Soovitused 01/2021 õiguskaitsedirektiivi kohase piisavuse võrdlusaluse kohta

Vastu võetud 2. veebruaril 2021

Sisukord

Euroopa Andmekaitsenõukogu

Võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiivi (EL) 2016/680 (mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK)[1] artikli 51 lõike 1 punkti b,

võttes arvesse oma kodukorra artiklit 12 ja artiklit 22,

ON VASTU VÕTNUD KÄESOLEVAD SOOVITUSED

1. SISSEJUHATUS

1. Artikli 29 alusel asutatud andmekaitse töörühm (WP29) on avaldanud töödokumendi[2] isikuandmete kaitse üldmääruse kohase piisavuse võrdlusaluse kohta[3]. Töödokumendi kinnitas Euroopa Andmekaitsenõukogu (EDPB) oma esimesel täiskogul.

2. Nagu on öeldud Lissaboni lepingule lisatud deklaratsioonis nr 21, võivad kriminaalasjades tehtava õigusalase koostöö ja politseikoostöö valdkonnas nende valdkondade erilise laadi tõttu osutuda vajalikuks Euroopa Liidu toimimise lepingu artikli 16 kohased erieeskirjad, mis käsitlevad üksikisikute kaitset isikuandmete töötlemisel ja selliste andmete vaba liikumist.

3. Sellel alusel võttis ELi seadusandja vastu direktiivi (EL) 2016/680 (edaspidi „õiguskaitsedirektiiv"), millega sätestatakse erinormid seoses pädevates asutustes isikuandmete töötlemisega **süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil.**

4. Õiguskaitsedirektiivis määratakse kindlaks alused, mis võimaldavad selles kontekstis edastada isikuandmeid kolmandasse riiki või rahvusvahelisele organisatsioonile. Üks sellise edastamise alus on Euroopa Komisjoni otsus, et kolmas riik või rahvusvaheline organisatsioon tagab isikuandmete kaitse piisava taseme.

5. Kui piisavuse võrdlusalust käsitleva töödokumendi WP254.rev01 eesmärk on anda Euroopa Komisjonile juhiseid isikuandmete kaitse taseme kohta kolmandates riikides ja rahvusvahelistes organisatsioonides seoses isikuandmete kaitse üldmäärusega, siis käesoleva dokumendi eesmärk on anda samasuguseid juhiseid seoses õiguskaitsedirektiiviga. Selles kontekstis kehtestatakse

[1] ELT L 119, 4.5.2016, lk 89.
[2] WP254.rev01, mille WP29 võttis vastu 28. novembril 2017, viimati muudetud ja muudatused vastu võetud 6. veebruaril 2018. Selles ajakohastatakse töödokumendi I peatükki „Isikuandmete edastamine kolmandatesse riikidesse: ELi andmekaitsedirektiivi artiklite 25 ja 26 kohaldamine", WP 12, mille WP29 võttis vastu 24. juulil 1998.
[3] Euroopa Parlamendi ja nõukogu 26. 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) (ELT L 119, 4.5.2016, lk 1).

dokumendiga kesksed isikuandmete kaitse põhimõtted, mis peavad olema kolmandas riigis või rahvusvahelise organisatsiooni õigusraamistikus olemas, et tagada sisuline samaväärsus ELi raamistikuga õiguskaitsedirektiivi kohaldamisalas (st isikuandmete töötlemiseks pädevates asutustes süütegude tõkestamise, uurimise, avastamise, nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil). Lisaks võib dokument anda juhiseid piisavuse saavutamisest huvitatud kolmandatele riikidele ja rahvusvahelistele organisatsioonidele.

6. Käesolevas dokumendis keskendutakse üksnes piisavusega seotud otsustele. Need on Euroopa Komisjoni rakendusaktid vastavalt õiguskaitsedirektiivi artikli 36 lõikele 3.

2. PIISAVUSE MÕISTE

7. Õiguskaitsedirektiiviga on kehtestatud eeskirjad, mis reguleerivad isikuandmete edastamist kolmandatesse riikidesse ja rahvusvahelistele organisatsioonidele ulatuses, mis kuulub selle direktiivi kohaldamisalasse. Isikuandmete rahvusvahelise edastamise eeskirjad on sätestatud õiguskaitsedirektiivi V peatükis, eelkõige selle artiklites 35–39.

8. Õiguskaitsedirektiivi artikli 36 kohaselt võib isikuandmeid kolmandale riigile või rahvusvahelisele organisatsioonile edastada, kui 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 Kohtu (edaspidi „Euroopa Kohtu“) praktikast[4] lähtuvalt tuleb seda sätet tõlgendada koostoimes õiguskaitsedirektiivi artikliga 35 („Isikuandmete edastamise üldpõhimõtted“), milles sätestatakse, et „kõiki [õiguskaitsedirektiivi V peatüki] sätteid kohaldatakse selleks, et tagada füüsiliste isikute kaitse käesoleva direktiiviga ette nähtud tasemel“.

9. Kui Euroopa Komisjon on otsustanud, et selline isikuandmete kaitse tase on tagatud, võib isikuandmeid edastada sellele kolmandale riigile, territooriumile, sektorile või rahvusvahelisele organisatsioonile ilma eriloata, välja arvatud juhul, kui muu liikmesriik, kust andmed saadi, peab andma edastamiseks loa, nagu on sätestatud õiguskaitsedirektiivi artiklites 35 ja 36 ning põhjenduses 66. See ei mõjuta vajadust töödelda isikuandmeid asjaomaste liikmesriikide asutustes, et täita direktiivi (EL) 2016/680 kohaselt vastu võetud riiklikke sätteid.

10. Euroopa Kohus on isikuandmete kaitse piisava taseme mõistet, mis oli olemas juba direktiivis 95/46[5] ja nõukogu raamotsuses 2008/977/JSK,[6] arendanud edasi nii selles kontekstis kui hiljuti ka isikuandmete kaitse üldmääruses.

11. Nagu Euroopa Kohus osutas, peab kolmanda riigi isikuandmete kaitse tase olema sisuliselt samaväärne sellega, mis on tagatud ELis, „kuigi vahendid sellise kaitsetaseme saavutamiseks võivad olla erinevad nendest, mida liidus rakendatakse“, aga seejuures „peavad need vahendid siiski praktikas osutuma tõhusaks“[7]. Seega ei pea kaitse taseme piisavuse saavutamiseks

[4] Kohtuasi C-311/18, Data Protection Commissioner *vs.* Facebook Ireland Ltd ja Maximillian Schrems, 16. juuli 2020, ECLI:EU:C:2020:559, punkt 92 (Schrems II).
[5] Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EÜT L 281, 23.11.1995, lk 31).
[6] Nõukogu 27. novembri 2008. aasta raamotsus 2008/977/JSK kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta (ELT L 350, 30.12.2008, lk 60).
[7] Kohtuasi C-362/14, Maximillian Schrems *vs.* Data Protection Commissioner, 6. oktoober 2015, ECLI:EU:C:2015:650, punktid 73 ja 74 (Schrems I).

kopeerima punkt-punktilt ELi õigusakte, vaid tuleb kehtestada asjaomaste õigusaktide kõige olulisemad nõuded.

12. Sellega seoses selgitas kohus ka seda, et komisjoni piisavusotsus peaks sisaldama mingeid järeldusi selle kohta, et kolmandas riigis on riigi tasandil olemas õigusnorme, mille eesmärk on piirata võimalikke sekkumisi nende isikute põhiõigustesse, kelle andmeid edastatakse liidust kolmandasse riiki, kusjuures neid sekkumisi on selle riigi asutustel *lubatud* toime panna, kui nad taotlevad õiguspäraseid eesmärke, nagu riiklik julgeolek[8].

13. Euroopa Komisjoni piisavusotsuste eesmärk on liikmesriikidele,[9] sealhulgas nende pädevatele andmekaitseasutustele[10] siduval viisil ametlikult kinnitada, et andmekaitse tase kolmandas riigis või rahvusvahelises organisatsioonis on sisuliselt samaväärne andmekaitse tasemega Euroopa Liidus. Kolmas riik peaks võtma kohustuse tagada piisav kaitse tase, mis sisuliselt vastab liidus tagatava kaitse tasemele, eelkõige juhul, kui andmeid töödeldakse ühes või mitmes kindlaksmääratud sektoris[11].

14. Piisavust on võimalik saavutada, kui omavahel kombineeritakse andmesubjektide õigused ja andmete töötlejate või töötlemist kontrollivate isikute kohustused ning sõltumatute asutuste 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[12].

3. ÕIGUSKAITSEDIREKTIIVI KOHASED KAITSE PIISAVUSE OTSUSTE MENETLUSLIKUD ASPEKTID

15. Et Euroopa Andmekaitsenõukogu saaks täita oma ülesannet nõustada Euroopa Komisjoni kooskõlas õiguskaitsedirektiivi artikli 51 lõike 1 punktiga g, tuleks andmekaitsenõukogule anda asjakohased dokumendid, sealhulgas asjakohane kirjavahetus ja Euroopa Komisjoni järeldused. On ülimalt vajalik, et kõik dokumendid edastatakse andmekaitsenõukogule piisavalt varakult ja tõlgitakse inglise keelde, et võimaldada enne piisavusotsuste lõplikku vastuvõtmist teavitatud ja kasulikke arutelusid. 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 Andmekaitsenõukogul hinnata komisjoni tehtud analüüsi andmekaitse taseme kohta kolmandas riigis või rahvusvahelises organisatsioonis.

---

[8] Schrems I, punkt 88.
[9] ELi toimimise lepingu artikli 288 lõige 2.
[10] Schrems I, punkt 52.
[11] Õiguskaitsedirektiivi põhjendus 67.
[12] Schrems I, punktid 72–74, ja Euroopa Kohtu 26. juuli 2017 aasta arvamus 1/15 Kanada ja Euroopa Liidu vahelise lepingu projekti kohta, ECLI:EU:C:2017:592 (arvamus 1/15), punkt 134: „Õigus isikuandmete kaitsele nõuab eelkõige, et liidu õiguses ette nähtud põhivabaduste ja -õiguste järjepidev kõrgetasemeline kaitse tagataks isikuandmete edastamisel liidust kolmandasse riiki. Kuigi vahendid sellise kaitsetaseme saavutamiseks võivad olla erinevad nendest, mida liidus rakendatakse liidu õigusest tulenevate nõuete järgimise tagamiseks, peavad need vahendid siiski praktikas osutuma tõhusaks, et tagada liidus kehtiva kaitsega sisuliselt samaväärne kaitse“.

16. Euroopa Andmekaitsenõukogu esitab õigeaegselt arvamuse Euroopa Komisjoni järelduste kohta, teeb kindlaks andmekaitse piisavuse tagamise raamistikus esinevad võimalikud puudused ja vajaduse korral annab võimalikke soovitusi.

17. Vastavalt õiguskaitsedirektiivi artikli 36 lõikele 4 on Euroopa Komisjoni ülesanne pidevalt jälgida suundumusi, mis võivad mõjutada kaitse piisavuse otsuse toimimist.

18. Õiguskaitsedirektiivi artikli 36 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. Sõltuvalt 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 tsüklit järk-järgult kohandada.

19. Seoses Euroopa Andmekaitsenõukogu ülesandega esitada Euroopa Komisjonile arvamus, kas kolmandas riigis, kolmanda riigi territooriumil või kolmanda riigi ühes või mitmes kindlaksmääratud sektoris või rahvusvahelises organisatsioonis ei ole enam tagatud isikuandmete kaitse piisav tase, peab andmekaitsenõukogu saama Euroopa Komisjonilt asjaomase kolmanda riigi või rahvusvahelise organisatsiooni vastavate suundumuste jälgimise kohta õigeaegselt sisulist teavet. Seega tuleb andmekaitsenõukogu alati hoida kursis otsuse läbivaatamise protsessiga ja kolmandasse riiki või rahvusvahelisse organisatsiooni tehtavate kontrollkäikudega. Euroopa Andmekaitsenõukogu soovitab, et teda kutsutaks nendes läbivaatamisprotsessides ja missioonides osalema, nagu oli ette nähtud Privacy Shieldi käsitlevas otsuses ning on ette nähtud Jaapanit puudutavates piisavusotsustes.

20. Märkida tuleks ka seda, et kui kolmas riik või rahvusvaheline organisatsioon ei taga enam piisavat kaitsetaset, on Euroopa Komisjonil vastavalt õiguskaitsedirektiivi artikli 36 lõikele 5 volitus kehtiv kaitse piisavuse otsus kehtetuks tunnistada, seda muuta või peatada selle kehtivus. Andmekaitsenõukogu osaleb kehtetuks tunnistamise, muutmise või peatamise menetluses sellega, et vastavalt õiguskaitsedirektiivi artikli 51 lõike 1 punktile g küsitakse tema arvamust.

21. Lisaks, ilma et see mõjutaks süüdistuse ettevalmistamise eest vastutava asutuse volitusi, peaksid järelevalveasutused olema ka volitatud tegema käesoleva direktiivi rikkumised teatavaks õigusasutustele või osalema kohtumenetluses[13]. Eeskätt tuleneb see Euroopa Kohtu otsusest kohtuasjas Schrems I, et andmekaitseasutusel peab olema võimalik osaleda kohtumenetlustes siseriiklikes kohtutes, kui see asutus peab põhjendatuks selle isiku esitatud väiteid piisavusotsuse kohta[14]. Seda hinnangut kinnitati ka otsusega kohtuasjas Schrems II[15].

[13] Vt õiguskaitsedirektiivi artikli 47 lõige 5 ja põhjendus 82.

[14] Vt Schrems I, punkt 65: „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“.

[15] Vt Schrems II, punkt 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“.

4. ELI PIISAVUSSTANDARDID POLITSEI- JA ÕIGUSALASE KOOSTÖÖ PUHUL

22. Sisu poolelt tuleks piisavusotsustes keskenduda asjaomase kolmanda riigi olemasolevate õigusaktide hindamisele tervikuna nii teoorias kui ka praktikas, pidades silmas õiguskaitsedirektiivi artiklis 36 sätestatud hindamiskriteeriume. Kolmanda riigi või rahvusvahelise organisatsiooni süsteem peab sisaldama järgmisi peamisi andmekaitse üld-, menetlus- ja jõustamispõhimõtteid ning -mehhanisme.

23. Õiguskaitsedirektiivi artikli 36 lõikes 2 on kindlaks määratud asjaolud, mida Euroopa Komisjon võtab arvesse, kui ta hindab, kas kaitse tase kolmandas riigis või rahvusvahelises organisatsioonis on piisav.

24. Eelkõige võtab komisjon arvesse õigusriigi põhimõtet ning inimõiguste ja põhivabaduste austamist,[16] asjaomaseid õigusakte ning ka nende õigusaktide rakendamist, tõhusaid ja kohtulikult kaitstavaid andmesubjekti õigusi ning tõhusat haldus- ja õiguskaitset nende andmesubjektide puhul, kelle isikuandmeid edastatakse, ühe või mitme sõltumatu järelevalveasutuse olemasolu ja tulemuslikku toimimist ning kolmanda riigi või rahvusvahelise organisatsiooni võetud rahvusvahelisi kohustusi.

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

26. Peamised andmekaitse üldpõhimõtted ning menetlus- ja jõustamisnõuded, mida võib pidada nõutavaks miinimumiks, et kaitse oleks piisav, on tuletatud ELi põhiõiguste hartast ja õiguskaitsedirektiivist. Üldised sätted isikuandmete kaitse ja eraelu puutumatuse kohta kolmandas riigis ei ole piisavad. Vastupidi, kolmanda riigi või rahvusvahelise organisatsiooni õigusraamistik peab sisaldama erisätteid, milles käsitletakse konkreetselt õigust isikuandmete kaitsele õiguskaitse valdkonnas. Kolmas riik peaks võtma kohustuse tagada piisav kaitse tase, mis sisuliselt vastab liidus tagatava kaitse tasemele. Need sätted peavad olema jõustatavad.

27. Lisaks leidis Euroopa Kohus seoses proportsionaalsuse põhimõttega,[17] et küsimust, kas eraelu puutumatuse ja andmete kaitse õiguse piiramine on õigustatud, tuleb ühelt poolt hinnata sellise

[16] Kolmanda riigi õigusraamistiku hindamisel tuleks võtta arvesse võimalust, et ELilt edastatud andmete põhjal võidakse määrata surmanuhtlus või rakendada mis tahes vormis julma ja ebainimlikku kohtlemist. Kui kolmanda riigi õiguses nähakse tõepoolest ette selline karistus või kohtlemine, tuleks kolmanda riigi õigusraamistikust leida täiendavad kaitsemeetmed, tagamaks, et EList edastatavaid andmeid ei kasutata surmanuhtluse või mis tahes vormis julma ja ebainimliku kohtlemise taotlemiseks ja määramiseks (nt rahvusvaheline leping, millega kehtestatakse edastamistingimused, kolmanda riigi võetud kohustus ELilt edastatud andmete põhjal mitte määrata surmanuhtlust või rakendada mis tahes vormis julma ja ebainimlikku kohtlemist või surmanuhtluse moratoorium).
[17] Harta artikli 52 lõige 1.

piiranguga kaasneva **riive raskust** kaaludes[18] ja teiselt poolt kontrollides, et selle piiranguga taotletava **üldisele huvile vastava eesmärgi olulisus** on selle raskusastmega vastavuses[19].

28. Euroopa Kohtu praktika kohaselt peab põhiõiguste riivet võimaldav õiguslik alus proportsionaalsuse põhimõttele vastamiseks ise määratlema, kui ulatuslikult tohib asjaomase õiguse teostamist piirata[20]. Isikuandmete kaitse erandeid ja piiranguid tuleb kohaldada üksnes rangelt vajalikus ulatuses[21]. Selle nõude täitmiseks tuleb asjaomastes õigusaktides lisaks kõnealuse meetme rakendamise ulatust reguleerivate selgete ja täpsete reeglite sätestamisele kehtestada ka minimaalsed kaitsemeetmed, et inimestel, kelle isikuandmeid edastatakse, oleksid piisavad tagatised nende isikuandmete tõhusaks kaitsmiseks 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“[22].

29. Andmekaitsenõukogu on võtnud vastu soovitused, mis määratlevad Euroopa Kohtu ja Euroopa Inimõiguste Kohtu praktikat kajastavad olulised jälgimise valdkonna tagatised, mis peavad kolmanda riigi õiguses olema, kui hinnatakse selle riigi jälgimismeetmeid andmesubjektide õiguste riive suhtes, kui sellesse riiki edastatakse isikuandmete kaitse üldmääruse alusel andmeid[23]. Selleks et hinnata, kas direktiivi artikli 36 lõike 2 punkti a tingimused on täidetud, tuleb andmekaitsenõukogu arvates võtta arvesse neis soovitustes sätestatud tagatisi, kui hinnatakse kolmanda riigi piisavuse vastavust õiguskaitsedirektiivile jälgimise valdkonnas, pidades ühtlasi silmas jälgimise valdkonna eritingimusi.

30. Seoses artikli 36 lõike 2 punkti b nõudega peaks kolmas riik mitte ainult tagama andmete kaitse tõhusa ja sõltumatu järelevalve, vaid ka nägema ette liikmesriikide andmekaitseasutustega tehtava koostöö mehhanismid[24].

31. Seoses artikli 36 lõike 2 punkti c nõudega peaks komisjon lisaks kolmanda riigi või rahvusvahelise organisatsiooni rahvusvahelistele kohustustele võtma arvesse ka kohustusi, mis tulenevad kolmanda riigi või rahvusvahelise organisatsiooni osalemisest mitmepoolsetes või piirkondlikes süsteemides, eelkõige seoses isikuandmete kaitsega, samuti selliste kohustuste rakendamist; eelkõige tuleks arvesse võtta kolmanda riigi ühinemist Euroopa Nõukogu 28. jaanuari 1981. aasta isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni ja selle lisaprotokolliga (konventsioon 108[25] ja selle ajakohastatud versioon, konventsioon 108+). Arvestada tuleks kolmanda riigi vastavust rahvusvahelistes dokumentides, nagu näiteks Euroopa Nõukogu praktilistes juhistes sätestatud põhimõtetele isikuandmete kasutamise kohta politseisektoris: kuidas kaitsta isikuandmeid kuritegevuse vastu võitlemisel.

---

[18] Näiteks märkis kohus, et „lõppseadme asukoha kindlakstegemist võimaldavate andmete reaalajas kogumisega kaasnev riive näib eriti raske, kuna need andmed annavad pädevatele riigisisestele asutustele võimaluse täpselt ja alaliselt jälgida mobiiltelefonide kasutajate liikumist (...)“ (liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18, La Quadrature du Net jt, 6. oktoober 2020, ECLI:EU:C:2020:791, punkt 187, sh viidatud kohtupraktika).
[19] La Quadrature du Net jt, punkt 131.
[20] Schrems II, punkt 180.
[21] Schrems II, punkt 176, sh viidatud kohtupraktika.
[22] Schrems II, punkt 176, sh viidatud kohtupraktika.
[23] Andmekaitsenõukogu soovitused 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis, vastu võetud 10. novembril 2020.
[24] Õiguskaitsedirektiivi põhjendus 67.
[25] Õiguskaitsedirektiivi põhjendus 68.

32. Piisavusotsus peaks tagama, et privaatsusõiguste sisu ja andmekaitse õiguste, nende tõhusa rakendamise, järelevalve ja jõustamise kaudu tagab kogu kolmanda riigi süsteem nõutava isikuandmete kaitse taseme, sealhulgas andmetele, mis on teel sellesse riiki. Nagu Euroopa Kohus on otsuses Schrems II rõhutanud, tuleks kindlustada isikuandmete kõrgetasemelise kaitse järjepidevus ka andmete edastamise korral kolmandasse riiki[26].

33. Viimaks, kui vastu võetakse kaitse piisavuse otsus üksnes kolmanda riigi territooriumi või kindlaksmääratud sektori kohta, peaks Euroopa Komisjon võtma arvesse selgeid ja objektiivseid kriteeriume, viidates näiteks konkreetsetele isikuandmete töötlemise toimingutele või kohaldatavate õigusnormide kohaldamisalale ning kolmandas riigis kehtivatele õigusaktidele[27].

A. Üldpõhimõtted ja kaitsemeetmed

a) Mõisted

34. Rakendada tuleks peamisi andmekaitsemõisted. Need ei pea täpselt vastama õiguskaitsedirektiivis kasutatud terminoloogiale, kuid peaksid kajastama Euroopa andmekaitseõiguses sätestatud mõisteid ja olema nendega kooskõlas. Õiguskaitsedirektiiv sisaldab näiteks järgmisi olulisi mõisteid: „isikuandmed“, „isikuandmete töötlemine“, „pädev asutus“, „vastutav töötleja“, „volitatud töötleja“, „vastuvõtja“, „delikaatsed andmed“, „õigsus“, „profiilianalüüs“, „lõimitud ja vaikimisi andmekaitse“, „järelevalveasutus“ ja „pseudonümiseerimine“.

b) Isikuandmete töötlemise seaduslikkus ja õiglus (artikkel 4 – põhjendus 26)

35. Harta artikli 8 lõike 2 kohaselt tuleb isikuandmeid töödelda muu hulgas „kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel“[28]. Õiguskaitse kontekstis tuleb aga märkida, et pädevatele asutustele institutsiooniliselt süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise eesmärgil seadusega antud ülesande täitmine annab neile õiguse nõuda või kohustada, et füüsilised isikud vastaksid esitatud taotlustele. Sellisel juhul ei tohiks andmesubjekti nõusolek olla pädevate asutuste jaoks isikuandmete töötlemise õiguslik alus[29].

36. See õiguslik alus peaks sätestama selged ja täpsed reeglid, mis reguleerivad asjaomaste andmetöötlustoimingute ulatust ja kohaldamist ning kehtestavad miinimumnõuded[30]. Lisaks tuletas Euroopa Kohus meelde, et „õigusakt peab olema riigisiseses õiguses õiguslikult siduv“[31].

---

[26] Vt punkt 93.
[27] Õiguskaitsedirektiivi põhjendus 67.
[28] Vt Schrems II, punkt 173.
[29] Õiguskaitsedirektiivi põhjenduses 35 öeldakse ka, et „[k]ui andmesubjektilt nõutakse juriidilise kohustuse täitmist, puudub andmesubjektil tõeline ja vaba valikuvõimalus ning seetõttu ei saa andmesubjekti reaktsiooni käsitada vabatahtliku tahteavaldusena. See ei tohiks takistada liikmesriikidel õigusaktidega ette näha, et andmesubjekt võib nõustuda oma isikuandmete käesoleva direktiivi eesmärkidel toimuva töötlemisega, nagu kriminaaluurimises tehtavad DNA testid või tema asukoha jälgimine elektrooniliste märgiste abil kriminaalkaristuste täitmisele pööramiseks“.
[30] Vt Schrems II, punktid 175 ja 180 ning arvamus 1/15, punkt 139, ja seal viidatud kohtupraktika.
[31] Vt kohtuasi C-623/17, Privacy International *vs*. Secretary of State for Foreign and Commonwealth Affairs jt, 6. oktoober 2020, ECLI:EU:C:2020:790, punkt 68. Samuti peaks olema selge, et kohtuotsuse prantsuskeelses versioonis kasutab Euroopa Kohus sõna „*réglementation*“, mis on laiema tähendusega kui üksnes parlamendi aktid.

37. Selleks et andmetöötlus oleks seaduslik,[32] peaks see olema vajalik süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ülesande täitmiseks, millega tegeleb pädev asutus[33]. Need eesmärgid peaksid olema sätestatud riigi õiguses.

38. Isikuandmeid töödeldakse õiglaselt. Andmekaitses kehtiv õiglase töötlemise põhimõte on määratletud harta artiklis 47 ja Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni („Euroopa inimõiguste konventsioon“) artiklis 6 õiglase kohtumenetluse õigusest eraldiseisva põhimõttena[34].

c) Eesmärgi piiramise põhimõte (artikkel 4)

39. Isikuandmete töötlemise konkreetsed eesmärgid, mis tuleks kindlaks määrata isikuandmete kogumise ajal, peaksid olema selged ja õiguspärased[35].

40. Andmeid tuleks töödelda täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise,[36] sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil kolmandas riigis, ning edaspidi kasutada mis tahes sellisel eesmärgil, kuivõrd see ei ole vastuolus töötlemise esialgse eesmärgiga (nt paralleelseks õiguskaitsemenetluseks või avalikes huvides arhiveerimise eesmärgil või teaduslikuks, statistiliseks või ajalooliseks kasutamiseks), ja kohaldada andmesubjekti õiguste ja vabaduste suhtes asjakohaseid kaitsemeetmeid. Kui isikuandmeid töötleb sama või erinev vastutav töötleja (pädev asutus[37]) süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil, mis on nende kogumise eesmärgist erinev, peaks selline töötlemine olema lubatud tingimusel, et see on asjaomaste õigusnormide kohaselt lubatud ning nimetatud teise eesmärgi saavutamiseks vajalik ja proportsionaalne[38]. Samuti tuleks arvesse võtta mehhanismi olemasolu, mille kaudu teavitatakse asjaomaste liikmesriikide pädevaid asutusi isikuandmete sellisest täiendavast töötlemisest[39]. Lisaks ei tohiks ühelgi juhul kahjustada õiguskaitsedirektiiviga tagatud füüsiliste isikute kaitse taset liidus, sealhulgas juhtudel, kui kolmandast riigist saadud isikuandmed saadetakse edasi vastutavatele töötlejatele või volitatud töötlejatele samas kolmandas riigis[40].

---

[32] Isikuandmete täielikult või osaliselt automatiseeritud töötlemine ja isikuandmete automatiseerimata töötlemine, kui isikuandmed kuuluvad andmete kogumisse või kui need kavatsetakse andmete kogumisse kanda.
[33] Pädevad asutused on mis tahes avaliku sektori asutused, mis on selleks eesmärgiks pädevad, või mis tahes muu organ või üksus, millele on seadusega tehtud ülesandeks teostada avalikku võimu ning antud selleks volitused.
[34] Õiguskaitsedirektiivi põhjendus 26.
[35] Õiguskaitsedirektiivi põhjendus 26.
[36] See sisaldab „politsei toiminguid juhul, kui eelnevalt pole teada, kas tegemist on süüteoga. Selline tegevus võib hõlmata ka avaliku võimu teostamist sunnimeetmete võtmisega, näiteks politsei tegevus demonstratsioonidel, suurtel spordiüritustel ja massirahutustel. Selline tegevus hõlmab ka avaliku korra säilitamist, mis on politseile või muule õiguskaitseasutusele antud ülesanne, et vajaduse korral kaitsta avalikku julgeolekut ja seadusega kaitstavaid ühiskonna põhihuve selliste ohtude eest ja hoida ära selliste ohtude teke avalikule julgeolekule ja seadusega kaitstavatele ühiskonna põhihuvidele, mis võivad viia süüteo toimepanemiseni“ (õiguskaitsedirektiivi põhjendus 12). Seda tuleb eristada riigi julgeoleku eesmärgist või tegevustest, mis kuuluvad Euroopa Liidu lepingu V jaotise 2. peatüki kohaldamisalasse (õiguskaitsedirektiivi põhjendus 14).
[37] Vt allmärkus 33.
[38] Õiguskaitsedirektiivi põhjendus 29.
[39] Selline mehhanism võib näiteks olla vastastikku kokkulepitud menetluskoodid, rahvusvahelise lepingu kohane teatamiskohustus, sealhulgas võimalikud automaatteated või muud sarnased läbipaistvusmeetmed.
[40] Õiguskaitsedirektiivi põhjendus 64.

d) Eritingimused edasiseks töötlemiseks muudel eesmärkidel (artikkel 9)

41. Seoses EList edastatud andmete täiendava töötlemise või avalikustamisega muudel eesmärkidel kui õiguskaitse, näiteks riigi julgeoleku eesmärkidel, peaks see samuti olema õigusega sätestatud, vajalik ja proportsionaalne. Samuti tuleks arvesse võtta selliste mehhanismide olemasolu, millega liikmesriikide pädevaid asutusi teavitatakse isikuandmete sellisest edasisest töötlemisest[41]. Ka peaks olema edasiselt töödeldud või avalikustatud andmete kaitsetase sama nagu siis, kui vastuvõttev pädev asutus neid esialgu töötles.

e) Võimalikult väheste andmete kogumine

42. Andmed peaksid olema piisavad ja asjakohased ning nad ei tohi olla töötlemise eesmärke silmas pidades ülemäärased. Eelkõige tuleks arvesse võtta lõimitud ja vaikimisi andmekaitse kohaldamise nõudeid, nagu piiratud sisestusväljad (struktureeritud side) või automatiseeritud või automatiseerimata kvaliteedikontrollid.

f) Andmete õigsuse põhimõte

43. Andmed peaksid olema õiged ja vajaduse korral ajakohastatud. Võttes arvesse töötlemise laadi ja eesmärki, tuleks sellegipoolest kohaldada andmete õigsuse põhimõtet. Eelkõige kohtumenetluses antakse isikuandmeid sisaldavaid ütlusi, mis põhinevad füüsiliste isikute subjektiivsel ettekujutusel toimunust ning mida ei saa alati kontrollida. Seetõttu ei tohiks õigsuse nõue puudutada tunnistuse õigsust, vaid üksnes tõsiasja, et konkreetne tunnistus on antud[42].

44. Tuleks tagada, et isikuandmeid, mis on ebaõiged, mittetäielikud või mis ei ole enam ajakohased, ei edastata ega tehta kättesaadavaks,[43] ning et ebaõigete andmete parandamiseks või kustutamiseks on ette nähtud menetlused. Eeskätt tuleks töödeldud andmete mis tahes liigitussüsteemi puhul arvesse võtta allika usaldusväärsust ja faktide kontrollimise taset[44].

g) Andmete säilitamise põhimõte

45. Isikuandmeid ei tohiks säilitada kauem, kui see on vajalik nende töötlemise eesmärgi täitmiseks. Isikuandmete kustutamiseks tuleks kehtestada asjakohased mehhanismid; see võib olla kindlaksmääratud ajavahemik või isikuandmete säilitamise vajaduse korrapärane läbivaatamine (või mõlema kombinatsioon: kindlaksmääratud maksimaalne ajavahemik ja korrapärane läbivaatamine teatud aja järel)[45]. Isikuandmetele, mida säilitatakse pikema aja jooksul avalikes huvides arhiveerimise eesmärgil või teaduslikuks, statistiliseks või ajalooliseks kasutamiseks, tuleks kehtestada asjakohased kaitsemeetmed (nt seoses juurdepääsuga)[46].

h) Turvalisuse ja konfidentsiaalsuse põhimõte (artikkel 29, põhjendused 28 ja 71)

46. Iga isikuandmeid töötlev üksus peaks kindlustama, et andmeid töödeldakse viisil, millega on tagatud andmete turvalisus, sealhulgas tuleb vältida isikuandmetele ning nende töötlemiseks

[41] Vt allmärkus 39.
[42] Õiguskaitsedirektiivi põhjendus 30.
[43] Õiguskaitsedirektiivi põhjendus 32.
[44] Nt 4x4 võrgustik usaldusväärsuse hindamiseks ja töötlemiskoodid.
[45] Õiguskaitsedirektiivi artikkel 5.
[46] Õiguskaitsedirektiivi põhjendus 26.

kasutatavatele seadmetele loata juurdepääsu või nende loata kasutamist. See sisaldab kaitset loata või ebaseadusliku töötlemise eest ning juhusliku kadumise, hävimise või kahjustumise eest; selleks kasutatakse asjakohaseid tehnilisi või korralduslikke meetmeid. Turvalisuse taseme väljaselgitamisel tuleks võtta arvesse teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke, samuti erineva tõenäosuse ja suurusega ohtusid füüsiliste isikute õigustele ja vabadustele.

47. Tagada tuleks turvalised sidekanalid andmeid edastavate liikmesriikide asutuste ja kolmandate riikide vastuvõtvate asutuste vahel.

i) Läbipaistvuse põhimõte (artikkel 13, põhjendused 26, 39, 42, 43, 44, 46)

48. Füüsilisi isikuid tuleks teavitada nende isikuandmete töötlemisega seotud ohtudest, normidest, kaitsemeetmetest ja õigustest ning sellest, kuidas nad saavad isikuandmete töötlemisega seoses oma õigusi kasutada[47].

49. Inimestele tuleks kättesaadavaks teha teave nende isikuandmete töötlemise kõigi põhielementide kohta. See teave peaks olema kergesti juurdepääsetav ja kergesti mõistetav, selges ja lihtsas sõnastuses. Selline teave peaks hõlmama töötlemise eesmärki, vastutava töötleja nime, asjaomase isiku õigusi[48] ja muud õigluse tagamiseks vajalikku teavet.

50. Selle teabe saamise õiguse puhul võib esineda mõningaid erandeid. Selline piiramine aga peaks olema lubatud seadusandliku meetmega ning olema vajalik ja proportsionaalne ametlike või õiguslike päringute, uurimiste või menetluste takistamise vältimiseks, süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise kahjustamise vältimiseks ning avaliku julgeoleku või riigi julgeoleku kaitsmiseks või teiste isikute õiguste ja vabaduste kaitsmiseks, kuni selline osaline või täielik piiramine on asjaomase füüsilise isiku põhiõigusi ja õigustatud huve nõuetekohaselt arvestades demokraatlikus ühiskonnas vajalik ja proportsionaalne meede. Samuti tuleks selliseid piiranguid kaaluda ja hinnata, võttes arvesse võimalust esitada kaebus järelevalveasutusele või kasutada õiguskaitsevahendit. Igal juhul peaks mis tahes võimalik piirang olema ajutine ja mitte lauspiirang ning kuuluma samalaadsete tingimuste, kaitsemeetmete ja piirangute raamistikku, mida nõutakse hartaga ja Euroopa inimõiguste konventsiooniga, nagu neid tõlgendavad Euroopa Kohus ja Euroopa Inimõiguste Kohus oma praktikas, ning eelkõige tuleb seejuures austada nende õiguste ja vabaduste põhiolemust.

j) Õigus pääseda juurde, parandada ja kustutada (artiklid 14 ja 16)

51. Andmesubjektil peaks olema õigus saada kinnitus selle kohta, kas teda käsitlevaid isikuandmeid töödeldakse või mitte, ning nende töötlemise korral tutvuda enda isikuandmetega. See õigus peaks sisaldama vähemalt kindlat teavet töötlemise kohta, näiteks töötlemise eesmärk ja õiguslik alus, õigus esitada järelevalveasutusele kaebus või asjaomaste isikuandmete liigid[49]. Eriti oluline on see juhul, kui läbipaistvus saavutatakse üldise teatega (nt teave ametiasutuse kodulehel).

52. Andmesubjektil peaks olema õigus taotleda kindlatel põhjustel oma isikuandmete parandamist, näiteks kui need osutuvad ebaõigeks või ebatäielikuks. Samuti peaks andmesubjektil olema õigus nõuda oma isikuandmete kustutamist, näiteks kui nende töötlemine ei ole enam vajalik või on ebaseaduslik.

[47] Õiguskaitsedirektiivi põhjendus 26.
[48] Nii sisulised õigused (õigus pääseda juurde, parandada jne) kui ka õigus õiguskaitsele.
[49] Õiguskaitsedirektiivi artikkel 14.

53. Nende õiguste kasutamine ei tohiks olla andmesubjektile liiga koormav.

k) Andmesubjekti õiguste piirangud

54. Nende õiguste võimalik piiramine võib esineda ametlike või õiguslike päringute, uurimiste või menetluste takistamise vältimiseks, süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise kahjustamise vältimiseks ning avaliku julgeoleku või riigi julgeoleku kaitsmiseks või teiste isikute õiguste ja vabaduste kaitsmiseks, kuni selline täielik või osaline piiramine on asjaomase füüsilise isiku põhiõigusi ja õigustatud huve nõuetekohaselt arvestades demokraatlikus ühiskonnas vajalik ja proportsionaalne meede. Samuti tuleks selliseid piiranguid kaaluda ja hinnata, võttes arvesse võimalust esitada kaebus järelevalveasutusele või kasutada õiguskaitsevahendit.

l) Edasisaatmise piirangud (artikkel 35, põhjendused 64–65)

55. Kui algne vastuvõtja saadab isikuandmeid edasi muusse kolmandasse riiki või muule rahvusvahelisele organisatsioonile, ei tohi see kahjustada kaitsetaset, mis on tagatud liidus neile füüsilistele isikutele, kelle isikuandmeid edastatakse. Seetõttu peaks andmete selline edasisaatmine olema lubatud üksnes juhul, kui on kindlustatud liidu õigusega tagatud kaitsetaseme järjepidevus[50]. Eelkõige peaks edasine vastuvõtja (st edasisaatmise vastuvõtja) olema pädev asutus õiguskaitse eesmärgil[51] ning sellised andmete edasisaatmised võivad toimuda üksnes piiratud ja kindlaksmääratud eesmärkidel ning kui selliseks töötlemiseks on õiguslik alus.

56. Samuti tuleb arvesse võtta mehhanismi olemasolu, mille kaudu asjaomase liikmesriigi pädevaid asutusi isikuandmete sellisest edasisaatmisest teavitada ja anda selleks luba. EList edastatud andmete algne vastuvõtja peaks olema vastutav ja suuteline tõendama, et liikmesriigi asjaomane pädev asutus on edasisaatmist lubanud[52] ning kui selle kolmanda riigi kohta, kuhu andmed edasi saadetakse, ei ole kaitse piisavuse otsust vastu võetud, on andmete edasisaatmise kohta kehtestatud asjakohased kaitsemeetmed[53].

m) Vastutamise põhimõte (artikli 4 lõige 4)

57. Vastutav töötleja peaks vastutama õiguskaitsedirektiivi artiklis 4 esitatud andmekaitsepõhimõtete täitmise eest ja olema võimeline nende täitmist tõendama.

[50] Vt ka arvamus 1/15.
[51] Vt allmärkus 33.
[52] Sellega seoses tuleks võtta arvesse, kas on kehtestatud kohustus rakendada edastavate liikmesriikide ametiasutuste määratud asjaomaseid töötlemiskoode.
[53] Eespool esitatud nõuded ei piira eritingimusi, mis on sätestatud õiguskaitsedirektiivis edasisaatmisele piisava kaitsetasemega riiki (artikli 35 lõike 1 punktid c ja e).

B. Näited täiendavatest põhimõtetest, mida tuleb kohaldada eri töötlemisliikide puhul

a) Andmete eriliigid (artikkel 10 ja põhjendus 37)

58. Isikuandmete eriliikide[54] töötlemisel tuleks kohaldada konkreetseid kaitsemeetmeid, mis on suunatud teatud kaasnevatele riskidele[55]. Need liigid peaksid kajastama õiguskaitsedirektiivi artiklis 10 sätestatut. Isikuandmete eriliikide töötlemise suhtes tuleks seega kohaldada konkreetseid kaitsemeetmeid ning see peaks olema lubatud üksnes juhul, kui see on teatud tingimustel rangelt vajalik, näiteks isiku eluliste huvide kaitsmiseks.

b) Automatiseeritud töötlusel põhinevate otsuste tegemine ja profiilianalüüs (artikkel 11 ja põhjendus 38)

59. Otsuseid, mis põhinevad üksnes automaatsel isikuandmete töötlemisel (automatiseeritud töötlusel põhinevate üksikotsuste tegemine), sealhulgas profiilianalüüsil, ja millel on andmesubjekti puudutavad negatiivsed õiguslikud tagajärjed või mis teda märkimisväärselt mõjutavad, peaks tegema üksnes teatavatel kolmanda riigi õigusraamistikus kehtestatud tingimustel[56].

60. Euroopa Liidu raamistikus sisaldavad näiteks need tingimused andmesubjektile konkreetse teabe andmist ja õigust otsesele isiklikule kontaktile vastutava töötlejaga, eelkõige õigust väljendada oma seisukohta, õigust saada selgitust otsuse kohta, mis tehti pärast sellist hindamist, ja õigust otsust vaidlustada.

61. Kolmanda riigi õiguses peaksid andmesubjekti õiguste ja vabaduste kohta olema igal juhul sätestatud vajalikud kaitsemeetmed. Sellega seoses tuleks arvesse võtta ka sellise mehhanismi olemasolu, mille kaudu teavitatakse asjaomase liikmesriigi pädevaid asutusi täiendavast töötlemisest, näiteks edastatud isikuandmete kasutamisest ulatuslikuks profiilianalüüsiks.

c) Lõimitud andmekaitse ja vaikimisi andmekaitse (artikkel 20)

62. Piisavuse hindamisel tuleks tähelepanu pöörata sellele, kas vastutaval töötlejal on kohustus võtta vastu sise-eeskirjad ja võtta meetmeid, mis järgivad eelkõige lõimitud andmekaitse ja vaikimisi andmekaitse põhimõtteid, rakendades teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke, samuti isikuandmete töötlemisest tulenevaid füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohtusid arvesse võttes nii isikuandmete töötlemisvahendite kindlaksmääramisel kui ka isikuandmete töötlemise ajal asjakohaseid tehnilisi ja korralduslikke meetmeid, nagu pseudonümiseerimine, mis on vajalikud andmekaitsepõhimõtete (nagu võimalikult väheste andmete kogumine) tõhusaks rakendamiseks ja vajalike kaitsemeetmete lõimimiseks isikuandmete töötlemisse.

[54] Tuntud ka kui „delikaatsed andmed“, millele on osutatud õiguskaitsedirektiivi põhjenduses 37.
[55] Sellised täiendavad kaitsemeetmed võivad olla nt konkreetsed turvameetmed, töötajate piiratud juurdepääsuõigus, täiendava töötlemise, automatiseeritud otsuste tegemise, edasijagamise või edasisaatmise piirangud.
[56] Arvamus 1/15, punkt 173.

C. Menetlus- ja jõustamismehhanismid

63. Kuigi vahendid, mida kolmas riik piisava kaitsetaseme saavutamiseks kasutab, võivad olla erinevad nendest, mida liidus rakendatakse,[57] peavad Euroopa süsteemiga kooskõlas oleval süsteemil olema järgmised elemendid:

a) Pädev sõltumatu järelevalveasutus (artikli 36 lõike 2 punkt b ja artikli 36 lõige 3 ning põhjendus 67)

64. Kolmandas riigis peaks olema olemas üks või mitu sõltumatut järelevalveasutust, kelle ülesanne on tagada andmekaitse ja eraelu puutumatuse sätete järgimine ning nendest kinnipidamine. Järelevalveasutus peab tegutsema oma ülesannete täitmisel ja volituste kasutamisel täiesti sõltumatult ja erapooletult ega tohi kelleltki küsida ega võtta vastu juhiseid. Sellega seoses peaksid järelevalveasutusel olema piisavad jõustamisvolitused, et tulemuslikult tagada andmekaitseõiguste järgimine ja suurendada teadlikkust. Tähelepanu tuleks pöörata ka järelevalveasutuse töötajatele ja eelarvele. Samuti peab järelevalveasutus olema võimeline korraldama omal algatusel uurimisi. Järelevalveasutuse ülesandeks peaks olema aidata ja nõustada andmesubjekte nende õiguste teostamisel (vt ka punkt c allpool). Asjakohasel juhul tuleks piisavusotsustes määratleda andmekaitsenormide jõustamisega tegelev(ad) järelevalveasutus(ed) ning koostöömehhanismid liikmesriikide järelevalveasutustega.

b) Andmekaitsenormide tõhus rakendamine

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

66. Kolmanda riigi andmekaitseraamistik peaks kohustama vastutavaid töötlejaid või nende nimel isikuandmeid töötlevaid isikuid andmekaitseraamistikust kinni pidama ja tagama, et nad on võimelised normide järgimist eelkõige pädevale järelevalveasutusele tõendama. Nende meetmete hulgas peaks olema isikuandmete töötlemise toimingute registri või logifailide pidamine asjakohase ajavahemiku jooksul. Need võivad sisaldada näiteks ka andmekaitsealaseid mõjuhinnanguid, andmekaitseametniku määramist või lõimitud ja vaikimisi andmekaitset.

c) Andmekaitsesüsteem peab hõlbustama andmesubjekti õiguste teostamist (õiguskaitsedirektiivi artiklid 12, 17 ning 46)

67. Kolmanda riigi andmekaitseraamistik peaks kohustama vastutavaid töötlejaid hõlbustama andmesubjektide õiguste teostamist, millele osutati eespool A jao punktis j, ning sätestama, et vastava taotluse korral annab järelevalveasutus mis tahes andmesubjektile teavet tema õiguste teostamise kohta[58].

d) Andmekaitsesüsteemiga tuleb tagada asjakohane õiguskaitsemehhanism

68. Kuigi praegu puudub kohtupraktika kolmanda riigi õigussüsteemi õiguskaitsedirektiivile vastava piisavuse kohta, on Euroopa Kohus tõlgendanud harta artiklis 47 sätestatud põhiõigust tõhusale

[57] Schrems I, punkt 74.
[58] Andmesubjektide õiguste teostamine võib olla nii otsene kui ka kaudne.

õiguskaitsevahendile kohtus. Harta artikli 47 esimeses lõigus sätestatakse, et igaühel, kelle liidu õigusega tagatud õigusi või vabadusi rikutakse, on selles artiklis kehtestatud tingimuste kohaselt õigus tõhusale õiguskaitsevahendile kohtus[59].

69. Euroopa Kohtu 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 põhisisu[60].

70. Üksikisikul peaks olema võimalik kasutada õiguskaitsevahendeid, et teostada oma õigusi kiiresti ja tulemuslikult, ilma tõkestavate kuludeta, ja tagada normide täitmine.

71. 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.

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

[59] Euroopa Kohtu arvamuse kohaselt saab tõhusat õiguskaitset lisaks kohtule tagada ka organ, kes pakub harta artiklis 47 ette nähtuga sisuliselt samaväärseid kaitsemeetmeid (vt Schrems II, punkt 197). See võib olla asjakohane eelkõige rahvusvaheliste organisatsioonide puhul.
[60] Schrems II, punktid 187 ja 194, sh viidatud kohtupraktika.