetmed ning neile peavad olema kättesaadavad kohtulikult kaitstavad õigused ja tõhusad õiguskaitsevahendid.

104 Sellise edastamise korral nõutava hindamise läbiviimisel tuleb eelkõige arvesse võtta nii liidus asuva vastutava töötleja või tema volitatud töötleja ja kolmandas riigis asuva isikuandmete vastuvõtja vahel kokku lepitud lepingutingimusi kui ka kolmanda riigi õigussüsteemiga seotud asjakohast teavet, mis puudutab selle riigi ametiasutuste võimalust edastatavatele isikuandmetele juurde pääseda. Viimati nimetatud aspekti osas hõlmab teave, mida tuleb määruse artikli 46 kohaldamisel arvesse võtta, asjaolusid, mis on mitteammendavalt loetletud määruse artikli 45 lõikes 2.

105 Seetõttu tuleb teisele, kolmandale ja kuuendale eelotsuse küsimusele vastata, et isikuandmete kaitse üldmääruse artikli 46 lõiget 1 ja artikli 46 lõike 2 punkti c tuleb tõlgendada nii, et nende sätetega nõutavad asjakohased kaitsemeetmed, kohtulikult kaitstavad õigused ja tõhusad õiguskaitsevahendid peavad andmesubjektidele, kelle isikuandmeid edastatakse kolmandasse riiki andmekaitse tüüptingimuste alusel, tagama õiguste kaitse, mille tase on sisuliselt samaväärne sellega, mis on liidus tagatud vastavalt üldmäärusele, tõlgendatuna lähtuvalt hartast. Selleks et hinnata sellise edastamise korral tagatud kaitse taset, tuleb eelkõige arvesse võtta nii liidus asuva vastutava töötleja või tema volitatud töötleja ja kolmandas riigis asuva isikuandmete vastuvõtja vahel kokku lepitud lepingutingimusi kui ka kolmanda riigi õigussüsteemiga seotud asjakohast teavet, mis puudutab selle riigi ametiasutuste võimalust nõnda edastatavatele isikuandmetele juurde pääseda ja mille hulka kuuluvad eelkõige asjaolud, mis on loetletud üldmääruse artikli 45 lõikes 2.

Kaheksas küsimus

106 Kaheksanda küsimusega soovib eelotsusetaotluse esitanud kohus sisuliselt teada, kas isikuandmete kaitse üldmääruse artikli 58 lõike 2 punkte f ja j tuleb tõlgendada nii, et pädev järelevalveasutus on kohustatud peatama või keelama komisjoni poolt vastu võetud andmekaitse tüüptingimuste alusel toimuva isikuandmete edastamise kolmandasse riiki, kui ta leiab, et selles kolmandas riigis neid tüüptingimusi ei järgita või ei saa järgida ja liidu õigusega, eelkõige isikuandmete kaitse üldmääruse artiklitega 45 ja 46 ja hartaga nõutavat edastatavate andmete kaitset ei saa tagada, või tuleb viidatud sätteid tõlgendada nii, et mainitud volituste kasutamine on piiratud erandjuhtudega.

107 Vastavalt harta artikli 8 lõikele 3 ning isikuandmete kaitse üldmääruse artikli 51 lõikele 1 ja artikli 57 lõike 1 punktile a on liikmesriikide järelevalveasutused seatud jälgima nende liidu õigusnormide järgimist, mis reguleerivad füüsiliste isikute kaitset isikuandmete töötlemisel. Seega on igal sellisel asutusel pädevus kindlaks teha, kas isikuandmete edastamine asutuse asukoha liikmesriigist kolmandasse riiki vastab selle määrusega kehtestatud nõuetele (vt analoogia alusel direktiivi 95/46 artikli 28 kohta 6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, EU:C:2015:650, punkt 47).

108 Nendest sätetest tuleneb, et järelevalveasutuste peamine ülesanne on jälgida isikuandmete kaitse üldmääruse kohaldamist ja tagada selle määruse järgimine. Selle ülesande täitmine on eriti tähtis olukorras, kus isikuandmeid edastatakse kolmandasse riiki, sest nagu nähtub juba selle määruse põhjendusest 116, võib „isikuandmete liikumine üle piiride liidust välja […] raskendada füüsiliste isikute võimalusi kasutada õigust andmete kaitsele, eelkõige kaitsta end sellise teabe ebaseadusliku kasutamise ja avaldamise eest“. Samas põhjenduses on täpsustatud, et sellisel juhul „võib järelevalveasutus sattuda olukorda, milles ta leiab, et ei suuda käsitleda kaebusi ega teostada uurimist väljapoole oma riigi piire jäävates küsimustes“.

109 Peale selle peab iga järelevalveasutus vastavalt isikuandmete kaitse üldmääruse artikli 57 lõike 1 punktile f oma territooriumil käsitlema kaebusi, mida iga andmesubjekt võib selle määruse artikli 77 lõike 1 alusel esitada, kui ta leiab, et teda puudutavate isikuandmete töötlemine rikub viidatud

määrust, ning uurima asjakohasel määral kaebuste sisu. Järelevalveasutus on kohustatud kaebuse nõutava hoolsusega läbi vaatama (vt analoogia alusel direktiivi 95/46 artikli 25 lõike 6 kohta 6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, EU:C:2015:650, punkt 63).

110 Isikuandmete kaitse üldmääruse artikli 78 lõigetes 1 ja 2 on tunnustatud iga isiku õigust tõhusale kohtulikule õiguskaitsevahendile muu hulgas juhul, kui järelevalveasutus ei käsitle tema kaebust. Selle määruse põhjenduses 141 on samuti viidatud „õigus[ele] tõhusale õiguskaitsevahendile kooskõlas harta artikliga 47“, kui järelevalveasutus „ei võta meetmeid juhul, kui need on vajalikud andmesubjekti õiguste kaitsmiseks“.

111 Esitatud kaebuste menetlemiseks on isikuandmete kaitse üldmääruse artikli 58 lõikega 1 antud järelevalveasutustele ulatuslikud uurimisvolitused. Kui järelevalveasutus leiab oma uurimise tulemusel, et andmesubjekt, kelle isikuandmed on edastatud kolmandasse riiki, ei ole selles riigis piisaval tasemel kaitstud, on ta liidu õiguse kohaselt kohustatud asjakohasel viisil reageerima, et tuvastatud puudus kõrvaldada, ja seda olenemata selle puuduse põhjusest või laadist. Sel otstarbel on määruse artikli 58 lõikes 2 loetletud erinevad parandusmeetmed, mida järelevalveasutus võib võtta.

112 Olgugi et sobiva ja vajaliku meetme valimine kuulub järelevalveasutuse pädevusse ja viimane peab selle valiku tegemisel arvesse võtma vaidlusaluse isikuandmete edastamise kõiki asjaolusid, peab ta oma ülesannet jälgida, et isikuandmete kaitse üldmäärust täielikult järgitaks, seejuures siiski täitma nõutava hoolikusega.

113 Sellega seoses olgu märgitud, et nagu rõhutas ka kohtujurist oma ettepaneku punktis 148, on järelevalveasutus isikuandmete kaitse üldmääruse artikli 58 lõike 2 punktide f ja j kohaselt kohustatud isikuandmete edastamise kolmandasse riiki peatama või keelama, kui ta kõiki edastamise asjaolusid arvestades leiab, et selles kolmandas riigis andmekaitse tüüptingimusi ei järgita või ei saa järgida ning et edastatavate andmete piisavat kaitset, mis on liidu õiguse kohaselt nõutav, ei ole võimalik tagada muude meetmete abil ning liidus asuv vastutav töötleja või tema volitatud töötleja ei ole ise andmete edastamist peatanud või lõpetanud.

114 Eelmises punktis esitatud tõlgendust ei väära andmekaitsevoliniku argumendid, mille kohaselt piiras otsuse 2010/87 artikkel 4 enne rakendusotsuse 2016/2297 jõustumist kehtinud redaktsioonis, tõlgendatuna lähtuvalt selle otsuse põhjendusest 11, järelevalveasutuste volitused isikuandmete kolmandasse riiki edastamise piiramisel või keelamisel teatud erandjuhtudega. Pärast rakendusotsuse 2016/2297 jõustumist kehtivas redaktsioonis viitab tüüptingimuste otsuse artikkel 4 nimelt järelevalveasutustel nüüd isikuandmete kaitse üldmääruse artikli 58 lõike 2 punktide f ja j alusel olevatele volitustele selline edastamine peatada või keelata, sidumata seejuures nende volituste kasutamist erandlike asjaoludega.

115 Igal juhul ei anna komisjonile isikuandmete kaitse üldmääruse artikli 46 lõike 2 punktiga c andmekaitse tüüptingimuste vastuvõtmiseks omistatud rakenduspädevus talle pädevust piirata volitusi, mis järelevalveasutustel on selle määruse artikli 58 lõike 2 alusel (vt analoogia alusel direktiivi 95/46 artikli 25 lõike 6 ja artikli 28 kohta 6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, EU:C:2015:650, punktid 102 ja 103). Ka rakendusotsuse 2016/2297 põhjenduses 5 on kinnitatud, et tüüptingimuste otsus „ei takista [järelevalveasutusel] oma volituste teostamist, et jälgida andmevooge, kaasa arvatud õigust peatada või keelustada isikuandmete edastamine, kui viimane otsustab, et edastamine viiakse läbi ELi või riikliku andmekaitse seadust rikkudes“.

116 Tuleb siiski täpsustada, et pädev järelevalveasutus on oma volituste teostamisel kohustatud täielikult järgima otsust, milles komisjon on otsustanud, tehes seda teatud juhtudel isikuandmete kaitse üldmääruse artikli 45 lõike 1 esimese lause alusel, et teatav kolmas riik tagab kaitse piisava taseme. Sellisel juhul ilmneb nimelt selle määruse artikli 45 lõike 1 teisest lausest koostoimes sama määruse põhjendusega 103, et isikuandmeid võib asjaomasesse kolmandasse riiki edastada ilma eriloata.

117 Vastavalt ELTL artikli 288 neljandale lõigule on komisjoni otsus kaitse piisavuse kohta kõigis oma aspektides siduv kõikidele adressaatideks olevatele liikmesriikidele ja seega ka kõikidele nende organitele osas, milles sellega tuvastatakse, et asjaomane kolmas riik tagab kaitse piisava taseme, ja osas, milles sellega antakse luba isikuandmeid edastada (vt analoogia alusel direktiivi 95/46 artikli 25 lõike 6 kohta 6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, EU:C:2015:650, punkt 51 ja seal viidatud kohtupraktika).

118 Seega seni, kuni Euroopa Kohus ei ole kaitse piisavuse otsust kehtetuks tunnistanud, ei tohi liikmesriigid ja nende organid, sealhulgas nende sõltumatud järelevalveasutused, võtta selle otsusega vastuolus olevaid meetmeid, näiteks akte, milles siduvalt tuvastatakse, et otsuses nimetatud kolmas riik ei taga kaitse piisavat taset (6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, EU:C:2015:650, punkt 52 ja seal viidatud kohtupraktika), ega järelikult ka peatada või keelata isikuandmete edastamist sellesse kolmandasse riiki.

119 Isikuandmete kaitse üldmääruse artikli 45 lõike 3 alusel komisjoni tehtud otsus ei tohiks siiski takistada isikuid, kelle isikuandmed on edastatud või võidakse edastada kolmandasse riiki, pöördumast isikuandmete kaitse üldmääruse artikli 77 lõike 1 alusel liikmesriigi järelevalveasutuste poole kaebusega oma õiguste ja vabaduste kaitseks seoses nende andmete töötlemisega. Samamoodi ei saa selline otsus välistada ega ka vähendada liikmesriigi järelevalveasutustele harta artikli 8 lõikega 3 ning nimetatud määruse artikli 51 lõikega 1 ja artikli 57 lõike 1 punktiga a sõnaselgelt antud volitusi (vt analoogia alusel direktiivi 95/46 artikli 25 lõike 6 ja artikli 28 kohta 6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, EU:C:2015:650, punkt 53).

120 Seega peab isegi juhul, kui komisjon on teinud otsuse kaitse piisavuse kohta, liikmesriigi pädeval järelevalveasutusel, kellele isik on esitanud kaebuse oma õiguste ja vabaduste kaitseks seoses tema isikuandmete töötlemisega, olema võimalik täiesti sõltumatult analüüsida, kas nende andmete edastamine vastab isikuandmete kaitse üldmäärusega kehtestatud nõuetele, ja vajaduse korral pöörduda riigisisesesse kohtusse, selleks et kohus esitaks juhul, kui tal on komisjoni otsuse kehtivuse suhtes samasugused kahtlused, eelotsusetaotluse kõnealuse otsuse kehtivuse analüüsimiseks (vt analoogia alusel direktiivi 95/46 artikli 25 lõike 6 ja artikli 28 kohta 6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, EU:C:2015:650, punktid 57 ja 65).

121 Eeltoodud kaalutlusi arvestades tuleb kaheksandale küsimusele vastata, et isikuandmete kaitse üldmääruse artikli 58 lõike 2 punkte f ja j tuleb tõlgendada nii, et kui puudub komisjoni poolt vastu võetud kehtiv kaitse piisavuse otsus, peab pädev järelevalveasutus peatama või keelama komisjoni poolt vastu võetud andmekaitse tüüptingimuste alusel toimuva andmete edastamise kolmandasse riiki, kui ta kõiki edastamise asjaolusid arvestades leiab, et selles kolmandas riigis neid tingimusi ei järgita või ei saa järgida ja liidu õigusega, eelkõige isikuandmete kaitse üldmääruse artiklitega 45 ja 46 ja hartaga nõutavat edastatavate andmete kaitset ei ole võimalik tagada muude meetmete abil ning liidus asuv vastutav töötleja või tema volitatud töötleja ei ole ise andmete edastamist peatanud või lõpetanud.

Seitsmes ja üheteistkümnes küsimus

122 Seitsmenda ja üheteistkümnenda küsimusega, mida tuleb analüüsida koos, palub eelotsusetaotluse esitanud kohus Euroopa Kohtul selgitada, kas tüüptingimuste otsus on harta artiklite 7, 8 ja 47 seisukohalt kehtiv.

123 Nagu nähtub seitsmenda küsimuse sõnastusest ja sellele eelotsusetaotluses lisatud selgitustest, on eelotsusetaotluse esitanud kohtul täpsemalt küsimus, kas tüüptingimuste otsusega on võimalik tagada kolmandatesse riikidesse edastatavate isikuandmete kaitse piisav tase, kui pidada silmas, et selles ette nähtud andmekaitse tüüptingimused ei ole nende kolmandate riikide ametiasutustele siduvad.

124 Tüüptingimuste otsuse artiklis 1 on sätestatud, et selle otsuse lisas sisalduvaid andmekaitse tüüptingimusi käsitatakse piisavate tagatistena üksikisikute eraelu puutumatuse ning põhiõiguste ja -vabaduste kaitseks, nagu on nõutud direktiivi 95/46 artikli 26 lõikes 2. Viimati nimetatud säte on sisuliselt üle võetud isikuandmete kaitse üldmääruse artikli 46 lõikesse 1 ja artikli 46 lõike 2 punkti c.

125 Samas, kuigi need tüüptingimused on siduvad liidus asuvale vastutavale töötlejale ja kolmandas riigis asuvale edastatavate isikuandmete vastuvõtjale, juhul kui nad on sõlminud lepingu, milles kõnealustele tüüptingimustele viidatakse, on siiski selge, et need tingimused ei saa olla siduvad selle kolmanda riigi ametiasutustele, sest viimased ei ole lepingu pooled.

126 Kuigi seetõttu esineb olukordi, kus isikuandmete vastuvõtjal on asjaomases kolmandas riigis kehtiva õiguse ja valitseva praktika tõttu võimalik tagada andmete vajalik kaitse ainuüksi andmekaitse tüüptingimuste alusel, esineb ka teistsuguseid olukordi, kus nendes tüüptingimustes ettenähtu ei tarvitse olla piisav meede, mis praktikas võimaldab tagada asjaomasesse kolmandasse riiki edastatud isikuandmete tõhusa kaitse. Nii on see eelkõige juhul, kui kolmanda riigi õigus võimaldab selle riigi avaliku võimu asutustel riivata andmesubjektide õigusi seoses nende andmetega.

127 Seetõttu tekib küsimus, kas komisjoni poolt isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkti c alusel vastu võetud otsus andmekaitse tüüptingimuste kohta on kehtetu, kui selles otsuses ei ole kaitsemeetmeid, millele saaks kohtus tugineda sellise kolmanda riigi avaliku võimu asutuste vastu, kuhu isikuandmeid nende tingimuste alusel edastatakse või võidakse edastada.

128 Isikuandmete kaitse üldmääruse artikli 46 lõikes 1 on ette nähtud, et kaitse piisavuse otsuse puudumisel võib vastutav töötleja või volitatud töötleja edastada isikuandmeid kolmandasse riiki üksnes juhul, kui vastutav töötleja või volitatud töötleja on sätestanud asjakohased kaitsemeetmed, ning tingimusel, et andmesubjektidele on kättesaadavad kohtulikult kaitstavad õigused ja tõhusad õiguskaitsevahendid. Selle määruse artikli 46 lõike 2 punkti c alusel võib need kaitsemeetmed ette näha komisjoni poolt vastu võetavate andmekaitse tüüptingimustega. Nendes sätetes ei ole aga kirjas, et kõik nimetatud kaitsemeetmed peavad tingimata olema ette nähtud komisjoni sellises otsuses nagu tüüptingimuste otsus.

129 Siinkohal tuleb märkida, et selline otsus erineb isikuandmete kaitse üldmääruse artikli 45 lõike 3 alusel vastu võetud kaitse piisavuse otsusest, milles eelkõige riiklikku julgeolekut ja riigiasutuste juurdepääsu isikuandmetele käsitlevate kolmanda riigi asjakohasete õigusaktide analüüsi põhjal tuvastatakse õiguslikult siduvalt, et kolmas riik või kolmanda riigi territoorium või kolmanda riigi üks või mitu kindlaksmääratud sektorit tagab isikuandmete kaitse piisava taseme ja et seega ei ole selle kolmanda riigi avaliku võimu asutuste juurdepääs sellistele andmetele takistuseks nende andmete edastamisele sellesse kolmandasse riiki. Komisjon võib sellise kaitse piisavuse otsuse vastu võtta ainult tingimusel, et ta on tuvastanud, et kolmanda riigi asjakohased õigusnormid näevad tõepoolest ette kõik nõutavad kaitsemeetmed, mis võimaldavad järeldada, et see riik tagab kaitse piisava taseme.

130 Seevastu otsuse puhul, millega komisjon võtab vastu andmekaitse tüüptingimused – nagu tüüptingimuste otsus –, milles ei ole silmas peetud teatavat kolmandat riiki või kolmanda riigi territooriumi või kolmanda riigi ühte või mitut kindlaksmääratud sektorit, ei saa isikuandmete kaitse üldmääruse artikli 46 lõikest 1 ja artikli 46 lõike 2 punktist c järeldada, et komisjonil on enne sellise otsuse vastuvõtmist kohustus hinnata, kas selles riigis, kuhu isikuandmed võidakse niisuguste tingimuste alusel edastada, on tagatud kaitse piisav tase.

131 Sellega seoses tuleb märkida, et üldmääruse artikli 46 lõike 1 kohaselt on komisjoni poolt vastu võetud kaitse piisavuse otsuse puudumisel liidus asuva vastutava töötleja või volitatud töötleja ülesanne muu hulgas näha ette asjakohased kaitsemeetmed. Selle määruse põhjendused 108 ja 114 kinnitavad, et kui komisjon ei ole teinud otsust kolmanda riigi andmekaitse taseme piisavuse kohta, peaks vastutav töötleja või volitatud töötleja „võtma meetmed, et korvata kolmanda riigi andmekaitse puudulik tase asjakohaste andmesubjekti kaitsmise meetmetega“, ja et „[n]eed kaitsemeetmed peaksid tagama liidu

siseseks töötlemiseks asjakohaste andmekaitsenõuete täitmise ja andmesubjektide õiguste kaitse, sealhulgas andmesubjektide kohtulikult kaitstavate õiguste ja tõhusate õiguskaitsevahendite kättesaadavuse […] liidus või kolmandas riigis“.

132 Kuna käesoleva kohtuotsuse punktist 125 nähtub, et lepingulistele andmekaitse tüüptingimustele on iseloomulik, et need ei saa olla siduvad kolmandate riikide avaliku võimu asutustele, kuid isikuandmete kaitse üldmääruse artikli 44, artikli 46 lõige 1 ja artikli 46 lõike 2 punkt c, tõlgendatuna lähtuvalt harta artiklitest 7, 8 ja 47, nõuavad, et füüsilistele isikutele selle määrusega tagatud kaitse taset ei tohi kahjustada, võib osutuda vajalikuks nendes andmekaitse tüüptingimustes ette nähtud kaitsemeetmete täiendamine. Sellega seoses on üldmääruse põhjenduses 109 ette nähtud, et „[v]astutavale töötlejale […] antud võimalus kasutada komisjoni või järelevalveasutuse vastu võetud standardseid andmekaitseklausleid ei tohiks takistada vastutavat töötlejat […] lisamast muid klausleid või täiendavaid kaitsemeetmeid“, ja täpsustatud, et neid „tuleks ergutada nägema ette täiendavaid kaitsemeetmeid […], mis täiendavad standardseid [andme]kaitseklausleid“.

133 Seega ilmneb, et komisjoni poolt üldmääruse artikli 46 lõike 2 punkti c alusel vastu võetud andmekaitse tüüptingimuste eesmärk on üksnes teha liidus asuvatele vastutavatele töötlejatele või nende volitatud töötlejatele kättesaadavaks lepingulised kaitsemeetmed, mis on ühtviisi kohaldatavad kõigis kolmandates riikides ja seda seega olenemata kaitsetasemest, mis neist riikidest igaühes tagatud on. Kuna andmekaitse tüüptingimused ei saa juba iseenesest anda tagatisi, mis lähevad kaugemale lepingulisest kohustusest tagada liidu õigusega nõutava kaitsetaseme järgimine, võivad need olenevalt ühes või teises kolmandas riigis valitsevast olukorrast vajada täiendavate meetmete võtmist vastutava töötleja poolt, et tagada nõutava kaitsetaseme järgimine.

134 Nagu märkis kohtujurist oma ettepaneku punktis 126, tugineb isikuandmete kaitse üldmääruse artikli 46 lõike 2 punktis c sätestatud lepinguline mehhanism liidus asuva vastutava töötleja või tema volitatud töötleja ning täiendavalt ka pädeva järelevalveasutuse vastutusele. Seetõttu on ennekõike vastutava töötleja või tema volitatud töötleja ülesanne kontrollida juhtumipõhiselt ja vajaduse korral koostöös andmete vastuvõtjaga, kas liidu õiguse seisukohalt tagab sihtkohaks oleva kolmanda riigi õigus andmekaitse tüüptingimuste alusel edastatud isikuandmete piisava kaitse, ja vajaduse korral näha lisaks tüüptingimustes ettenähtutele ette täiendavad kaitsemeetmed.

135 Kui liidus asuval vastutaval töötlejal või tema volitatud töötlejal ei ole võimalik võtta sellise kaitse tagamiseks piisavaid täiendavaid meetmeid, peavad nemad või nende asemel pädev järelevalveasutus isikuandmete kolmandasse riiki edastamise peatama või lõpetama. Nii on see eelkõige juhul, kui selle kolmanda riigi kehtiv õigus paneb liidust edastatud isikuandmete vastuvõtjale kohustusi, mis on nende tingimustega vastuolus, ja tekitab seetõttu kahtluse, kas lepinguga tagatud kaitse selle kolmanda riigi avaliku võimu asutuste juurdepääsu eest neile andmetele on piisaval tasemel.

136 Seetõttu ei saa üksnes asjaolu, et komisjoni poolt isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkti c alusel vastu võetud otsuses sisalduvad andmekaitse tüüptingimused – nagu tüüptingimuste otsuse lisas sisalduvad tüüptingimused – ei ole siduvad sellise kolmanda riigi ametisutustele, kuhu isikuandmeid võidakse edastada, mõjutada selle otsuse kehtivust.

137 Küll aga sõltub selle otsuse kehtivus küsimusest, kas vastavalt nõudele, mis tuleneb isikuandmete kaitse üldmääruse artikli 46 lõikest 1 ja artikli 46 lõike 2 punktist c, tõlgendatuna lähtuvalt harta artiklitest 7, 8 ja 47, sisaldab see otsus tõhusaid mehhanisme, mis praktikas võimaldavad tagada, et järgitakse liidu õigusega nõutava kaitse taset ja et selliste tingimuste alusel toimuv isikuandmete edastamine peatatakse või keelatakse juhul, kui neid tingimusi rikutakse või kui neid ei ole võimalik täita.

138 Tüüptingimuste otsuse lisas esitatud andmekaitse tüüptingimustes sisalduvate kaitsemeetmete kohta ilmneb 4. tingimuse punktidest a ja b, 5. tingimuse punktist a, 9. tingimusest ning 11. tingimuse lõikest 1, et liidus asuv vastutav töötleja, vastuvõtja, kellele isikuandmed edastatakse, ning tema võimalik volitatud töötleja võtavad vastastikku kohustuse, et asjaomaste andmete töötlemine, sealhulgas

edastamine, on toimunud ja toimub ka tulevikus „kooskõlas kohaldatava andmekaitseseaduse asjaomaste sätetega“, mille all, nagu nähtub selle otsuse artikli 3 punktis f olevast määratlusest, peetakse silmas „õigusakt[i], mis kaitseb üksikisikute põhiõigusi ja -vabadusi ning eriti nende eraelu puutumatuse õigust seoses isikuandmete töötlemisega ning mis on kohaldatav vastutava andmetöötleja suhtes liikmesriigis, kus andmeeksportija asub“. Sellise õigusakti moodustavad ka isikuandmete kaitse üldmääruse sätted, tõlgendatuna lähtuvalt hartast.

139 Vastavalt 5. tingimuse punktile a võtab kolmandas riigis asuv vastuvõtja, kellele isikuandmed edastatakse, endale kohustuse anda liidus asuvale vastutavale töötlejale viivitamata teada asjaolust, et tal ei ole võimalik sõlmitud lepingust tulenevaid kohustusi täita. Vastavalt 5. tingimuse punktile b kinnitab vastuvõtja, et tal ei ole põhjust uskuda, et tema suhtes kohaldatav õigus takistab tal täita lepingust tulenevaid kohustusi, ning kohustub juhul, kui ta saab teada, et asjaomastes õigusaktides on tehtud teda puudutavaid muudatusi, millel tõenäoliselt on negatiivne mõju tüüptingimuste otsuse lisas sisalduvatest tüüptingimustest tulenevatele tagatistele ja kohustustele, teatama neist muudatustest viivitamata vastutavale töötlejale. Kuigi 5. tingimuse punkti d alapunkt i võimaldab vastuvõtjal, kellele isikuandmed edastatakse, selliste õigusaktide alusel, millest tuleneb näiteks uurimissaladuse hoidmiseks kehtiv kriminaalmenetluslik keeld, jätta teatamata liidus asuvale vastutavale töötlejale õiguskaitseorganite õiguslikult siduvatest taotlustest isikuandmete avaldamiseks, on ta 5. tingimuse punkti a alusel siiski kohustatud teavitama vastutavat töötlejat asjaolust, et tal on võimatu andmekaitse tüüptingimusi täita.

140 Nende kahe kirjeldatud olukorra puhul annavad viidatud 5. tingimuse punktid a ja b liidus asuvale vastutavale töötlejale õiguse andmete edastamine peatada ja/või leping üles öelda. Võttes arvesse nõudeid, mis tulenevad isikuandmete kaitse üldmääruse artikli 46 lõikest 1 ja artikli 46 lõike 2 punktist c, tõlgendatuna lähtuvalt harta artiklitest 7 ja 8, on vastutav töötleja kohustatud isikuandmete edastamise peatama ja/või lepingu üles ütlema, kui andmete vastuvõtja ei ole või enam ei ole võimeline tagama andmekaitse tüüptingimuste täitmist. Vastasel juhul rikuks vastutav töötleja nõudeid, mis tulenevad talle tüüptingimuste otsuse lisas sisalduva 4. tingimuse punktist a, tõlgendatuna lähtuvalt isikuandmete kaitse üldmääruse ja harta sätetest.

141 Seega ilmneb, et selles lisas sisalduva 4. tingimuse punkt a ning 5. tingimuse punktid a ja b panevad liidus asuvale vastutavale töötlejale ja vastuvõtjale, kellele isikuandmed edastatakse, kohustuse enne isikuandmete kolmandasse riiki edastamisele asumist veenduda, et kolmanda riigi õigusaktid võimaldavad vastuvõtjal tüüptingimuste otsuse lisas sisalduvaid tüüptingimusi täita. Seoses selleks vajaliku kontrolliga on 5. tingimusega seotud joonealuses märkuses täpsustatud, et kolmanda riigi õigusaktide kohustuslikud nõuded, mis ei lähe kaugemale demokraatlikus ühiskonnas riikliku julgeoleku, riigikaitse ja avaliku korra tagamiseks vajalikust, ei ole andmekaitse tüüptingimustega vastuolus. Küll aga käsitatakse nende tingimuste rikkumisena – nagu rõhutas ka kohtujurist oma ettepaneku punktis 131 – seda, kui täidetakse sellist sihtkohaks oleva kolmanda riigi õigusest tulenevat kohustust, mis läheb kaugemale sel otstarbel vajalikust. Nende osapoolte hinnangus sellise kohustuse vajalikkusele tuleb juhul, kui komisjon on teinud isikuandmete kaitse üldmääruse artikli 45 lõike 3 alusel otsuse, milles ta tuvastab vastavas kolmandas riigis tagatud kaitse taseme piisavuse, arvesse võtta selles otsuses tuvastatut.

142 Sellest tuleneb, et liidus asuv vastutav töötleja ja vastuvõtja, kellele isikuandmed edastatakse, on kohustatud enne kontrollima, kas asjaomases kolmandas riigis on tagatud liidu õigusega nõutav kaitsetase. Kui andmete vastuvõtjal võib osutuda võimatuks neid tüüptingimusi täita, on ta 5. tingimuse punkti b alusel kohustatud sellest teatama vastutavale töötlejale, kelle ülesanne on seepeale andmete edastamine peatada ja/või leping üles öelda.

143 Kui kolmandasse riiki edastatud isikuandmete vastuvõtja annab vastutavale töötlejale tüüptingimuste otsuse lisas sisalduva 5. tingimuse punkti b alusel teada, et asjaomase kolmanda riigi õigusaktid ei võimalda tal täita selles lisas sisalduvaid andmekaitse tüüptingimusi, tuleneb sama lisa 12. tingimusest,

et sellesse kolmandasse riiki juba edastatud isikuandmed ja nendest tehtud koopiad tuleb täielikult tagastada või hävitada. Igal juhul on selle lisa 6. tingimuses ette nähtud sanktsioon tüüptingimuste rikkumise eest, kuivõrd selles on andmesubjektile antud õigus nõuda tekitatud kahju eest hüvitist.

144 Olgu lisatud, et tüüptingimuste otsuse lisas sisalduva 4. tingimuse punkti f alusel kohustub liidus asuv vastutav töötleja juhul, kui teatavat liiki andmeid võidakse edastada kolmandasse riiki, mis ei taga kaitse piisavat taset, andma sellest andmesubjektile teada enne edastamist või võimalikult kiiresti pärast edastamist. See teave võib anda andmesubjektile võimaluse kasutada vastutava töötleja suhtes õiguskaitsevahendit, mis tal on sama lisa 3. tingimuse esimese lõigu alusel, ning nõuda, et vastutav töötleja peataks kavandatud edastamise, ütleks isikuandmete vastuvõtjaga sõlmitud lepingu üles või – kui see on asjakohane – nõuaks, et viimane edastatud andmed tagastaks või hävitaks.

145 Viimaks on liidus asuv vastutav töötleja nimetatud lisas sisalduva 4. tingimuse punkti g alusel kohustatud juhul, kui isikuandmete vastuvõtja annab talle selle lisa 5. tingimuse punkti b alusel teada, et teda puudutavasse õigusakti on tehtud muudatus, millel tõenäoliselt on andmekaitse tüüptingimustest tulenevatele tagatistele ja kohustustele märkimisväärne negatiivne mõju, edastama selle teate pädevale järelevalveasutusele, kui ta otsustab sellest teatest hoolimata edastamist jätkata või andmete edastamise peatamise tühistada. Sellise teate edastamine pädevale järelevalveasutusele ja viimase õigus isikuandmete vastuvõtjat sama lisa 8. tingimuse lõike 2 alusel auditeerida võimaldavad järelevalveasutusel kindlaks teha, kas kavandatud edastamine tuleb kaitse piisava taseme tagamiseks peatada või keelata.

146 Selles küsimuses kinnitab tüüptingimuste otsuse artikkel 4, tõlgendatuna lähtuvalt rakendusotsuse 2016/2297 põhjendusest 5, et tüüptingimuste otsus ei takista pädeval järelevalveasutusel peatada või keelata sellele otsusele lisatud andmekaitse tüüptingimuste alusel toimuvat isikuandmete edastamist kolmandasse riiki. Sellega seoses olgu märgitud, et nagu tuleneb vastusest kaheksandale küsimusele, on järelevalveasutus juhul, kui puudub komisjoni poolt kehtivalt vastu võetud kaitse piisavuse otsus, kohustatud isikuandmete kaitse üldmääruse artikli 58 lõike 2 punktide f ja j alusel sellise edastamise peatama või keelama, kui ta kõiki edastamise asjaolusid arvestades leiab, et selles kolmandas riigis neid tingimusi ei järgita või ei saa järgida ja liidu õigusega nõutavat edastatavate andmete kaitset ei ole võimalik tagada muude meetmete abil ning liidus asuv vastutav töötleja või tema volitatud töötleja ei ole ise andmete edastamist peatanud või lõpetanud.

147 Mis puudutab andmekaitsevoliniku esile toodud asjaolu, et erinevate liikmesriikide järelevalveasutused võivad sellise kolmanda riigi suunal toimuva isikuandmete edastamise suhtes teha lahknevaid otsuseid, siis tuleb lisada, et isikuandmete kaitse üldmääruse artikli 55 lõikest 1 ja artikli 57 lõike 1 punktist a tuleneb, et üldjuhul on iga järelevalveasutuse ülesanne jälgida selle määruse järgimist oma liikmesriigi territooriumil. Peale selle on üldmääruse artikli 64 lõikes 2 erinevate otsuste vältimiseks ette nähtud, et järelevalveasutus, kes leiab, et isikuandmete edastamine teatavasse kolmandasse riiki tuleb üldkehtivalt keelata, võib pöörduda Euroopa andmekaitsenõukogusse arvamuse saamiseks ja juhul, kui mõni järelevalveasutus antud arvamust ei järgi, võib andmekaitsenõukogu selle määruse artikli 65 lõike 1 punkti c alusel teha siduva otsuse.

148 Sellest järeldub, et tüüptingimuste otsuses on ette nähtud tõhusad mehhanismid, mis praktikas võimaldavad tagada, et selle otsuse lisas sisalduvate tüüptingimuste alusel toimuv isikuandmete edastamine peatatakse või keelatakse juhul, kui andmete vastuvõtja neid tingimusi rikub või kui tal ei ole neid võimalik täita.

149 Kõiki eeltoodud kaalutlusi arvestades tuleb seitsmendale ja üheteistkümnendale küsimusele vastata, et tüüptingimuste otsuse analüüsimisel harta artiklite 7, 8 ja 47 alusel ei ilmnenud asjaolusid, mis mõjutaksid selle otsuse kehtivust.

Neljas, viies, üheksas ja kümnes küsimus

150 Üheksanda küsimusega palub eelotsusetaotluse esitanud kohus sisuliselt selgitada, kas ja mil määral on liikmesriigi järelevalveasutus seotud Privacy Shieldi otsuses tuvastatuga, mille kohaselt USA tagab kaitse piisava taseme. Neljanda, viienda ja kümnenda küsimusega palub see kohus sisuliselt selgitada, kas tema enese poolt USA õiguse kohta tuvastatut arvestades rikub tüüptingimuste otsuse lisas sisalduvate tüüptingimuste alusel isikuandmete edastamine sellesse kolmandasse riiki harta artiklitega 7, 8 ja 47 tagatud õigusi, ning küsib Euroopa Kohtult täpsemalt, kas Privacy Shieldi otsuse III lisas mainitud ombudsmani ametikoha loomine on viidatud artikliga 47 kooskõlas.

151 Sissejuhatuseks olgu märgitud, et kuigi andmekaitsevolinik seab põhikohtuasjas esitatud avalduses kahtluse alla ainult tüüptingimuste otsuse kehtivuse, esitati see avaldus eelotsusetaotluse esitanud kohtule enne Privacy Shieldi otsuse vastuvõtmist. Kuna eelotsust taotlev kohus pärib neljanda ja viienda küsimusega Euroopa Kohtult üldiselt kaitse kohta, mis harta artiklite 7, 8 ja 47 alusel peab sellise andmeedastuse korral tagatud olema, peab Euroopa Kohus hinnangu andmisel arvesse võtma ka vahepeal vastu võetud Privacy Shieldi otsusest tulenevaid tagajärgi. See on nii seda enam, et nimetatud kohus küsib oma kümnendas küsimuses sõnaselgelt, kas harta artikliga 47 nõutava kaitse saab tagada viimati nimetatud otsuses mainitud ombudsmani abil.

152 Peale selle ilmneb eelotsusetaotluses olevatest selgitustest, et põhikohtuasja menetluses väitis Facebook Ireland, et Privacy Shieldi otsusel on andmekaitsevoliniku jaoks siduvad tagajärjed osas, mis puudutab USA poolt tagatud kaitse taseme piisavuse tuvastamist ja seeläbi ka sellesse kolmandasse riiki tüüptingimuste otsuse lisas sisalduvate andmekaitse tüüptingimuste alusel toimuva isikuandmete edastamise seaduslikkust.

153 Nagu aga ilmneb käesoleva kohtuotsuse punktist 59, rõhutas eelotsusetaotluse esitanud kohus oma 3. oktoobri 2017. aasta otsuses, mis on lisatud eelotsusetaotlusele, et ta peab arvesse võtma avalduse esitamise ja tema korraldatud kohtuistungi vahele jääval ajal toimunud õigusalaseid muudatusi. Seega tundub, et nimetatud kohus on põhikohtuasja lahendamisel kohustatud arvesse võtma Privacy Shieldi otsuse vastuvõtmisest tulenevat asjaolude muutumist ning selle otsuse võimalikke siduvaid tagajärgi.

154 Täpsemalt on siduvate tagajärgede olemasolu, mis on Privacy Shieldi otsuses tehtud järeldusel USA poolt tagatud kaitse taseme piisavuse kohta, asjakohane selleks, et hinnata nii käesoleva kohtuotsuse punktides 141 ja 142 mainitud kohustusi, mis vastutaval töötlejal ja isikuandmete vastuvõtjal on juhul, kui neid andmeid edastatakse kolmandasse riiki tüüptingimuste otsuse lisas sisalduvate andmekaitse tüüptingimuste alusel, kui ka kohustusi, mis võivad sellisel juhul olla järelevalveasutusel selline edastamine peatada või keelata.

155 Mis täpsemalt puudutab Privacy Shieldi otsuse siduvaid tagajärgi, siis selle otsuse artikli 1 lõikes 1 on kirjas, et „Ameerika Ühendriigid tagavad ELi-USA andmekaitseraamistiku Privacy Shield alusel [isikuandmete kaitse üldmääruse artikli 45 lõike 1] tähenduses piisava kaitsetaseme isikuandmetele, mis edastatakse [Euroopa Liidust] Ameerika Ühendriikides asuvatele organisatsioonidele“. Selle otsuse artikli 1 lõike 3 kohaselt loetakse isikuandmed edastatuks selle andmekaitseraamistiku alusel juhul, kui need edastatakse liidust USAs asuvatele organisatsioonidele, mis kuuluvad Privacy Shieldi nimekirja, mida haldab ja mille teeb avalikkusele kättesaadavaks USA kaubandusministeerium kooskõlas selle otsuse II lisas esitatud põhimõtete I ja III jaoga.

156 Nagu nähtub käesoleva kohtuotsuse punktides 117 ja 118 viidatud kohtupraktikast, on Privacy Shieldi otsus järelevalveasutustele siduv osas, milles tuvastatakse, et USA tagab kaitse piisava taseme, ja seetõttu antakse sellega luba edastada isikuandmeid ELi-USA andmekaitseraamistiku Privacy Shield alusel. Seega senikaua, kuni Euroopa Kohus ei ole seda otsust kehtetuks tunnistanud, ei saa pädev järelevalveasutus peatada või keelata isikuandmete edastamist Privacy Shieldi nimekirja kuuluvale organisatsioonile põhjendusega, et vastupidi komisjoni selles otsuses antud hinnangule leiab tema, et

USA õigusaktid, mis reguleerivad selle kolmanda riigi avaliku võimu asutuste võimalust pääseda riikliku julgeoleku, õiguskaitse ja muu avaliku huvi eesmärgil juurde selle andmekaitseraamistiku alusel edastatud isikuandmetele ja neid andmeid kasutada, ei taga kaitse piisavat taset.

157 Vastavalt käesoleva kohtuotsuse punktides 119 ja 120 viidatud kohtupraktikale ei tähenda eelnev siiski, et pädev järelevalveasutus, kellele isik on esitanud kaebuse, ei peaks täiesti sõltumatult uurima, kas vaidlusaluse isikuandmete edastamise puhul on järgitud isikuandmete kaitse üldmääruses ette nähtud nõudeid, ja juhul kui ta leiab, et selle isiku esitatud väited seavad kaitse piisavuse otsuse kehtivuse kahtluse alla, esitama avalduse liikmesriigi kohtule, et viimane esitaks Euroopa Kohtule eelotsusetaotluse selle otsuse kehtivuse hindamiseks.

158 Isikuandmete kaitse üldmääruse artikli 77 lõike 1 alusel esitatud kaebust, milles isik, kelle isikuandmed on edastatud või võidakse edastada kolmandasse riiki, väidab, et asjaomases riigis kehtiv õigus ja valitsev praktika ei taga kaitse piisavat taset hoolimata sellest, mida komisjon on tuvastanud selle määruse artikli 45 lõike 3 alusel vastu võetud otsuses, tuleb nimelt mõista nii, et sisuliselt puudutab see kõnealuse otsuse kooskõla isikute eraelu ning põhiõiguste ja -vabaduste kaitsega (vt analoogia alusel direktiivi 95/46 artikli 25 lõike 6 ja artikli 28 lõike 4 kohta 6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, EU:C:2015:650, punkt 59).

159 Käesoleval juhul on M. Schrems sisuliselt palunud andmekaitsevolinikul keelata või peatada tema isikuandmete edastamine Facebook Irelandi poolt USAs asuvale Facebook Inc-le, põhjendusega, et see kolmas riik ei taga kaitse piisavat taset. Kuna andmekaitsevolinik pöördus M. Schremsi väidete läbivaatamiseks korraldatud uurimise järel eelotsusetaotluse esitanud kohtusse, tundub sellel kohtul talle esitatud tõendeid ja toimunud võistlevat kohtuvaidlust arvestades olevat küsimus, kas M. Schremsi kahtlused selles kolmandas riigis tagatud kaitse taseme piisavuse kohta on põhjendatud, olenemata sellest, mida komisjon on vahepeal Privacy Shieldi otsuses tuvastanud, mistõttu ta on esitanud Euroopa Kohtule neljanda, viienda ja kümnenda eelotsuse küsimuse.

160 Nagu märkis kohtujurist oma ettepaneku punktis 175, tuleb neid eelotsuse küsimusi mõista nii, et sisuliselt seavad need kahtluse alla komisjoni poolt Privacy Shieldi otsuses tuvastatu, mille kohaselt USA tagab selle otsuse alusel liidust sellesse kolmandasse riiki edastatud isikuandmete kaitse piisava taseme, ja seega ka selle otsuse kehtivuse.

161 Arvestades käesoleva kohtuotsuse punktides 121 ja 157–160 esitatud kaalutlusi, tuleb eelotsusetaotluse esitanud kohtule täieliku vastuse andmiseks seega analüüsida, kas Privacy Shieldi otsus vastab nõuetele, mis tulenevad isikuandmete kaitse üldmäärusest, tõlgendatuna lähtuvalt hartast (vt analoogia alusel 6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, EU:C:2015:650, punkt 67).

162 Selleks et komisjoni saaks isikuandmete kaitse üldmääruse artikli 45 lõike 3 alusel vastu võtta kaitse piisavuse otsuse, on tarvis, et see institutsioon oleks nõuetekohaselt põhjendatult tuvastanud, et asjasse puutuv kolmas riik on oma riigisisese õigusega või endale võetud rahvusvaheliste kohustustega tõepoolest taganud põhiõiguste kaitse taseme, mis on sisuliselt samaväärne liidu õiguskorras tagatuga (vt analoogia alusel direktiivi 95/46 artikli 25 lõike 6 kohta 6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, EU:C:2015:650, punkt 96).

Privacy Shieldi otsuse sisu

163 Komisjon tuvastas Privacy Shieldi otsuse artikli 1 lõikes 1, et USA tagab ELi-USA andmekaitseraamistiku Privacy Shield alusel kaitse piisava taseme isikuandmetele, mis edastatakse liidust Ameerika Ühendriikides asuvatele organisatsioonidele, kusjuures sama otsuse artikli 1 lõike 2 kohaselt koosneb nimetatud andmekaitseraamistik 7. juulil 2016 USA kaubandusministeeriumi poolt välja antud põhimõtetest, mis on esitatud selle otsuse II lisas, ning ametlikest kinnitustest ja kohustustest, mis on esitatud sama otsuse I ja III–VII lisas loetletud dokumentides.

164 Samas on Privacy Shieldi otsuse II lisa „ELi-USA andmekaitseraamistiku Privacy Shield põhimõtted“ punktis I.5 ühtlasi täpsustatud, et nende põhimõtete järgimist võib piirata muu hulgas „riikliku julgeoleku, avaliku huvi või õiguskaitseliste vajaduste täitmiseks vajalikus ulatuses“. Seega on selles otsuses sama moodi nagu otsuses 2000/520 ette nähtud nende vajaduste esimus kõnealuste põhimõtete ees ning selle esimuse kohaselt on kinnituse andnud USA organisatsioonid, kes saavad liidust isikuandmeid, kohustatud nendest põhimõtetest piiramatult kõrvale kalduma, kui need lähevad nimetatud vajadustega vastuollu ja on seega nendega kokkusobimatud (vt analoogia alusel otsuse 2000/520 kohta 6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, EU:C:2015:650, punkt 86).

165 Kuna Privacy Shieldi otsuse II lisa punktis I.5 ette nähtud erand on üldist laadi, muudab see võimalikuks USA riiklikku julgeolekut ja avalikku huvi puudutavatel vajadustel või USA riigisisesel õigusel põhinevad nende isikute põhiõiguste riived, kelle isikuandmed on edastatud või võidakse edastada liidust USAsse (vt analoogia alusel otsuse 2000/520 kohta 6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, EU:C:2015:650, punkt 87). Täpsemalt – ja nagu on tõdetud ka Privacy Shieldi otsuses – võivad sellised riived tuleneda sellest, et USA avaliku võimu asutused võivad liidust USAsse edastatavatele isikuandmetele juurde pääseda ja neid andmeid kasutada FISA artiklil 702 põhinevate jälgimisprogrammide PRISM ja UPSTREAM ning korralduse E.O. 12333 alusel.

166 Selles kontekstis hindas komisjon Privacy Shieldi otsuse põhjendustes 67–135 piiranguid ja kaitsemeetmeid, mis on sätestatud USA õigusaktides, eelkõige FISA artiklis 702, korralduses E.O. 12333 ja suunises PPD-28, seoses USA avaliku võimu asutuste võimalusega pääseda riikliku julgeoleku, avaliku korra ja muul üldist huvi teenival eesmärgil juurde ELi-USA andmekaitseraamistiku Privacy Shield alusel edastatud isikuandmetele ja neid andmeid kasutada.

167 Selle hindamise tulemusel sedastas komisjon selle otsuse põhjenduses 136, et „Ameerika Ühendriigid tagavad […] piisava kaitsetaseme isikuandmetele, mis edastatakse liidust põhimõtete järgimist kinnitanud organisatsioonidele Ameerika Ühendriikides“, ja leidis otsuse põhjenduses 140 „USA õigussüsteemi kohta saada oleva teabe […] põhjal, et selliste isikute põhiõiguste riivamine Ameerika Ühendriikides riikliku julgeoleku, õiguskaitse või muu avaliku huvi eesmärgil, kelle isikuandmeid edastatakse liidust Ameerika Ühendriikidesse, ja põhimõtete järgimist kinnitanud organisatsioonidele sellest tulenevalt kehtivad piirangud eraelu puutumatuse põhimõtete järgimisel, piirduvad asjaomase seadusliku eesmärgi saavutamiseks rangelt vajalikuga ning tagatud on tõhus õiguskaitse sellise riive vastu“.

Kaitse piisava taseme tuvastamine

168 Arvestades asjaolusid, mida komisjon mainis Privacy Shieldi otsuses, ning asjaolusid, mille eelotsusetaotluse esitanud kohus on tuvastanud põhikohtusja menetluses, kahtleb see kohus, kas USA õigus tõepoolest tagab kaitse piisava taseme, mida nõuab isikuandmete kaitse üldmääruse artikkel 45, tõlgendatuna lähtuvalt harta artiklitega 7, 8 ja 47 kaitstud põhiõigustest. Täpsemalt leiab nimetatud kohus, et selle kolmanda riigi õiguses ei ole ette nähtud piiranguid ja kaitsemeetmeid, mida on vaja tema riigisiseste õigusnormidega lubatud riivete tõttu, ega taga ka tõhusat kohtulikku kaitset selliste riivete vastu. Ta lisab sellega seoses, et andmekaitseraamistiku Privacy Shield ombudsmani ametikoha loomine ei saa tema hinnangul neid lünki täita, sest ombudsmani ei saa samastada kohtuga harta artikli 47 tähenduses.

169 Mis esiteks puudutab harta artikleid 7 ja 8, millel on oma osa liidus nõutava kaitse taseme kujundamisel, mille järgimise peab komisjon olema tuvastanud, enne kui ta saab isikuandmete kaitse üldmääruse artikli 45 lõike 1 alusel vastu võtta kaitse piisavuse otsuse, siis olgu märgitud, et harta artikkel 7 tagab igaühe õiguse sellele, et austataks tema era- ja perekonnaelu, kodu ja edastatavate sõnumite saladust. Harta artikli 8 lõige 1 aga annab sõnaselgelt igaühele õiguse tema isikuandmete kaitsele.

170 Seega mõjutab füüsilise isiku isikuandmetele nende säilitamiseks või kasutamiseks juurde pääsemine selle isiku põhiõigust eraelu puutumatusele, mida kaitseb harta artikkel 7, ja see õigus laieneb kogu teabele tuvastatud või tuvastatava füüsilise isiku kohta. Selline andmetöötlemine kuulub ka harta artikli 8 kohaldamisalasse, kuna tegemist on isikuandmete töötlemisega selle artikli tähenduses, mistõttu peab see tingimata vastama kõnealuses artiklis ette nähtud andmekaitsenõuetele (vt selle kohta 9. novembri 2010. aasta kohtuotsus Volker und Markus Schecke ja Eifert, C-92/09 ja C-93/09, EU:C:2010:662, punktid 49 ja 52; 8. aprilli 2014. aasta kohtuotsus Digital Rights Ireland jt, C-293/12 ja C-594/12, EU:C:2014:238, punkt 29, ning 26. juuli 2017. aasta arvamus 1/15 (ELi-Kanada broneeringuinfo leping), EU:C:2017:592, punktid 122 ja 123).

171 Euroopa Kohus on juba leidnud, et isikuandmete edastamine kolmandale isikule, näiteks avaliku võimu asutusele, kujutab endast harta artiklitega 7 ja 8 tagatud põhiõiguse riivet, olenemata sellest, kuidas edastatud teavet hiljem kasutatakse. Sama kehtib isikuandmete säilitamise ning isikuandmetele juurdepääsu suhtes, mis antakse ametiasutustele, et nad saaksid andmeid kasutada, olenemata sellest, kas asjasse puutuvad eraelulised andmed on delikaatsed või mitte või kas puudutatud isikud on selle riive tõttu pidanud taluma mingeid ebamugavusi või mitte (vt selle kohta 20. mai 2003. aasta kohtuotsus Österreichischer Rundfunk jt, C-465/00, C-138/01 ja C-139/01, EU:C:2003:294, punktid 74 ja 75; 8. aprilli 2014. aasta kohtuotsus Digital Rights Ireland jt, C-293/12 ja C-594/12, EU:C:2014:238, punktid 33–36, ning 26. juuli 2017. aasta arvamus 1/15 (ELi-Kanada broneeringuinfo leping), EU:C:2017:592, punktid 124 ja 126).

172 Harta artiklites 7 ja 8 tunnustatud õigused ei ole siiski absoluutsed eelisõigused, vaid neid tuleb arvesse võtta kooskõlas nende ülesandega ühiskonnas (vt selle kohta 9. novembri 2010. aasta kohtuotsus Volker und Markus Schecke ja Eifert, C-92/09 ja C-93/09, EU:C:2010:662, punkt 48 ja seal viidatud kohtupraktika; 17. oktoobri 2013. aasta kohtuotsus Schwarz, C-291/12, EU:C:2013:670, punkt 33 ja seal viidatud kohtupraktika, ning 26. juuli 2017. aasta arvamus 1/15 (ELi-Kanada broneeringuinfo leping), EU:C:2017:592, punkt 136).

173 Sellega seoses tuleb ka märkida, et harta artikli 8 lõike 2 kohaselt tuleb isikuandmeid töödelda muu hulgas „kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel“.

174 Lisaks tohib harta artikli 52 lõike 1 esimese lause kohaselt hartaga tunnustatud õiguste ja vabaduste teostamist piirata ainult seadusega ning nimetatud õiguste ja vabaduste olemust arvestades. Vastavalt harta artikli 52 lõike 1 teisele lausele võib proportsionaalsuse põhimõtte kohaselt neile õigustele ja vabadustele piiranguid seada üksnes juhul, kui need on vajalikud ning vastavad tegelikult liidu tunnustatud üldist huvi pakkuvatele eesmärkidele või kui on vaja kaitsta teiste isikute õigusi ja vabadusi.

175 Viimati mainitud aspekti kohta olgu lisatud, et nõue, mille kohaselt peab põhiõiguste teostamise igasugune piiramine olema sätestatud seaduses, tähendab, et õiguslik alus, mis võimaldab nendesse õigustesse sekkuda, peab ise määratlema, kui ulatuslikult tohib asjaomase õiguse teostamist piirata (vt 26. juuli 2017. aasta arvamus 1/15 (ELi-Kanada broneeringuinfo leping), EU:C:2017:592, punkt 139 ja seal viidatud kohtupraktika).

176 Viimaks peavad isikuandmete kaitse erandid ja piirangud proportsionaalsuse põhimõtte järgimiseks piirduma rangelt vajalikuga, mistõttu peavad riivet sisaldavas õigusaktis olema ette nähtud selged ja täpsed reeglid, mis reguleerivad asjaomase meetme ulatust ja kohaldamist ning millega on kehtestatud miinimumnõuded, millest tulenevalt on isikutel, kelle andmed on edastatud, piisavad tagatised, mis võimaldavad tõhusalt kaitsta nende isikuandmeid kuritarvitamise ohu eest. Täpsemalt peab õigusaktis olema märgitud, millistel asjaoludel ja tingimustel võib nende andmete töötlemist hõlmava meetme võtta, tagades seeläbi, et riive piirdub rangelt vajalikuga. Niisuguste tagatiste olemasolu on veel

vajalikum siis, kui isikuandmeid töödeldakse automaatselt (vt selle kohta 26. juuli 2017. aasta arvamus 1/15 (ELi-Kanada broneeringuinfo leping), EU:C:2017:592, punktid 140 ja 141 ning seal viidatud kohtupraktika).

177 Isikuandmete kaitse üldmääruse artikli 45 lõike 2 punktis a on selle kohta täpsustatud, et kolmanda riigi poolt tagatud kaitse taseme piisavuse hindamisel võtab komisjon muu hulgas arvesse „tõhusate ja kohtulikult kaitstavate õiguste […] olemasolu andmesubjektide jaoks“, kelle isikuandmeid edastatakse.

178 Käesoleval juhul on komisjoni poolt Privacy Shieldi otsuses tehtud järeldus, et USA tagab kaitse taseme, mis on sisuliselt samaväärne kaitsega, mille liidus tagab isikuandmete kaitse üldmäärus, tõlgendatuna lähtuvalt harta artiklitest 7 ja 8, seatud kahtluse alla muu hulgas põhjusel, et FISA artiklil 702 ja korraldusel E.O. 12333 põhinevate jälgimisprogrammide suhtes ei kehti nõuded, mis proportsionaalsuse põhimõtet järgides tagaksid kaitse taseme, mis on sisuliselt samaväärne harta artikli 52 lõike 1 teise lausega tagatuga. Seega tuleb uurida, kas nende jälgimisprogrammide rakendamisel järgitakse selliseid nõudeid, ilma et enne oleks vaja kindlaks teha, kas selles kolmandas riigis täidetakse tingimusi, mis on sisuliselt samaväärsed harta artikli 52 lõike 1 esimeses lauses ettenähtutega.

179 FISA artiklil 702 põhinevate jälgimisprogrammide kohta tõdes komisjon Privacy Shieldi otsuse põhjenduses 109, et selle artikli kohaselt „ei anna FISC luba üksikuteks jälgimismeetmeteks; selle asemel annab ta load jälgimisprogrammide jaoks (nt PRISM, UPSTREAM) vastavalt iga-aastastele vastavuskinnitustele, mille koostavad justiitsminister ja riigi luuredirektor“. Samast põhjendusest selgub, et FISC kontrolli eesmärk on kindlaks teha, kas need jälgimisprogrammid vastavad eesmärgile saada välisluureinfot, kuid ei puuduta küsimust, „kas isikud on välisluureinfo kogumise sihtmärgiks valitud õigesti“.

180 Seega ilmneb, et FISA artiklist 702 ei saa mingil viisil tuletada piiranguid selles ette nähtud volitusele rakendada jälgimisprogramme välisluureinfo saamiseks, nagu ka mitte kaitsemeetmeid USA-välistele isikutele, kes on nende programmide potentsiaalseks sihtmärgiks. Neil asjaoludel ja nagu sisuliselt märkis kohtujurist oma ettepaneku punktides 291, 292 ja 297, ei ole selle artikli abil võimalik tagada kaitse taset, mis oleks sisuliselt samaväärne hartaga tagatuga vastavalt tõlgendusele, mis hartale on antud käesoleva kohtuotsuse punktides 175 ja 176 viidatud kohtupraktikas ja mille kohaselt õiguslik alus, mis võimaldab põhiõiguste riivet, peab proportsionaalsuse põhimõttele vastamiseks ise määratlema, kui ulatuslikult tohib asjaomase õiguse teostamist piirata, ning nägema ette selged ja täpsed reeglid, mis reguleerivad asjaomase meetme ulatust ja kohaldamist ning millega on kehtestatud miinimumnõuded.

181 Privacy Shieldi otsuses on küll tõdetud, et FISA artiklil 702 põhinevate jälgimisprogrammide rakendamisel peab järgima suunisest PPD-28 tulenevaid nõudeid. Samas, kuigi komisjon on Privacy Shieldi otsuse põhjendustes 69 ja 77 rõhutanud, et nimetatud suunisest tulenevad nõuded on USA luureteenistustele siduvad, möönis USA valitsus vastuseks Euroopa Kohtu esitatud küsimusele, et suunis PPD-28 ei anna andmesubjektidele õigusi, millele saaks USA ametiasutuste vastu kohtus tugineda. Seega ei ole selle abil võimalik tagada kaitse taset, mis oleks sisuliselt samaväärne hartaga tagatuga, erinevalt sellest, mida nõuab isikuandmete kaitse üldmääruse artikli 45 lõike 2 punkt a, mille kohaselt eeldab sellise kaitse taseme tuvastamine muu hulgas tõhusate ja kohtulikult kaitstavate õiguste olemasolu andmesubjektide jaoks, kelle isikuandmeid on kõnealusesse kolmandasse riiki edastatud.

182 Seoses korraldusel E.O. 12333 põhinevate jälgimisprogrammidega ilmneb Euroopa Kohtu käsutuses olevast toimikust, et ka see korraldus ei anna õigusi, millele saaks USA ametiasutuste vastu kohtus tugineda.

183 Olgu lisatud, et suunise PPD-28 alusel, mida tuleb kahes eelmises punktis käsitletud programmi rakendamisel järgida, on võimalik „„laiaulatuslik“ kogumine“, mis tähendab „suhteliselt suure koguse signaaliluure teel kogutava teabe või andmete omandamist tingimustel, kus luureühendusel ei ole

võimalik otsingu täpsustamiseks kasutada midagi, mille abil identifitseerida konkreetseid objekte“, nagu on täpsustatud riigi luuredirektori büroo (Office of the Director of National Intelligence) 21. juuni 2016. aasta kirjas USA kaubandusministeeriumile ja väliskaubandusametile, mis on ära toodud Privacy Shieldi otsuse VI lisas. See võimalus pääseda korraldusel E.O. 12333 põhinevate jälgimisprogrammide raames juurde USAsse liikuvatele andmetele, ilma et selle juurdepääsu suhtes toimuks mingitki kohtulikku kontrolli, ei sea igal juhul piisavalt selgelt ja täpselt piire isikuandmete sellisele laiaulatuslikule kogumisele.

184 Seega ilmneb, et ei FISA artikkel 702 ega korraldus E.O. 12333 koostoimes suunisega PPD-28 ei vasta liidu õiguses proportsionaalsuse põhimõttest tulenevatele nõuetele, mistõttu ei saa asuda seisukohale, et nendel sätetel põhinevad jälgimisprogrammid piirduvad rangelt vajalikuga.

185 Neil asjaoludel ei ole isikuandmete kaitse piirangud, mis tulenevad USAriigisisestest õigusnormidest, mis reguleerivad USA avaliku võimu asutuste õigust pääseda juurde liidust USAsse edastatavatele isikuandmetele ja neid andmeid kasutada, ning millele komisjon Privacy Shieldi otsuses hinnangu andis, piiritletud viisil, mis vastaks liidu õiguses harta artikli 52 lõike 1 teises lauses ettenähtuga sisuliselt samaväärsetele nõuetele.

186 Mis teiseks puudutab harta artiklit 47, millel on oma osa liidus nõutava kaitse taseme kujundamisel, mille järgimise peab komisjon olema tuvastanud enne, kui ta saab vastu võtta otsuse isikuandmete kaitse üldmääruse artikli 45 lõike 1 alusel, siis olgu märgitud, et selle artikli 47 esimeses lõigus on nõutud, et igaühel, kelle liidu õigusega tagatud õigusi või vabadusi rikutakse, on selles artiklis kehtestatud tingimuste kohaselt õigus tõhusale õiguskaitsevahendile kohtus. Selle artikli teises lõigus on sätestatud, et igaühel on õigus asja arutamisele sõltumatus ja erapooletus kohtus.

187 Väljakujunenud kohtupraktika kohaselt on tõhusa kohtuliku kontrolli olemasolu, mille eesmärk on tagada liidu õigusnormide järgimine, juba iseenesest õigusriigi olemuslik tunnus. Seega ei järgi õigusakt, milles ei ole õigussubjektile 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 olemust (6. oktoobri 2015. aasta kohtuotsus Schrems, C-362/14, EU:C:2015:650, punkt 95 ja seal viidatud kohtupraktika).

188 Isikuandmete kaitse üldmääruse artikli 45 lõike 2 punktis a on sellega seoses nõutud, et komisjon võtaks kolmanda riigi poolt tagatud kaitse taseme piisavuse hindamisel muu hulgas arvesse „tõhusa haldus- ja õiguskaitse olemasolu andmesubjektide jaoks, kelle isikuandmeid edastatakse“. Isikuandmete kaitse üldmääruse põhjenduses 104 on sellega seoses rõhutatud, et „kolmas riik [peaks] tagama andmete kaitse tõhusa ja sõltumatu järelevalve ja nägema ette liikmesriikide andmekaitseasutustega tehtava koostöö mehhanismid“, ja täpsustatud, et „andmesubjektidele [tuleks] tagada tõhusad ja kohtulikult kaitstavad õigused ning tõhus haldus- ja õiguskaitse“.

189 Selliste tõhusate õiguskaitsevahendite olemasolu asjasse puutuvas kolmandas riigis on eriti tähtis kontekstis, kus on tegemist isikuandmete edastamisega sellesse kolmandasse riiki, kuna nähtuvalt isikuandmete kaitse üldmääruse põhjendusest 116 võib andmesubjekt sattuda olukorda, kus liidu haldusasutustel ja kohtutel puuduvad piisavad volitused ja vahendid, saavutamaks tulemuslikku lahendust andmesubjekti kaebusele, mille kohaselt on tema kolmandasse riiki edastatud isikuandmeid seal õigusvastaselt töödeldud, mistõttu ta on sunnitud pöörduma selle kolmanda riigi ametivõimude ja riigisiseste kohute poole.

190 Käesoleval juhul on komisjoni poolt Privacy Shieldi otsuses tehtud järeldus, et USA tagab harta artikliga 47 tagatuga sisuliselt samaväärse kaitse taseme, seatud kahtluse alla eelkõige põhjusel, et andmekaitseraamistiku Privacy Shield ombudsmani ametikoha loomine ei saa täita komisjoni enda poolt tuvastatud lünki nende isikute kohtulikus kaitses, kelle isikuandmeid sellesse kolmandasse riiki edastatakse.

191 Sellega seoses märkis komisjon Privacy Shieldi otsuse põhjenduses 115, et kuigi „[füüsilistele] isikutele, sealhulgas [liidu] andmesubjektidele, keda on riikliku julgeoleku huvides ebaseaduslikult (elektrooniliselt) jälgitud, on saadaval erinevaid õiguskaitsevõimalusi, on samas selge, et vähemalt mõnesid USA luureametkondade kasutatavaid õiguslikke aluseid (nt korraldust E.O. 12333) need ei hõlma“. Seega tõi ta nimetatud põhjenduses 115 esile, et seoses korraldusega E.O. 12333 puuduvad igasugused õiguskaitsevahendid. Käesoleva kohtuotsuse punktis 187 viidatud kohtupraktika kohaselt ei ole sellise lünga tõttu kohtulikus kaitses presidendi korraldusel põhinevatest jälgimisprogrammidest tulenevate riivete eest võimalik teha järeldust – nagu tegi komisjon Privacy Shieldi otsuses –, et USA õigus tagab harta artikliga 47 tagatuga sisuliselt samaväärse kaitse taseme.

192 Mis lisaks puudutab nii FISA artiklil 702 kui ka korraldusel E.O. 12333 põhinevaid jälgimisprogramme, siis käesoleva kohtuotsuse punktides 181 ja 182 on märgitud, et ei suunis PPD-28 ega korraldus E.O. 12333 ei anna andmesubjektidele USA ametivõimude vastu kohtulikult kaitstavaid õigusi, mistõttu neil isikutel puudub õigus tõhusale õiguskaitsevahendile.

193 Komisjon on Privacy Shieldi otsuse põhjendustes 115 ja 116 siiski tõdenud, et kuna on olemas USA ametivõimude loodud ombudsmani mehhanism, mida on kirjeldatud USA riigisekretäri 7. juuli 2016. aasta kirjas Euroopa Komisjoni õigus- ja tarbijaküsimuste ning soolise võrdõiguslikkuse volinikule, mis sisaldub selle otsuse III lisas, ja kuna ombudsmanile on pandud ülesanne olla „rahvusvahelise infotehnoloogiaalase diplomaatia vanemkoordinaator“, võib USA puhul asuda seisukohale, et seal on tagatud harta artikliga 47 tagatuga sisuliselt samaväärne kaitse tase.

194 Küsimust, kas Privacy Shieldi otsuses kirjeldatud ombudsmani mehhanism võimaldab tõepoolest korvata komisjoni tuvastatud puudujääke õiguses kohtulikule kaitsele, peab vastavalt harta artiklist 47 ja käesoleva kohtuotsuse punktis 187 viidatud kohtupraktikast tulenevatele nõuetele hindama, lähtudes põhimõttest, et õigussubjektil peab olema võimalus kasutada õiguskaitsevahendeid sõltumatus ja erapooletus kohtus, et tutvuda teda puudutavate isikuandmetega või lasta neisse parandusi teha või neid kustutada.

195 Käesoleva kohtuotsuse punktis 193 mainitud kirjas on andmekaitseraamistiku Privacy Shield ombudsmani aga kirjeldatud küll kui „luureühendusest sõltumatut“, kuid alluvat „otse riigisekretärile, kes tagab, et ombudsman täidab oma kohustusi objektiivselt ning väärmõjudeta, mis võiksid tema antavaid otsuseid mõjutada“. Peale asjaolu, et ombudsmani määrab riigisekretär ja ta kuulub välisministeeriumi koosseisu, nagu tõdes komisjon selle otsuse punktis 116, ei sisalda see otsus ühtki viidet sellele, et ombudsmani tagandamine või tema ametisse nimetamise otsuse tühistamine eeldaks erilisi kaitsemeetmeid, see aga seab kahtluse alla ombudsmani sõltumatuse täitevvõimust, nagu osutas kohtujurist oma ettepaneku punktis 337 (vt selle kohta 21. jaanuari 2020. aasta kohtuotsus Banco de Santander, C-274/14, EU:C:2020:17, punktid 60 ja 63 ning seal viidatud kohtupraktika).

196 Samuti tuleb nõustuda kohtujuristi ettepaneku punktis 338 rõhutatuga, et kuigi Privacy Shieldi otsuse põhjenduses 120 on mainitud USA valitsuse lubadust, et asjaomane luureteenistuse üksus peab andmekaitseraamistiku Privacy Shield ombudsmani poolt tuvastatud normide mis tahes rikkumise parandama, ei ole selles otsuses ühtki viidet sellele, et ombudsmanil on pädevus teha luureteenistustele siduvaid otsuseid, ega ole tuvastatud ühtki selle lubadusega kaasnevat seadusest tulenevat kaitsemeedet, millele andmesubjektid tugineda saaksid.

197 Seega ei anna Privacy Shieldi otsuses käsitletud ombudsmani mehhanism andmesubjektidele, kelle andmeid edastatakse USAsse, õiguskaitsevahendit sellises organis, kes pakub harta artiklis 47 ette nähtutega sisuliselt samaväärseid kaitsemeetmeid.

198 Järelikult, kuna komisjon tuvastas Privacy Shieldi otsuse artikli 1 lõikes 1, et USA tagab ELi-USA andmekaitseraamistiku Privacy Shield alusel piisava kaitse taseme isikuandmetele, mis edastatakse liidust selle kolmandas riigis asuvatele organisatsioonidele, on ta rikkunud nõudeid, mis tulenevad isikuandmete kaitse üldmääruse artikli 45 lõikest 1, tõlgendatuna lähtuvalt harta artiklitest 7, 8 ja 47.

199 Sellest järeldub, et Privacy Shieldi otsuse artikkel 1 on vastuolus isikuandmete kaitse üldmääruse artikli 45 lõikega 1, tõlgendatuna lähtuvalt harta artiklitest 7, 8 ja 47, ja seetõttu kehtetu.

200 Kuna Privacy Shieldi otsuse artikkel 1 on selle otsuse artiklitest 2–6 ning otsuse lisadest lahutamatu, mõjutab selle kehtetus kogu otsuse kehtivust.

201 Kõiki eeltoodud kaalutlusi arvestades tuleb teha järeldus, et Privacy Shieldi otsus on kehtetu.

202 Seoses küsimusega, kas selle otsuse tagajärjed tuleks jätta kehtima, et vältida õiguslünga tekkimist (vt selle kohta 28. aprilli 2016. aasta kohtuotsus Borealis Polyolefine jt, C-191/14, C-192/14, C-295/14, C-389/14 ja C-391/14–C-393/14, EU:C:2016:311, punkt 106), tuleb tõdeda, et isikuandmete kaitse üldmääruse artiklit 49 arvesse võttes ei tekita sellise kaitse piisavuse tuvastamise otsuse nagu Privacy Shieldi otsus kehtetuks tunnistamine sellist õiguslünka. Selles artiklis on nimelt täpselt sätestatud tingimused, mis üldmääruse artikli 45 lõikes 3 ette nähtud kaitse piisavuse otsuse või üldmääruse artiklis 46 osutatud asjakohaste kaitsemeetmete puudumisel peavad olema täidetud, et isikuandmeid oleks lubatud kolmandasse riiki edastada.

Kohtukulud

203 Kuna põhikohtuasja poolte jaoks on käesolev menetlus eelotsusetaotluse esitanud kohtus pooleli oleva asja üks staadium, otsustab kohtukulude jaotuse liikmesriigi 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 27. aprilli 2016. aasta määruse (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) artikli 2 lõikeid 1 ja 2 tuleb tõlgendada nii, et selle määruse kohaldamisalasse kuulub olukord, kus liikmesriigis asuv äriühing edastab ärilisel eesmärgil isikuandmeid kolmandas riigis asuvale teisele äriühingule, olenemata asjaolust, et edastamise käigus või järel võivad kõnealuseid andmeid töödelda asjaomase kolmanda riigi ametiasutused avaliku korra, riigikaitse ja riikliku julgeolekuga seotud eesmärkidel.**

2. **Määruse 2016/679 artikli 46 lõiget 1 ja artikli 46 lõike 2 punkti c tuleb tõlgendada nii, et nende sätetega nõutavad asjakohased kaitsemeetmed, kohtulikult kaitstavad õigused ja tõhusad õiguskaitsevahendid peavad andmesubjektidele, kelle isikuandmeid edastatakse kolmandasse riiki andmekaitse tüüptingimuste alusel, tagama õiguste kaitse, mille tase on sisuliselt samaväärne sellega, mis on Euroopa Liidus tagatud vastavalt kõnealusele määrusele, tõlgendatuna lähtuvalt Euroopa Liidu põhiõiguste hartast. Selleks et hinnata sellise edastamise korral tagatud kaitse taset, tuleb eelkõige arvesse võtta nii Euroopa Liidus asuva vastutava töötleja või tema volitatud töötleja ja kolmandas riigis asuva isikuandmete vastuvõtja vahel kokku lepitud lepingutingimusi kui ka kolmanda riigi õigussüsteemiga seotud asjakohast teavet, mis puudutab selle riigi ametiasutuste võimalust nõnda edastatavatele isikuandmetele juurde pääseda ja mille hulka kuuluvad eelkõige asjaolud, mis on loetletud kõnealuse määruse artikli 45 lõikes 2.**

3. **Määruse 2016/679 artikli 58 lõike 2 punkte f ja j tuleb tõlgendada nii, et kui puudub Euroopa Komisjoni poolt vastu võetud kehtiv kaitse piisavuse otsus, peab pädev järelevalveasutus peatama või keelama komisjoni poolt vastu võetud andmekaitse tüüptingimuste alusel toimuva andmete edastamise kolmandasse riiki, kui ta kõiki edastamise asjaolusid arvestades leiab, et selles kolmandas riigis neid tingimusi ei järgita või ei saa järgida ja liidu õigusega,**

eelkõige selle määruse artiklitega 45 ja 46 ja põhiõiguste hartaga nõutavat edastatavate andmete kaitset ei ole võimalik tagada muude meetmete abil ning liidus asuv vastutav töötleja või tema volitatud töötleja ei ole ise andmete edastamist peatanud või lõpetanud.

4. **Komisjoni 5. veebruari 2010. aasta otsuse 2010/87/EL kolmandates riikides asuvatele volitatud töötlejatele isikuandmete edastamise lepingu tüüptingimuste kohta Euroopa Parlamendi ja nõukogu direktiivi 95/46/EÜ alusel (muudetud komisjoni 16. detsembri 2016. aasta rakendusotsusega (EL) 2016/2297) analüüsimisel põhiõiguste harta artiklite 7, 8 ja 47 alusel ei ilmnenud asjaolusid, mis mõjutaksid selle otsuse kehtivust.**

5. **Komisjoni 12. juuli 2016. aasta rakendusotsus (EL) 2016/1250 isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ on kehtetu.**

Allkirjad