



18/ET

WP 254 rev. 01

## Artikli 29 tööühm

### Piisavuse võrdlusalus

Vastu võetud 28. novembril 2017

Viimati muudetud ja muudatused vastu võetud 6. veebruaril 2018

Tööühm on asutatud direktiivi 95/46/EÜ artikli 29 alusel. Tegemist on Euroopa sõltumatu nõuandeorganiga andmekaitse ja eraelu puutumatuse küsimustes. Tööühma ülesandeid on kirjeldatud direktiivi 95/46/EÜ artiklis 30 ja direktiivi 2002/58/EÜ artiklis 15.

Sekretariaaditeenused tagab Euroopa Komisjoni õigusküsimuste peadirektoraadi direktoraat C (põhiõigused ja liidu kodakondsus), B-1049 Brüssel, Belgia, kabinet nr MO-59 02/013.

Veebisait: [http://ec.europa.eu/newsroom/article29/news.cfm?item\\_type=1358&tpa\\_id=6936](http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936)

## **Sissejuhatus**

ELi andmekaitseasutuste tööühm<sup>1</sup> (artikli 29 tööühm) on varem avaldanud töödokumendi, milles käsitletakse isikuandmete edastamist kolmandatesse riikidesse (WP 12)<sup>2</sup>. Seoses andmekaitse direktiivi asendamisega ELi isikuandmete kaitse üldmäärusega<sup>3</sup> vaatab artikli 29 tööühm läbi oma varasemad suunised – töödokumendi WP 12 –, et seda uue õigusakti ja Euroopa Liidu Kohtu hiljutise kohtupraktika<sup>4</sup> valguses ajakohastada.

Käesoleva töödokumendi eesmärk on ajakohastada töödokumendi WP 12 esimest peatükki, milles käsitletakse kolmanda riigi, kolmanda riigi territooriumi, kolmanda riigi ühe või mitme kindlaksmääratud sektori või rahvusvahelise organisatsiooni (edaspidi „kolmandad riigid või rahvusvahelised organisatsioonid“) andmekaitse taseme piisavust. Käesolev dokument vaadatakse lähiaastail korduvalt läbi ja vajaduse korral ajakohastatakse seda, lähtudes isikuandmete kaitse üldmääruse kohaldamisel saadud praktilistest kogemustest. Töödokumendi teist peatükki („*Lähenemisviisi kohaldamine riikide suhtes, kes on ratifitseerinud isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni*“) ja kolmandat peatükki („*Lähenemisviisi kohaldamine sektori eneseregulatsiooni suhtes*“) tuleks ajakohastada hiljem.

Käesolevas töödokumendis keskendutakse üksnes kaitse piisavuse otsustele, mis on isikuandmete kaitse üldmääruse artikli 45 kohased Euroopa Komisjoni rakendusaktid<sup>5</sup>. Muid isikuandmete kolmandatesse riikidesse ja rahvusvahelistele organisatsioonidele edastamise aspekte (siduvad kontsernisüsteemide eeskirjad, erandid) uuritakse järgmistes töödokumentides, mis avaldatakse eraldi.

Käesolevas dokumendis antakse Euroopa Komisjonile ja artikli 29 tööühmale isikuandmete kaitse üldmääruse alusel suuniseid kolmandate riikide ja rahvusvaheliste organisatsioonide andmekaitse taseme hindamiseks, määrates kindlaks peamised andmekaitsepõhimõtted, mida tuleb kolmanda riigi õigusraamistikus või rahvusvahelises organisatsioonis järgida, et tagada sisuline samaväärsus ELi raamistikuga. Peale selle võivad sellest dokumendist juhtnööre saada piisavuse saavutamiseks huvitatud kolmandad riigid ja rahvusvahelised organisatsioonid. Käesolevas töödokumendis sätestatud põhimõtted ei ole siiski suunatud otse vastutavatele või volitatud töötajatele.

Töödokument koosneb järgmisest neljast peatükist.

**1. peatükk:** üldist teavet piisavuse mõiste kohta;

**2. peatükk:** isikuandmete kaitse üldmääruse kohased kaitse piisavuse otsuste menetluslikud aspektid;

**3. peatükk:** üldised andmekaitsepõhimõtted. Selles peatükis sätestatakse peamised andmekaitse üldpõhimõtted, millega tagatakse, et andmekaitse tase kolmandas riigis või rahvusvahelises organisatsioonis on sisuliselt samaväärne tasemega, mis on ette nähtud ELi õigusaktidega.

**4. peatükk:** olulised tagatised õiguskaitseasutuste ja riiklike julgeolekuasutuste juurdepääsul isikuandmetele, millega piiratakse sekkumist põhiõigustesse. See peatükk sisaldab õiguskaitseasutuste ja riiklike julgeolekuasutuste juurdepääsul kohaldatavaid olulisi tagatiseid, mis põhinevad 2015. aastal Euroopa Liidu Kohtus tehtud Schremsi kohtuotsusel ja 2016. aastal vastu võetud artikli 29 tööühma töödokumendil oluliste tagatiste kohta.

---

<sup>1</sup> Loodud ELi andmekaitse direktiivi 95/46/EÜ artikli 29 alusel.

<sup>2</sup> Töödokument „Isikuandmete edastamine kolmandatesse riikidesse: ELi andmekaitse direktiivi artiklite 25 ja 26 kohaldamine“ (WP 12), mille artikli 29 tööühm võttis vastu 24. juulil 1998.

<sup>3</sup> Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (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) (EMPs kohaldatav tekst).

<sup>4</sup> Sh kohtuotsus, 6. oktoober 2015, Maximilian Schrems vs. Data Protection Commissioner, C-362/14.

<sup>5</sup> Lisateavet rakendusaktide kohta leiab isikuandmete kaitse üldmääruse artikli 45 lõikest 3 ja artikli 93 lõikest 2.

## 1. peatükk. Üldist teavet piisavuse mõiste kohta

Isikuandmete kaitse üldmääruse artikli 45 lõikes 1 on sätestatud põhimõte, et isikuandmeid edastatakse kolmandale riigile või rahvusvahelisele organisatsioonile vaid siis, kui asjaomane kolmas riik või asjaomase kolmanda riigi territoorium või asjaomase kolmanda riigi üks või mitu kindlaksmääratud sektorit või rahvusvaheline organisatsioon tagab isikuandmete kaitse piisava taseme.

Euroopa Liidu Kohus on mõistet „kaitse piisav tase“, mida kasutati juba direktiivi 95/46 alusel, edasi arendanud. Siinkohal on oluline meenutada standardit, mille Euroopa Liidu Kohus on kehtestanud Schremsi kohtuotsusega, kus on öeldud, et kaitse tase kolmandas riigis peab olema „sisuliselt samaväärne“ sellega, mis on tagatud ELis, kuid „vahendid, mida kolmas riik sellega seoses niisuguse kaitsetaseme saavutamiseks kasutab, võivad olla erinevad nendest, mida liidus rakendatakse“<sup>6</sup>. Seepärast ei ole eesmärk kopeerida punkt-punktilt Euroopa õigusakte, vaid teha kindlaks asjaomaste õigusaktide kõige olulisemad nõuded.

Euroopa Komisjoni piisavusotsuste eesmärk on liikmesriikidele siduval viisil<sup>7</sup> ametlikult kinnitada, et andmekaitse tase kolmandas riigis või rahvusvahelises organisatsioonis on sisuliselt samaväärne andmekaitse tasemega Euroopa Liidus<sup>8</sup>. Piisavust on võimalik saavutada, kui omavahel kombineeritakse andmesubjektide õigused ja andmete töötajate või töötlemist kontrollivate isikute kohustused ning sõltumatute organite teostatav järelevalve. Samas on andmekaitse-eeskirjad tulemuslikud vaid siis, kui on võimalik tagada nende täitmine ja kui neist praktikas kinni peetakse. Seetõttu on kolmandasse riiki või rahvusvahelisele organisatsioonile edastatavate isikuandmete suhtes kohaldatavate normide sisu kõrval vaja vaadelda ka süsteemi, mis on sisse seatud nende normide tulemuslikkuse tagamiseks. Andmekaitse-eeskirjade tulemuslikkuse seisukohast on väga oluline, et olemas oleksid tõhusad mehhanismid nende eeskirjade täitmise tagamiseks.

Isikuandmete kaitse üldmääruse artikli 45 lõikes 2 on kindlaks määratud asjaolud, mida Euroopa Komisjon võtab arvesse hinnates seda, kas kaitse tase kolmandas riigis või rahvusvahelises organisatsioonis on piisav.

Näiteks võtab komisjon arvesse õigusriigi põhimõtet, inimõiguste ja põhivabaduste austamist, asjaomaseid õigusakte, ühe või mitme sõltumatu järelevalveasutuse olemasolu ja tõhusat toimimist ning kolmanda riigi või rahvusvahelise organisatsiooni rahvusvahelisi kohustusi.

Seepärast on selge, et ükskõik milline kaitse piisavuse sisuline analüüs peab sisaldama kaht põhielementi: kohaldatavate normide sisu ja vahendid, millega tagatakse nende tulemuslik kohaldamine. Euroopa Komisjoni ülesanne on korrapäraselt kontrollida, kas kehtestatud normid ka praktikas toimivad.

Peamised andmekaitse üldpõhimõtted ja menetlus-/jõustamisnõuded, mida võib lugeda vajalikuks miinimumiks, et kaitse oleks piisav, on tuletatud ELi põhiõiguste hartast ja isikuandmete kaitse üldmäärusest. Lisaks tuleks arvesse võtta muid rahvusvahelisi andmekaitsealaseid kokkuleppeid, näiteks isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni<sup>9</sup>.

Samuti tuleb tähelepanu pöörata õigusraamistikule, mida kohaldatakse avaliku sektori asutuste juurdepääsul isikuandmetele. Lisasuuniseid sellel kohta on esitatud töödokumendis WP 237 (olulisi tagatisi käsitlev dokument),<sup>10</sup> milles vaadeldakse jälgimistegevusega seoses kohaldatavaid kaitsemeetmeid.

<sup>6</sup> Kohtuotsus, 6. oktoober 2015, Maximillian Schrems vs. Data Protection Commissioner, C-362/14, punktid 73 ja 74.

<sup>7</sup> ELi toimimise lepingu artikli 288 lõige 2.

<sup>8</sup> Kohtuotsus, 6. oktoober 2015, Maximillian Schrems vs. Data Protection Commissioner, C-362/14, punkt 52.

<sup>9</sup> Isikuandmete kaitse üldmääruse põhjendus 105.

<sup>10</sup> Töödokument 01/2016, milles käsitletakse eraelu puutumatuse ja andmekaitsega seotud põhiõigustesse sekkumise põhjendatust juhul, kui isikuandmete edastamisel rakendatakse jälgimismeetmeid (Euroopa olulised tagatised), 16/EN WP 237, 13. aprill 2016.

Üldistest sätetest isikuandmete kaitse ja eraelu puutumatuse kohta kolmandas riigis ei piisa. Kolmanda riigi või rahvusvahelise organisatsiooni õigusraamistik peab sisaldama erisätteid, milles käsitletakse isikuandmete kaitse õiguse praktiliste aspektidega seotud konkreetseid vajadusi. Need sätted peavad olema jõustatavad.

## **2. peatükk. Isikuandmete kaitse üldmääruse kohased kaitse piisavuse otsuste menetluslikud aspektid**

Et Euroopa Andmekaitsekoostöökoostöö saaks täita oma ülesannet nõustada Euroopa Komisjoni koostöös isikuandmete kaitse üldmääruse artikli 70 lõike 1 punktiga s, tuleks andmekaitsekoostöökoostööle esitada asjakohased dokumendid, sealhulgas asjakohane kirjavahetus ja Euroopa Komisjoni järeldused. Kui õigusraamistik on keeruline, peaksid nende dokumentide hulka kuuluma ka kõik kolmanda riigi või rahvusvahelise organisatsiooni andmekaitse taseme kohta koostatud aruanded. Euroopa Komisjoni esitatav teave peab igal juhul olema põhjalik ning võimaldama Euroopa Andmekaitsekoostöökoostööle esitada hinnang andmekaitse taseme kohta kolmandas riigis. Euroopa Andmekaitsekoostöökoostöö esitab õigeaegselt arvamuse Euroopa Komisjoni järelduste kohta ja teeb kindlaks andmekaitse piisavuse tagamise raamistikus esinevad võimalikud puudused. Samuti püüab andmekaitsekoostöökoostöö esitada kohandamis- või muutmissettepanekud, et võimalikud puudused kõrvaldada.

Vastavalt isikuandmete kaitse üldmääruse artikli 45 lõikele 4 on Euroopa Komisjoni ülesanne pidevalt jälgida suundumusi, mis võivad mõjutada kaitse piisavuse otsuse toimimist.

Isikuandmete kaitse üldmääruse artikli 45 lõikes 3 on sätestatud, et korrapärane läbivaatamine peab toimuma vähemalt nelja aasta tagant. See on siiski üldine ajakava, mida tuleb kohandada iga kolmanda riigi või rahvusvahelise organisatsiooni puhul, kelle kohta on tehtud kaitse piisavuse otsus. Sõltuvat konkreetsetest asjaoludest võib ette näha lühema läbivaatamise tsükli. Ka vahejuhtumid või muu teave asjaomase kolmanda riigi või rahvusvahelise organisatsiooni õigusraamistiku või sellesse tehtud muudatuste kohta võivad kaasa tuua vajaduse vaadata kõnealune otsus läbi ettenähtust varem. Samuti tundub olevat asjakohane vaadata täiesti uus kaitse piisavuse otsus esimest korda läbi võrdlemisi ruttu ja sõltuvalt läbivaatamise tulemusest läbivaatamise tsükli järk-järgult kohandada.

Kuna Euroopa Andmekaitsekoostöökoostöö on volitus esitada Euroopa Komisjonile arvamus selle kohta, kas kolmandas riigis, kolmanda riigi territooriumil või kolmanda riigi ühes või mitmes kindlaksmääratud sektoris või rahvusvahelises organisatsioonis ei ole enam tagatud piisaval tasemel kaitset, peab andmekaitsekoostöökoostöö saama õigeaegselt sisulist teavet Euroopa Komisjoni tegevuse kohta asjaomases kolmandas riigis või rahvusvahelises organisatsioonis esinevate suundumuste jälgimisel. Seega tuleb andmekaitsekoostöökoostöö alati kursis hoida otsuse läbivaatamise protsessiga ja kolmandasse riiki või rahvusvahelisse organisatsiooni tehtavate kontrollkäikudega. Euroopa Andmekaitsekoostöökoostöö oleks hea meel kutse üle neis läbivaatamistes ja kontrollkäikudes osaleda.

Märkida tuleks ka seda, et vastavalt isikuandmete kaitse üldmääruse artikli 45 lõikele 5 on Euroopa Komisjonil õigus kehtiv kaitse piisavuse otsus kehtetuks tunnistada, seda muuta või peatada selle kehtivus. Otsuse kehtetuks tunnistamise, muutmise või kehtivuse peatamise protsessi tuleks kaasata Euroopa Andmekaitsekoostöökoostöö, kelle arvamust tuleks küsida koostöös artikli 70 lõike 1 punktiga s.

Peale selle, nagu on nüüd tunnistatud isikuandmete kaitse üldmääruse artikli 58 lõikes 5 ja vastavalt Euroopa Liidu Kohtu otsusele Schremsi kohtuasjas peab andmekaitseasutusel olema võimalik osaleda kohtumenetluses, kui ta leiab, et nõue, mille isik on esitanud seoses kaitse piisavuse otsusega, on põhjendatud: „Sellega seoses on liikmesriigi seadusandja kohustatud ette nägema õiguskaitsevahendid, mis võimaldavad järelevalveasutusel esitada siseriiklikes kohtutes väiteid, mida ta peab põhjendatuks, selleks et kohtud juhul, kui neil on komisjoni otsuse kehtivuse suhtes samasugused kahtlused, esitaksid eelotsusetaotluse kõnealuse otsuse kehtivuse analüüsimiseks“<sup>11</sup>.

<sup>11</sup> Kohtuotsus, 6. oktoober 2015, Maximilian Schrems vs. Data Protection Commissioner, C-362/14, punkt 65.

**3. peatükk. Üldised andmekaitsepõhimõtted, millega tagatakse, et andmekaitse tase kolmandas riigis, kolmanda riigi territooriumil, kolmanda riigi ühes või mitmes kindlaksmääratud sektoris või rahvusvahelises organisatsioonis on sisuliselt samaväärne tasemega, mis on tagatud ELi õigusaktidega**

**Kolmanda riigi või rahvusvahelise organisatsiooni süsteem peab sisaldama järgmisi peamisi andmekaitse üldpõhimõtteid ning menetlus-/jõustamis põhimõtteid ja -mehhanisme.**

#### **A. Üldpõhimõtted**

##### **1) Mõisted**

Rakendada tuleks peamisi andmekaitsemõisteid ja/või -põhimõtteid. Need ei pea vastama täpselt isikuandmete kaitse üldmääruses kasutatud terminoloogiale, kuid peaksid kajastama Euroopa andmekaitseõiguses sätestatud mõisteid ja olema nendega kooskõlas. Isikuandmete kaitse üldmäärus sisaldab näiteks järgmisi olulisi mõisteid: isikuandmed, isikuandmete töötlemine, vastutav töötleja, volitatud töötleja, vastuvõtja ja tundlikud andmed.

##### **2) Õiguspärasel eesmärgidel toimuva seadusliku ja õiglasel töötlemise alused**

Andmeid tuleb töödelda seaduslikult, õiglaselt ja õiguspäraselt.

Õiguslikud alused, millele tuginedes võib andmeid seaduslikult, õiglaselt ja õiguspäraselt töödelda, tuleks sätestada piisavalt selgelt. Euroopa õigusraamistikus tunnistatakse mitut sellist õiguslikku alust, näiteks sätted liikmesriigi õiguses, andmesubjekti nõusolek, lepingu täitmine või vastutava töötleja või kolmanda isiku õigustatud huvi, mis ei kaalu üles üksikisiku huve.

##### **3) Eesmärgi piiramise põhimõte**

Andmeid tuleks töödelda konkreetsel eesmärgil ja kasutada seejärel üksnes sel määral, mil see on kooskõlas töötlemise eesmärgiga.

##### **4) Andmete kvaliteedi ja proportsionaalsuse põhimõte**

Andmed peaksid olema õiged ja vajaduse korral ajakohastatud. Andmed peaksid olema piisavad ja asjakohased ning nad ei tohi olla töötlemise eesmärgi silmas pidades ülemääraseks.

##### **5) Andmete säilitamise põhimõte**

Isikuandmeid ei tohiks üldjuhul säilitada kauem kui see on vajalik andmete töötlemise eesmärgi täitmiseks.

##### **6) Turvalisuse ja konfidentsiaalsuse põhimõte**

Isikuandmeid töötlev üksus peaks kandma asjakohaseid tehnilisi või korralduslikke meetmeid kasutades hoolt selle eest, et andmeid töödeldakse viisil, millega on tagatud andmete turvalisus, sealhulgas kaitse loata või ebaseadusliku töötlemise ning juhusliku kaotamise, hävitamise või kahjustamise eest. Turvalisuse taseme puhul tuleks arvesse võtta teaduse ja tehnoloogia viimast arengut ja seonduvaid kulusid.

## **7) Läbipaistvuse põhimõte**

Igale üksikisikule tuleks anda selget, kergesti kättesaadavat, kokkuvõtlikku, läbipaistvat ja arusaadavat teavet kõikide tema isikuandmete töötlemise põhiaspektide kohta. Selline teave peaks hõlmama töötlemise eesmärki, vastutava töötleja nime, asjaomase isiku õigusi ja muud õigluse tagamiseks vajalikku teavet. Teatud tingimustel võidakse teha sellest teabe saamise õigusest erand, näiteks et kaitsta kriminaaluurimisi, riigi julgeolekut, kohtusüsteemi sõltumatust ja kohtumenetlusi või muid üldist avalikku huvi pakkuvaid olulisi eesmärke, nagu on sätestatud isikuandmete kaitse üldmääruse artiklis 23.

## **8) Õigus andmetega tutvuda, nõuda andmete parandamist ja kustutamist ning esitada vastuväiteid**

Andmesubjektil peaks olema õigus saada kinnitus selle kohta, kas teda käsitlevaid andmeid töödeldakse, ning õigus oma andmetega tutvuda, sealhulgas saada koopia kõikidest endaga seotud andmetest, mida töödeldakse.

Andmesubjektil peaks olema õigus nõuda kindlaksmääratud põhjustel vajaduse korral oma isikuandmete parandamist, näiteks kui andmed osutuvad ebaõigeks või mittetäielikuks, ja andmete kustutamist, näiteks kui nende töötlemine ei ole enam vajalik või kui see on ebaseaduslik.

Samuti peaks andmesubjektil olema õigus esitada oma konkreetsest olukorrast lähtudes mõjuval õiguspärasel põhjusel igal ajal vastuväiteid oma andmete töötlemisele kolmanda riigi õigusraamistikus kehtestatud konkreetsetel tingimustel. Isikuandmete kaitse üldmääruses hõlmavad sellised tingimused näiteks olukorda, kus töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks, või olukorda, kus töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral.

Nende õiguste kasutamine ei tohiks olla andmesubjektile liiga koormav. Kõnealustest õigustest võidakse teha erandeid, näiteks et kaitsta kriminaaluurimisi, riigi julgeolekut, kohtusüsteemi sõltumatust ja kohtumenetlusi või muid üldist avalikku huvi pakkuvaid olulisi eesmärke, nagu on sätestatud isikuandmete kaitse üldmääruse artiklis 23.

## **9) Andmete edasisaatmise piirangud**

Isikuandmete esmasel vastuvõtjal tuleks lubada saadud andmed edasi saata vaid juhul, kui andmete järgmise vastuvõtja suhtes (st isiku suhtes, kellele andmed edasi saadetakse) kohaldatakse samuti norme (sh lepingust tulenevaid nõudeid), mis tagavad piisaval tasemel kaitse, ja kui kõnealune isik järgib andmete vastutava töötleja nimel töötlemisel asjakohaseid juhiseid. Andmete edasisaatmine ei tohi kahjustada nendele füüsilistele isikutele tagatud kaitse taset, kelle andmeid edastatakse. EList edastatud andmete esmane vastuvõtja peab tagama, et kaitse piisavuse otsuse puudumisel on seoses andmete edasisaatmisega ette nähtud piisavad kaitsemeetmed. Selline andmete edasisaatmine peaks toimuma vaid piiratud ja kindlaksmääratud eesmärkidel ning üksnes seni, kuni selliseks töötlemiseks on õiguslik alus.

## **B. Näited täiendavatest üldpõhimõtetest, mida kohaldada erinevate töötlemisliikide puhul**

### **1) Isikuandmete eriliigid**

Isikuandmete eriliikide<sup>12</sup> töötlemisel tuleks kohaldada konkreetseid kaitsemeetmeid. Need eriliigid on sätestatud isikuandmete kaitse üldmääruse artiklites 9 ja 10. Sellise kaitse tagamiseks tuleks kohaldada andmete töötlemisel rangemaid nõudeid, näiteks et andmesubjekt peab andma töötlemiseks selgesõnalise nõusoleku, või rakendada täiendavaid turvameetmeid.

---

<sup>12</sup> Tuntud ka kui „tundlikud andmed“, millele on osutatud isikuandmete kaitse üldmääruse põhjenduses 10.

## **2) Otseturundus**

Kui andmeid töödeldakse otseturunduse eesmärgil, peaks andmesubjektil olema võimalik esitada igal ajal ja tasuta vastuväiteid oma andmete töötlemisele sel eesmärgil.

## **3) Automatiseeritud otsuste tegemine ja profiilianalüüs**

Otsuseid, mis põhinevad üksnes automaatsel isikuandmete töötlemisel (automatiseeritud töötlusel põhinevate üksikotsuste tegemine), sealhulgas profiilianalüüsil, ja mis toovad kaasa õiguslikke tagajärgi või avaldavad andmesubjektile olulist mõju, võib teha üksnes teatavatel kolmanda riigi õigusraamistikus kehtestatud tingimustel. Euroopa õigusraamistikus kuuluvad selliste tingimuste hulka näiteks vajadus saada andmesubjektilt selgesõnaline nõusolek või sellise otsuse vajalikkus lepingu sõlmimiseks. Andmesubjektil peaks olema õigus sellele, et tema kohta ei tehta otsust, mis ei ole kooskõlas selliste kolmanda riigi õigusraamistikus sätestatud tingimustega. Kolmanda riigi õiguses peaksid igal juhul olema ette nähtud vajalikud kaitsemeetmed, sealhulgas õigus saada teavet otsuse tegemise konkreetsete põhjuste ja kasutatud loogika kohta, õigus ebaõige või mittetäieliku teabe parandamisele ning õigus otsus vaidlustada, kui selle vastuvõtmisel on lähtutud ebaõigetest faktidest.

## **C. Menetlus-/jõustamismehhanismid**

**Ehkki vahendid, mida kolmas riik kasutab kaitse piisava taseme tagamiseks, võivad olla erinevad nendest, mida rakendatakse Euroopa Liidus<sup>13</sup>, peab Euroopa süsteemiga kooskõlas olev süsteem hõlmama järgmisi elemente.**

### **1) Pädev sõltumatu järelevalveasutus**

Olemas peaks olema üks või mitu sõltumatut järelevalveasutust, kelle ülesanne on teostada järelevalvet andmekaitse ja eraelu puutumatuse alaste sätete järgimise üle kolmandas riigis ning tagada nendest sätetest kinnipidamine. Järelevalveasutus peab tegutsema oma ülesannete täitmisel ja volituste kasutamisel täiesti sõltumatult ja erapooletult ning ei tohi kelleltki küsida ega võtta vastu juhiseid. Sellega seoses peaks järelevalveasutusel olema kõik vajalikud volitused ja ülesanded, et tagada andmekaitseõiguste järgimine ja suurendada teadlikkust. Tähelepanu tuleks pöörata ka järelevalveasutuse töötajatele ja eelarvele. Samuti peaks järelevalveasutusel olema võimalik korraldada omal algatusel uurimisi.

### **2) Andmekaitse süsteem peab tagama, et üldiselt järgitakse andmekaitse norme hästi**

Kolmanda riigi süsteem peaks tagama vastutavate töötajate ja nende nimel andmeid töötlevate isikute suure vastutuse ja teadlikkuse oma kohustustest, ülesannetest ja vastutusest ning andmesubjektide teadlikkuse oma õigustest ja nende kasutamise vahenditest. Eeskirjade täitmise tagamisel võib olla oluline roll tõhusatel ja heidutatavatel karistustel, nagu ka ametiasutuste, audiitorite või sõltumatute andmekaitseametnike teostatava otsese kontrolli süsteemidel.

### **3) Vastutus**

Kolmanda riigi andmekaitseraamistik peaks kohustama vastutavaid töötlejaid ja/või nende nimel isikuandmeid töötlevaid isikuid andmekaitseraamistikust kinni pidama ja tagama, et nad on võimelised normide järgimist eelkõige pädevale järelevalveasutusele tõendama. Selleks kasutatavate meetmete hulka võivad kuuluda näiteks andmekaitsealased mõjuhinnangud, isikuandmete töötlemise toimingute

---

<sup>13</sup> Kohtuotsus, 6. oktoober 2015, Maximilian Schrems vs. Data Protection Commissioner, C-362/14, punkt 74.

registri pidamine või logifailide säilitamine asjakohase ajavahemiku jooksul, andmekaitseametniku määramine või lõimitud ja vaikimisi andmekaitse.

**4) Andmekaitse süsteem peab toetama ja abistama üksikuid andmesubjekte nende õiguste kasutamisel ning pakkuma asjakohaseid õiguskaitsemehhanisme**

Üksikisikul peaks olema võimalik kasutada õiguskaitsevahendeid, et teostada oma õigusi kiiresti ja tulemuslikult ning ilma tõkestavate kuludeta ning tagada normide täitmine. Selleks peavad olema sisse seatud järelevalvemehhanismid, mis võimaldavad sõltumatult kaebusi uurida ning teha kindlaks isikuandmete kaitse ja eraelu austamise õiguse mis tahes rikkumine ja selle eest karistada.

Juhuks kui normidest kinni ei peeta, tuleks andmesubjektile ette näha ka tõhus haldus- ja õiguskaitse, sealhulgas hüvitis tema isikuandmete ebaseadusliku töötlemisega tekitatud kahju eest. See on oluline element, mis peab hõlmama vaidluste sõltumatu lahendamise või vahekohtu süsteemi, mis võimaldab maksta hüvitist või määrata karistuse, kui see on asjakohane.



#### **4. peatükk. Olulised tagatised kolmandates riikides õiguskaitseasutuste ja riiklike julgeolekuasutuste juurdepääsul isikuandmetele, millega piiratakse sekkumist põhiõigustesse**

Kaitse taseme piisavuse hindamisel on komisjon isikuandmete kaitse üldmääruse artikli 45 lõike 2 punkti a alusel kohustatud arvesse võtma asjaomaseid õigusakte, nii üldiseid kui ka valdkondlikke, sealhulgas õigusakte, mis käsitlevad avalikku julgeolekut, kaitset, riiklikku julgeolekut, karistusõigust ja riigiasutuste juurdepääsu isikuandmetele, ning selliste õigusaktide rakendamist.

Euroopa Liidu Kohus märgib Schremsi kohtuotsuses, et „väljendit „kaitse piisav tase“ [tuleb] siiski mõista nii, et see nõuab, et kolmas riik tõepoolest tagab oma siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega põhiõiguste ja -vabaduste kaitse taseme, mis on sisuliselt samaväärne sellega, mis on liidus tagatud vastavalt direktiivile 95/46 koostoimes hartaga“. Kuigi vahendid, mida kolmas riik sellega seoses kasutab, võivad olla erinevad nendest, mida liidus rakendatakse, peavad need vahendid siiski praktikas osutama tõhusaks<sup>14</sup>.

Sellega seoses märgib kohus kriitiliselt ka seda, et programmi Safe Harbor käsitlev varasem otsus ei sisalda „mingeid järeldusi selle kohta, et Ameerika Ühendriikides kehtiks riigi tasandil õigusnorme, mille eesmärk oleks piirata võimalikke sekkumisi nende isikute põhiõigustesse, kelle andmeid edastatakse liidust Ameerika Ühendriikidesse, kusjuures neid sekkumisi on selle riigi asutustel lubatud toime panna, kui nad taotleavad õiguspäraseid eesmäärke, nagu riiklik julgeolek“.

Artikli 29 töörühm on määranud 13. aprillil 2016 vastu võetud töödokumendis WP 237 kindlaks olulised tagatised, mis kajastavad Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu kohtupraktikat järelevalve valdkonnas. Ehkki selles töödokumendis esitatud soovitused jäävad kehtima ja neid tuleks arvesse võtta kolmanda riigi järelevalve piisavuse hindamisel, võidakse neid tagatise kohaldada teisiti olukorras, kus on tegemist õiguskaitseasutuste ja riiklike julgeolekuasutuste juurdepääsuga andmetele. Kõik kolmandad riigid peavad selleks, et nende kaitse taset peetaks piisavaks, siiski järgima nii riigi julgeoleku kui ka õiguskaitse huvides andmetele juurdepääsu andmisel neid nelja tagatist:

- 1) töötlemine peab põhinema selgetel, täpsetel ja ligipääsetavatel normidel (õiguslik alus);**
- 2) taotletavate õiguspärase eesmärkidega seoses tuleb tõendada töötlemise vajalikkust ja proportsionaalsust;**
- 3) töötlemise üle tuleb teostada sõltumatut järelevalvet;**
- 4) üksikisikutele peavad olema kättesaadavad tõhusad õiguskaitsevahendid.**

---

<sup>14</sup> Kohtuotsus, 6. oktoober 2015, Maximilian Schrems vs. Data Protection Commissioner, C-362/14, punkt 74.