

Suunised



Suunised 2/2020 määruse 2016/679 artikli 46 lõike 2 punkti a ja artikli 46 lõike 3 punkti b kohta seoses isikuandmete edastamisega EMP riikide ja EMP-väliste riikide avaliku sektori asutuste ja organite vahel

Version 2.0

Vastu võetud 15. detsembril 2020

Versioonid

Versioon 2.0	15. detsember 2020	Suuniste vastuvõtmine pärast avalikku konsultatsiooni
Versioon 1.0	18. veebruar 2020	Suuniste vastuvõtmine avalikuks konsultatsiooniks

Sisukord

1	Üldist.....	5
1.1	Eesmärk.....	5
1.2	Andmete rahvusvahelise edastamise suhtes kohaldatavad üldeeskirjad	6
1.3	Avaliku sektori asutuse või organi määratlus	6
2	Üldised soovitusel asjakohaste kaitsemeetmete kohta nii isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkti a kui ka artikli 46 lõike 3 punkti b tähenduses.....	7
2.1	Eesmärk ja kohaldamisala.....	8
2.2	Määratlused	8
2.3	Andmekaitsepõhimõtted	8
2.3.1	Eesmärgikohasuse põhimõte	8
2.3.2	Andmete õigsuse ja võimalikult väheste andmete kogumise põhimõtted.....	9
2.3.3	Säilitamise piiramise põhimõte	9
2.3.4	Andmete turvalisus ja konfidentsiaalsus.....	9
2.4	Andmesubjektide õigused	10
2.4.1	Õigus läbipaistvusele	10
2.4.2	Õigus andmetega tutvuda, neid parandada, kustutada, nende töötlemist piirata ja esitada vastuväiteid	11
2.4.3	Automatiseeritud töötlusel põhinevate üksikotsuste tegemine.....	12
2.4.4	Õigus õiguskaitsele	12
2.4.5	Andmesubjektide õiguste piiramine	12
2.5	Andmete edasisaatmise ja jagamise (sh avalikustamise ja ametiasutuste juurdepääsu) piirangud	12
2.6	Tundlikud isikuandmed.....	14
2.7	Õiguskaitsemehhanismid.....	14
2.8	Järelevalvemehhanismid.....	16
2.9	Lõpetamisklausel	17
3	Konkreetne teave isikuandmete kaitse üldmääruse artikli 46 kohta	18
3.1	Konkreetne teave õiguslikult siduvate ja täitmisele pööratavate dokumentide kohta – isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkt a	18
3.2	Konkreetne teave halduskokkulepete kohta – isikuandmete kaitse üldmääruse artikli 46 lõike 3 punkt b	18
4	Menetluslikud küsimused.....	20

Euroopa Andmekaitsekohtu,

võttes arvesse 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) (edaspidi „isikuandmete kaitse üldmäärus“) artikli 70 lõike 1 punkti e,

võttes arvesse Euroopa Majanduspiirkonna (EMP) lepingut, eriti selle XI lisa ja protokoll nr 37, mida on muudetud EMP ühiskomitee 6. juuli 2018. aasta otsusega nr 154/2018¹,

võttes arvesse oma töökorra artikleid 12 ja 22,

ON VASTU VÕTNUD JÄRGMISED SUUNISED:

¹ Kõiki suunistes sisalduvaid viiteid liikmesriikidele tuleb mõista viidetena EMP liikmesriikidele.

1 ÜLDIST

1.1 Eesmärk

1. Käesoleva dokumendi eesmärk on anda juhiseid isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkti a ja artikli 46 lõike 3 punkti b kohaldamiseks seoses isikuandmete edastamisega EMP riikide avaliku sektori asutustelt või organitelt (edaspidi „avalik-õiguslikud asutused“) kolmandate riikide avalik-õiguslikele asutustele või rahvusvahelistele organisatsioonidele ulatuses, milles need ei ole hõlmatud Euroopa Komisjoni otsusega andmekaitse piisavuse kohta². Avalik-õiguslikud asutused võivad otsustada kasutada neid mehhanisme, mida isikuandmete kaitse üldmääruses peetakse nende olukorras kohasemaks, kuid nad võivad kasutada ka muid sobivaid vahendeid, millega nähakse ette asjakohased kaitsemeetmed kooskõlas isikuandmete kaitse üldmääruse artikliga 46.
2. Suuniste eesmärk on anda ülevaade Euroopa Andmekaitsekoostöögruppi ootustest kaitsemeetmete suhtes, mis tuleb kehtestada avalik-õiguslike asutuste vahelise õiguslikult siduva ja täitmisele pööratava dokumendiga vastavalt isikuandmete kaitse üldmääruse artikli 46 lõike 2 punktile a või pädeva järelevalveasutuse loal avalik-õiguslike asutuste vahelistesse halduskokkulepetesse lisatavate sätetega vastavalt isikuandmete kaitse üldmääruse artikli 46 lõike 3 punktile b³. Euroopa Andmekaitsekoostöögrupp soovib tungivalt, et osalised lähtuksid juba selliste dokumentide või kokkulepete sõlmimise või muutmise kavandamise varases etapis käesolevatest suunistest⁴.
3. Neid suuniseid tuleb lugeda koostoimes Euroopa Andmekaitsekoostöögruppi varasemate dokumentidega (sh tema eelkäija, artikli 29 alusel asutatud andmekaitse töörühma⁵ („artikli 29 töörühm“) heakskiidetud dokumendid), mis käsitlevad territoriaalse kohaldamisalaga ja isikuandmete kolmandatele riikidele edastamisega seotud keskseid küsimusi⁶. Suunised vaadatakse läbi ja vajaduse korral ajakohastatakse, tuginedes isikuandmete kaitse üldmääruse kohaldamisel saadud praktilistele kogemustele.
4. Käesolevates suunistes käsitletakse isikuandmete kaitse üldmääruse kohaldamisalasse kuuluvat rahvusvahelist andmete edastamist avalik-õiguslike asutuste vahel mitmesugustel halduskoostöö eesmärkidel. Sellest tulenevalt ja kooskõlas isikuandmete kaitse üldmääruse artikli 2 lõikega 2 ei hõlma suunised andmete edastamist avaliku julgeoleku, riigikaitse või riigi julgeoleku valdkonnas. Lisaks ei käsitleta suunistes andmete töötlemist ja edastamist pädevate asutuste poolt kriminaalõiguse täitmise tagamise eesmärgil, kuna seda reguleeritakse eraldi õigusaktiga, st õiguskaitse direktiiviga⁷. Suunistes keskendutakse üksnes andmete edastamisele avalik-õiguslike asutuste vahel ning need ei hõlma

² Näiteks Jaapani avalik-õiguslikud asutused, mida Jaapanit käsitlev kaitse piisavuse otsus ei hõlma, sest see hõlmab üksnes erasektori organisatsioone.

³ Isikuandmete kaitse üldmääruse artikli 46 lõike 2 punktis a osutatud õiguslikult siduvatele ja täitmisele pööratavatele dokumentidele ning sama määruse artikli 46 lõike 3 punktis b osutatud halduskokkulepetele viitamisel kasutatakse käesolevates suunistes mõistet „rahvusvahelised lepingud“.

⁴ Isikuandmete kaitse üldmääruse artiklis 96 on sätestatud, et enne 24. mail 2016 sõlmitud lepingud jäävad jõusse kuni nende muutmise, asendamise või tühistamiseni.

⁵ Andmekaitse direktiivi 95/46/EÜ artikli 29 alusel loodud ELi andmekaitseasutuste töörühm.

⁶ Vt artikli 29 töörühm, „Adequacy Referential“ (WP254 rev.01, mille Euroopa Andmekaitsekoostöögrupp kiitis heaks 25. mail 2018), Euroopa Andmekaitsekoostöögruppi suunised 2/2018 määruse 2016/679 artiklis 49 sätestatud erandite kohta ja Euroopa Andmekaitsekoostöögruppi suunised 3/2018 isikuandmete kaitse üldmääruse territoriaalse kohaldamisala kohta (artikkel 3).

⁷ 27. aprilli 2016. aasta direktiiv (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.

isikuandmete edastamist avalik-õiguslikult asutuselt eraõiguslikule üksusele või eraõiguslikult üksuselt avalik-õiguslikule asutusele.

1.2 Andmete rahvusvahelise edastamise suhtes kohaldatavad üldeeskirjad

5. Isikuandmete kaitse üldmääruse artikli 44 kohaselt peab isikuandmeid kolmandatele riikidele või rahvusvahelistele organisatsioonidele edastav andmeekspordija järgima isikuandmete kaitse üldmääruse V peatüki sätteid ja täitma lisaks ka kõnealuse määruse muude sätete tingimused. Eelkõige peab iga töötlemistoiming vastama isikuandmete kaitse üldmääruse artiklis 5 sätestatud andmekaitsepõhimõtetele, olema vastavalt selle määruse artiklile 6 seaduslik ja vastama andmete eriliikide puhul kõnealuse määruse artiklile 9. Seega on vajalik kaheastmeline kontroll: esiteks peab õiguslik alus olema andmete töötlemise suhtes kohaldatav koos isikuandmete kaitse üldmääruse kõigi asjakohaste sätetega; teiseks tuleb järgida isikuandmete kaitse üldmääruse V peatüki sätteid.
6. Isikuandmete kaitse üldmääruse artiklis 46 on sätestatud, et „[a]rtikli 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“. Sellised asjakohased kaitsemeetmed võib ette näha avalik-õiguslike asutuste vahelise õiguslikult siduva ja täitmisele pööratava dokumendiga (isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkt a) või pädeva järelevalveasutuse loal sätetega, mis lisatakse avalik-õiguslike asutuste vahelistesse halduskokkulepetesse ning mis hõlmavad andmesubjektide kohtulikult kaitstavaid ja tõhusaid õigusi (isikuandmete kaitse üldmääruse artikli 46 lõike 3 punkt b). Euroopa Liidu Kohus on selgitanud, et need asjakohased kaitsemeetmed peavad tagama selle, et andmesubjektidele, kelle isikuandmeid edastatakse, oleks tagatud selline õiguste kaitse tase, mis on sisuliselt samaväärne EMPs tagatuga⁸.
7. Lisaks sellele lahendusele ja juhtudeks, kui selline lahendus puudub, on isikuandmete kaitse üldmääruse artiklis 49 esitatud mõningad olukorrad, kus andmete rahvusvaheline edastamine on lubatud, kuigi Euroopa Komisjon ei ole teinud otsust andmekaitse piisavuse kohta⁹. Üks erand hõlmab andmete edastamist, mis on vajalik liidu õiguses või vastutava töötleja suhtes kohaldatavas liikmesriigi õiguses tunnustatud avalikust huvist tulenevatel kaalukatel põhjustel, sealhulgas rahvusvahelise koostöö vastastikkuse põhimõtte vaimus¹⁰. Nagu on aga Euroopa Andmekaitseõukogu varasemates suunistes selgitatud, tuleb isikuandmete kaitse üldmääruse artiklis 49 sätestatud erandeid tõlgendada kitsendavalt ja need on peamiselt seotud töötlemistoimingutega, mis on juhtumipõhised ja mittekorduvad¹¹.

1.3 Avaliku sektori asutuse või organi määratlus

8. Isikuandmete kaitse üldmääruses puudub mõiste „avaliku sektori asutus või organ“ määratlus. Euroopa Andmekaitseõukogu peab seda mõistet piisavalt laiaks, et hõlmata nii kolmandate riikide avalik-õiguslikke asutusi kui ka rahvusvahelisi organisatsioone¹². Kolmandate riikide avalik-õiguslike

⁸ Kohtuotsus, Euroopa Liidu Kohus, Data Protection Commissioner vs. Facebook Ireland ja Maximilian Schrems („Schrems II“), C-311/18, punkt 96.

⁹ Lisateave artikli 49 ja selle üldise koosmõju kohta artikliga 46 on kättesaadav Euroopa Andmekaitseõukogu suunistest 2/2018 määruse 2016/679 artiklis 49 sätestatud erandite kohta.

¹⁰ Vt Euroopa Andmekaitseõukogu suunistest 2/2018 määruse 2016/679 artiklis 49 sätestatud erandite kohta, lk 10.

¹¹ Vt Euroopa Andmekaitseõukogu suunistest määruse 2016/679 artiklis 49 sätestatud erandite kohta, lk 5.

¹² Vt ka isikuandmete kaitse üldmääruse põhjendus 108.

asutuste puhul tuleb see mõiste kindlaks määrata siseriikliku õiguse alusel. Seega hõlmavad avalik-õiguslikud asutused eri tasandi valitsusasutusi (nt riiklikud, piirkondlikud ja kohalikud asutused), kuid võivad hõlmata ka muid avalik-õiguslikke asutusi (nt rakendusametid, ülikoolid, haiglad jne)¹³. Isikuandmete kaitse üldmääruse artikli 4 punkti 26 kohaselt tähendab „rahvusvaheline organisatsioon“ organisatsiooni ja sellele alluvaid asutusi, mida reguleerib rahvusvaheline avalik õigus, või mis tahes muud asutust, mis on loodud kahe riigi vahelise lepinguga või selle alusel.

9. Euroopa Andmekaitsekoostöögrupi tuleb meelde, et isikuandmete kaitse üldmääruse kohaldamine ei piira rahvusvahelise avaliku õiguse sätete, näiteks rahvusvaheliste organisatsioonide privileege ja immunitete reguleerivate sätete kohaldamist. Samal ajal on oluline meenutada, et iga EMPs tegutsev avalik-õiguslik asutus, kes edastab andmeid rahvusvahelistele organisatsioonidele, peab järgima isikuandmete kaitse üldmääruse norme andmete edastamise kohta kolmandatele riikidele või rahvusvahelistele organisatsioonidele¹⁴.

2 ÜLDISED SOOVITUSED ASJAKOHASTE KAITSEMEETMETE KOHTA NII ISIKUANDMETE KAITSE ÜLDMÄÄRUSE ARTIKLI 46 LÕIKE 2 PUNKTI a KUI KA ARTIKLI 46 LÕIKE 3 PUNKTI b TÄHENDUSES

10. Erinevalt direktiivi 95/46/EÜ artikli 26 lõikest 2 on isikuandmete kaitse üldmääruse artiklis 46 sätestatud täiendavad asjakohased kaitsemeetmed andmete edastamiseks avalik-õiguslike asutuste vahel:
 - (i) õiguslikult siduv ja täitmisele pööratav dokument (isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkt a) või
 - (ii) halduskokkulepetesse lisatavad sätted (isikuandmete kaitse üldmääruse artikli 46 lõike 3 punkt b).

Need dokumendid ja kokkulepped võivad olla kahe- või mitmepoolsed.

11. Järgmises jaotises esitatakse mõned üldised soovitused eesmärgiga aidata tagada, et avalik-õiguslike asutuste vahelised õiguslikult siduvad dokumendid või halduskokkulepped (edaspidi „rahvusvahelised lepingud“) on isikuandmete kaitse üldmäärusega kooskõlas.
12. Isikuandmete kaitse üldmääruse artiklis 46 ja põhjenduses 108 ei ole sätestatud konkreetseid kaitsemeetmeid, mis tuleb sellistesse rahvusvahelistesse lepingutesse lisada, kuid Euroopa Andmekaitsekoostöögrupp on koostanud isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkti a ja artikli 46 lõike 3 punkti b kohastes avalik-õiguslike asutuste vahelistesse rahvusvahelistesse lepingutesse lisatavate minimaalsete kaitsemeetmete loetelu, võttes arvesse isikuandmete kaitse üldmääruse artiklit 44¹⁵ ja Euroopa Liidu Kohtu hiljutist kohtupraktikat¹⁶. Nende kaitsemeetmete

¹³ Vt nt mõistete „avaliku sektori asutus“ ja „avalik-õiguslik isik“ määratlust Euroopa Parlamendi ja nõukogu 17. novembri 2003. aasta direktiivi 2003/98/EÜ (avaliku sektori valduses oleva teabe taaskasutamise kohta) artikli 2 punktides 1 ja 2 (ELT L 345, 31.12.2003, lk 90).

¹⁴ Vt Euroopa Andmekaitsekoostöögrupi suunised 3/2018 isikuandmete kaitse üldmääruse territoriaalse kohaldamisala kohta, lk 23.

¹⁵ Isikuandmete kaitse üldmääruse artiklis 44 on sätestatud: „Kõiki käesoleva peatüki sätteid kohaldatakse selleks, et tagada, et käesoleva määrusega tagatud füüsiliste isikute kaitse taset ei kahjustata“.

¹⁶ Kohtuotsus, Euroopa Liidu Kohus, 16. juuli 2020, Data Protection Commissioner vs. Facebook Ireland Ltd ja Maximilian Schrems („Schrems II“), C-311/18.

eesmärk on tagada, et isikuandmete kaitse üldmäärusega füüsilistele isikutele ette nähtud kaitsetaset ei kahjustata, kui nende isikuandmeid edastatakse väljapoole EMPd, ning et andmesubjektidele oleks tagatud selline õiguste kaitse tase, mis on sisuliselt samaväärne sellega, mis on kõnealuse määrusega ELis tagatud¹⁷.

13. Vastavalt Euroopa Liidu Kohtu hiljutisele kohtupraktikale¹⁸ on andmeid edastava liikmesriigis avalik-õigusliku asutuse ülesanne hinnata – vajaduse korral vastuvõtva avalik-õigusliku asutuse abiga –, kas kolmandas riigis on tagatud liidu õigusega nõutav kaitsetase, et teha kindlaks, kas rahvusvahelises lepingus sätestatud kaitsemeetmete loetelu on võimalik praktikas järgida, võttes arvesse kolmanda riigi õigusaktidest tulenevat võimalikku riivet seoses nende kaitsemeetmete järgimisega.
14. Sellega seoses tuleks ka märkida, et käesolevates suunistes loetletud kaitsemeetmete tagamiseks võib rahvusvahelistes lepingutes tugineda kolmanda riigi õiguses või rahvusvahelise organisatsiooni siseeeskirjas / reguleerivas raamistikus juba ette nähtud elementidele.

2.1 Eesmärk ja kohaldamisala

15. Rahvusvahelistes lepingutes peaks olema kindlaks määratud lepingu kohaldamisala ning sätestatud selgelt ja konkreetset lepingu eesmärk. Lisaks tuleks neis selgelt märkida mõjutatud isikuandmete liigid ning lepingu alusel edastatavate ja töödeldavate isikuandmete töötlemise liik.

2.2 Määratlused

16. Rahvusvahelised lepingud peaksid sisaldama konkreetse lepingu puhul asjakohaste, isikuandmetega seotud põhimõistete ja õiguste määratlusi, mis on kooskõlas isikuandmete kaitse üldmäärusega. Näiteks peaksid sellised lepingud sisaldama järgmiste oluliste mõistete (kui neile viidatakse) määratlusi: isikuandmed, isikuandmete töötlemine, vastutav töötleja, volitatud töötleja, vastuvõtja ja tundlikud andmed.

2.3 Andmekaitsepõhimõtted

17. Rahvusvahelistes lepingutes tuleb kasutada konkreetset sõnastust, millega kohustatakse kumbagi lepinguosalist tagama peamiste andmekaitsepõhimõtete järgimist.

2.3.1 Eesmärgikohasuse põhimõte

18. Rahvusvahelistes lepingutes peaksid olema sätestatud isikuandmete edastamise ja töötlemise eesmärgid, sealhulgas nendega kooskõlas olevad edasise töötlemise eesmärgid, ning neis tuleks välistada andmete edasine töötlemine algsete eesmärkidega vastuolus olevatel eesmärkidel. Algsete eesmärkidega kooskõlas olevad eesmärgid võivad hõlmata avalikes huvides arhiveerimist, samuti töötlemist teadus- või ajaloouringute või statistilisel eesmärgil. Selguse huvides peaksid andmete töötlemise ja edastamise konkreetset eesmärgid olema rahvusvahelises lepingus loetletud.
19. Selleks et vältida „funktsioonide laienemise“ ohtu, peaks sellistes lepingutes olema ka sätestatud, et edastatud andmeid ei tohi kasutada ühelgi muul eesmärgil peale lepingus sõnaselgelt nimetatud eesmärkide, välja arvatud allpool olevas punktis kirjeldatud viisil.

¹⁷ Kohtuotsus, Euroopa Liidu Kohus, 16. juuli 2020, Data Protection Commissioner vs. Facebook Ireland Ltd ja Maximillian Schrems („Schrems II“), C-311/18, punkt 105.

¹⁸ Samas.

20. Kui mõlemad rahvusvahelise lepingu osalised soovivad lubada isikuandmeid saaval avalik-õiguslikul asutusel kasutada edastatud isikuandmeid esialgsest erineval viisil, mis on algse eesmärgiga kooskõlas, võib isikuandmeid saav avalik-õiguslik asutus neid isikuandmeid edaspidi kasutada ainult juhul, kui see kasutamine on esialgse kasutamisega kooskõlas ja sellest on eelnevalt teatatud andmeid edastavale avalik-õiguslikule asutusele, kes võib konkreetsel põhjustel vastuväiteid esitada.

2.3.2 Andmete õigsuse ja võimalikult väheste andmete kogumise põhimõtted

21. Rahvusvahelises lepingus peab olema sätestatud, et edastatavad ja töödeldavad andmed peavad olema asjakohased ja olulised ning piiratud sellega, mis on nende edastamise ja edasise töötlemise eesmärkide saavutamiseks vajalik.
22. Praktikas on võimalikult väheste andmete kogumise põhimõtte oluline selleks, et vältida asjakohatute või ülemääraste isikuandmete edastamist.
23. Peale selle peaksid andmed olema töötlemise eesmärgi seisukohast õiged ja ajakohased. Seepärast peab rahvusvahelises lepingus olema sätestatud isikuandmeid edastava lepinguosalise kohustus tagada lepingu alusel edastatavate isikuandmete õigsus ja vajaduse korral nende ajakohastamine. Lisaks sellele peaks lepingus olema sätestatud, et kui üks lepinguosaline saab teada ebaõigete või aegunud andmete edastamisest või töötlemisest, peab ta sellest teisele lepinguosalisele viivitamata teatama. Samuti tuleks lepinguga tagada, et kui selgub, et edastatud või töödeldavad andmed on ebaõiged, võtab iga andmeid töötlev osaline kõik mõistlikud meetmed teabe parandamiseks või kustutamiseks.

2.3.3 Säilitamise piiramise põhimõtte

24. Lepinguosalisel peavad tagama, et rahvusvaheline leping sisaldab andmete säilitamist käsitlevat klauslit. Selles klauslis peaks olema eelkõige sätestatud, et isikuandmeid ei säilitata määramata aja jooksul, vaid neid hoitakse andmesubjekte tuvastada võimaldaval kujul ainult seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks andmeid edastati ja hiljem töödeldi. See võib hõlmata andmete säilitamist seni, kuni see on vajalik avalikes huvides arhiveerimise, teadus- või ajaloouringute või statistilisel eesmärgil, tingimusel et andmesubjektide õiguste ja vabaduste kaitsmiseks on kehtestatud asjakohased tehnilised ja korralduslikud meetmed, näiteks täiendavad tehnilised meetmed (nt turvameetmed, pseudonümiseerimine) ning juurdepääsupiirangud. Kui maksimaalne säilitamisperiood ei ole juba sätestatud siseriiklikes õigusaktides või rahvusvahelise organisatsiooni sise-eeskirjas / reguleerivas raamistikus, tuleks maksimaalne säilitamisperiood ette näha lepingu tekstis.

2.3.4 Andmete turvalisus ja konfidentsiaalsus

25. Lepinguosalisel peaksid võtma kohustuse tagada nende teostatava isikuandmete töötlemise ja edastamise turvalisus ja konfidentsiaalsus.

Eelkõige peaksid lepinguosalisel võtma kohustuse kehtestada asjakohased tehnilised ja korralduslikud meetmed, et kaitsta isikuandmeid juhusliku või ebaseadusliku juurdepääsu, hävitamise, kaotamineku, muutmise ja loata avalikustamise eest. Need meetmed võivad hõlmata näiteks krüpteerimist (sh andmete liikumise ajal), pseudonümiseerimist, teabe märgistamist EMPst edastatavate isikuandmetena, isikuandmetele juurdepääsu piiramist, isikuandmete turvalise säilitamise tagamist või selliste poliitikameetmete rakendamist, mille eesmärk on tagada isikuandmete turvalisus ja konfidentsiaalsus.

Turvalisuse taseme puhul tuleks arvesse võtta riske, tehnika taset ja seonduvaid kulusid.

26. Lisaks võib rahvusvahelises lepingus sätestada, et kui üks lepinguosalistest saab teada isikuandmetega seotud rikkumisest, teavitab ta sellest võimalikult kiiresti teist lepinguosalist (teisi lepinguosalisi) ning rakendab mõistlikke ja asjakohaseid abinõusid isikuandmetega seotud rikkumise heastamiseks ja võimaliku kahjuliku mõju minimeerimiseks, sealhulgas teavitades andmesubjekti põhjendamatu viivitusega isikuandmetega seotud rikkumisest, kui see rikkumine kujutab endast tõenäoliselt suurt ohtu füüsilise isiku õigustele ja vabadustele.

Rahvusvahelises lepingus tuleks kindlaks määrata ka isikuandmetega seotud rikkumisest teatamise tähtaeg ja andmesubjekti teavitamise kord.

2.4 Andmesubjektide õigused

27. Rahvusvaheline leping peab tagama andmesubjektide kohtulikult kaitstavad ja tõhusad õigused, nagu on sätestatud isikuandmete kaitse üldmääruse artikli 46 lõikes 1 ja põhjenduses 108.
28. Lepingus peaksid olema loetletud andmesubjektidele kättesaadavad õigused, sealhulgas lepinguosaliste võetavad konkreetsed kohustused nende õiguste tagamiseks. Selleks et rahvusvaheline leping oleks tõhus, tuleb selles ette näha mehhanismid, mis tagavad lepingu tegeliku kohaldamise. Lisaks sellele tuleb andmesubjekti õiguste võimaliku rikkumise puhuks näha ette asjakohased õiguskaitsevahendid.

2.4.1 Õigus läbipaistvusele

29. Lepinguosalisel peavad tagama, et rahvusvahelises lepingus kirjeldatakse sõnaselgelt lepinguosaliste läbipaistvuskohustusi.
30. Sellised kohustused peaksid ühelt poolt hõlmama üldist teadaannet, mis sisaldab vähemalt teavet selle kohta, kuidas ja miks avalik-õiguslikud asutused võivad isikuandmeid töödelda ja edastada, millise vahendi abil isikuandmeid edastatakse, millistele üksustele neid andmeid võib edastada, millised õigused on andmesubjektidele kättesaadavad ja milliseid piiranguid kohaldatakse ning milliseid õiguskaitsevahendeid on võimalik kasutada, samuti vaidlustamiseks või nõude esitamiseks vajalikke kontaktandmeid.
31. Siiski on oluline meenutada, et isikuandmeid edastava avalik-õigusliku asutuse puhul ei piisa üldisest teadaandest asjaomase asutuse veebisaidil. Isikuandmeid edastav avalik-õiguslik asutus peaks andmesubjektidele andma individuaalset teavet kooskõlas isikuandmete kaitse üldmääruse artiklites 13 ja 14 sätestatud teavitamisnõuetega¹⁹.

Rahvusvahelise lepinguga võib ette näha ka mõningad erandid sellisest individuaalselt antavast teabest. Neid erandeid on vähe ja need peaksid olema kooskõlas isikuandmete kaitse üldmääruse artikli 14 lõikes 5 sätestatud eranditega; näiteks juhud, kui andmesubjektil on teave juba olemas või kui sellise teabe esitamine osutub võimatuks või eeldaks ebaproportsionaalseid jõupingutusi.

32. Lepinguosalisel peavad võtma kohustuse teha rahvusvaheline leping andmesubjektidele taotluse korral kättesaadavaks ning avaldada oma veebisaidil kas kogu rahvusvaheline leping või sätted, millega

¹⁹ Vt Euroopa Andmekaitsekomitee suunised määruse 2016/679 kohase läbipaistvuse kohta, WP 260 rev.01, lk 13–22.

nähakse ette asjakohased kaitsemeetmed. Tundliku või muu konfidentsiaalse teabe kaitsmiseks vajalikus ulatuses võib rahvusvahelise lepingu teksti enne selle jagamist või üldsusele kättesaadavaks tegemist redigeerida. Kui see on vajalik selleks, et andmesubjektil oleks võimalik rahvusvahelise lepingu sisust aru saada, peavad lepinguosalisel esitama lepingu teksti sisuka kokkuvõtte.

2.4.2 Õigus andmetega tutvuda, neid parandada, kustutada, nende töötlemist piirata ja esitada vastuväiteid

33. Rahvusvaheline leping peaks kaitsma andmesubjekti õigust saada kõigi temaga seotud töödeldavate isikuandmete kohta teavet ja nendega tutvuda, neid parandada, kustutada ja nende töötlemist piirata ning asjakohasel juhul õigust esitada andmete töötlemise suhtes vastuväiteid andmesubjekti konkreetse olukorraga seotud põhjustel.
34. Seoses andmetega tutvumise õigusega tuleks rahvusvahelises lepingus sätestada, et isikul on õigus saada isikuandmeid saavalt avalik-õiguslikult asutuselt kinnitus selle kohta, kas tema isikuandmeid töödeldakse või mitte, ning kui töödeldakse, siis on tal õigus nende andmetega tutvuda, samuti on tal õigus saada töötlemise kohta konkreetset teavet, mis käsitleb muu hulgas töötlemise eesmärki, asjaomaseid isikuandmete liike, isikuid, kellele isikuandmed avalikustatakse, kavandatud säilitamistähtaega ja õiguskaitse võimalusi.
35. Lisaks sellele tuleks lepingus kindlaks määrata, millal neid õigusi saab kasutada, ning esitada üksikasjad selle kohta, kuidas andmesubjektid saavad neid õigusi kummagi lepinguosalise suhtes kasutada, samuti selle kohta, kuidas lepinguosalisel asjakohastele taotlustele vastavad. Näiteks seoses andmete kustutamisega võiks rahvusvahelises lepingus sätestada, et andmed tuleb kustutada, kui neid on töödeldud ebaseaduslikult või kui neid ei ole töötlemise eesmärgi saavutamiseks enam vaja. Peale selle tuleks rahvusvahelises lepingus sätestada, et lepinguosalisel vastavad andmesubjektide taotlustele mõistlikul viisil ja õigel ajal. Rahvusvahelises lepingus võiks ka sätestada, et lepinguosalisel võivad võtta asjakohaseid meetmeid, näiteks nõuda mõistlikke tasusid halduskulude katmiseks, kui andmesubjekti taotlused on selgelt põhjendamatud või ülemäärased, eelkõige seetõttu, et need on korduvad.
36. Rahvusvahelise lepinguga tuleks samuti ette näha isikuandmeid edastava avalik-õigusliku asutuse kohustus anda andmesubjektile pärast tema isikuandmete edastamist tarbetu viivitusega teavet tema taotluse alusel võetud meetmete kohta, mis tulenevad rahvusvahelise lepinguga ette nähtud õigustest; selleks tuleks lepingus ette näha asjakohane tähtaeg (nt üks kuu). Kui lepinguosalisel ei võta andmesubjekti taotluse alusel meetmeid, tuleks andmesubjektile viivitamata esitada teave meetmete võtmata jätmise põhjuste ning kaebuse esitamise ja õiguskaitsevahendite kasutamise võimaluse kohta; selleks tuleks lepingus ette näha asjakohane tähtaeg (nt ühe kuu jooksul alates taotluse saamisest).
37. Rahvusvahelises lepingus võib ette näha ka erandid nendest õigustest. Näiteks võib ette näha erandid isikuandmete kaitse üldmääruse artikli 15 lõikes 4 ja artikli 17 lõikes 3 sätestatud õigusest andmetega tutvuda ja andmed kustutada. Samamoodi võib ette näha erandid individuaalsetest õigustest, kui isikuandmeid töödeldakse teadus- või ajaloouringute, statistilisel või arhiveerimise eesmärgil, niivõrd kui need õigused võivad tõenäoliselt muuta nende konkreetsete eesmärkide saavutamise võimatuks või seda tõsiselt takistada ning tingimusel, et kehtestatakse asjakohased kaitsemeetmed (nt tehnilised ja korralduslikud meetmed, sealhulgas pseudonümiseerimine). Lisaks võib lepinguga ette näha, et selgelt põhjendamatult või ülemääraste taotluste korral võivad lepinguosalisel keelduda taotluse alusel meetmeid võtmast.

2.4.3 Automatiseeritud töötlusel põhinevate üksikotsuste tegemine

38. Kui see on konkreetse lepingu puhul asjakohane, peaksid rahvusvahelised lepingud üldreeglina sisaldama klauslit, mille kohaselt ei tee isikuandmeid saav avalik-õiguslik asutus üksikotsust, mis põhineb üksnes automatiseeritud töötlusel, sealhulgas profiilianalüüsil, mis toob kaasa asjaomast andmesubjekti puudutavaid õiguslikke tagajärgi või avaldab talle muul sarnasel viisil märkimisväärset mõju. Kui isikuandmete edastamise eesmärk hõlmab andmeid saava avalik-õigusliku asutuse võimalust teha otsuseid, mis põhinevad üksnes automatiseeritud töötlemisel isikuandmete kaitse üldmääruse artikli 22 tähenduses, peaks selline otsuse tegemine toimuma üksnes teataval rahvusvahelises lepingus sätestatud tingimustel, näiteks andmesubjekti sõnaselgel nõusolekul. Kui otsus sellistele tingimustele ei vasta, peaks andmesubjektil olema õigus sellele, et tema suhtes sellist otsust ei tehta. Kui rahvusvaheline leping võimaldab teha automatiseeritud üksikotsuseid, tuleks lepingus igal juhul ette näha vajalikud kaitsemeetmed, sealhulgas õigus saada teavet otsuse aluseks olevate konkreetsete põhjuste ja kasutatud loogika kohta, õigus parandada ebaõiget või mittetäielikku teavet ning õigus otsuse vaidlustamisele ja inimsekkumisele.

2.4.4 Õigus õiguskaitsele

39. Andmesubjektile tagatud õigused peavad olema kohtulikult kaitstavad ja tõhusad. Seetõttu peab andmesubjektil olema juurdepääs õiguskaitsele. Õiguskaitsemehhanismide pakkumise viiside näited on esitatud allpool jaotistes 2.7 ja 3.

2.4.5 Andmesubjektide õiguste piiramine

40. Rahvusvahelises lepingus võib näha ette ka andmesubjektide õiguste piirangud. Need peaksid olema kooskõlas isikuandmete kaitse üldmääruse artiklis 23 sätestatud piirangutega. Iga selline piirang peab olema proportsionaalne meede, mis on demokraatlikus ühiskonnas vajalik, et kaitsta üldist avalikku huvi pakkuvaid olulisi eesmärke, mis vastavad isikuandmete kaitse üldmääruse artikli 23 lõikes 1 loetletud eesmärkidele, sealhulgas eesmärk tagada teiste isikute õigused ja vabadus, riigi julgeolek ja riigikaitse ning süütegude tõkestamine, uurimine, avastamine või nende eest vastutusele võtmine. See peab olema ette nähtud seadusega või rahvusvahelise organisatsiooni suhtes kohaldatava siseeeskirjaga / reguleeriva raamistikuga ning kehtib ainult seni, kuni piirangu põhjus püsib.

2.5 Andmete edasisaatmise ja jagamise (sh avalikustamise ja ametiasutuste juurdepääsu) piirangud

41. Üldjuhul tuleks rahvusvahelise lepinguga sõnaselgelt välistada võimalus, et isikuandmed saanud avalik-õiguslik asutus või rahvusvaheline organisatsioon saadab need edasi isikutele, kes ei ole lepinguga seotud. Sõltuvalt lepingu reguleerimisest ja konkreetsetest asjaoludest võivad lepinguosalisel pidada vajalikuks andmete edasisaatmist lubada. Sellisel juhul ja tingimusel, et järgitakse eesmärgikohasuse põhimõtet,²⁰ tuleks rahvusvahelise lepinguga ette näha, et selline edasisaatmine võib toimuda üksnes juhul, kui andmeid edastav avalik-õiguslik asutus on andnud selleks eelneva sõnaselge loa ning andmeid saavad kolmandad isikud kohustuvad järgima samu andmekaitsepõhimõtteid ja kaitsemeetmeid, mis on sätestatud rahvusvahelises lepingus. See peaks hõlmama kohustust tagada andmesubjektidele samad andmekaitseõigused ja tagatised, nagu on sätestatud rahvusvahelises lepingus, et andmete edasisaatmisel õiguste kaitse tase ei väheneks.

²⁰ Vt jaotis 2.3.1.

42. Üldjuhul tuleks isikuandmete jagamisel sama riigi piires kohaldada samu kaitsemeetmeid nagu andmete edasisaatmise korral, st rahvusvaheline leping peab sellise edasisaatmise välistama ja erandid peaksid olema üldiselt lubatud üksnes juhul, kui andmeid edastav avalik-õiguslik asutus on andnud selleks eelneva sõnaselge loa ning andmeid saavad kolmandad isikud kohustuvad järgima samu andmekaitsepõhimõtteid ja kaitsemeetmeid, mis on sätestatud rahvusvahelises lepingus.
43. Soovitav on, et enne isikuandmeid edastavalt avalik-õiguslikult asutuselt sõnaselge loa taotlemist esitaks isikuandmeid saav avalik-õiguslik asutus või rahvusvaheline organisatsioon piisavalt teavet isikuandmete liigi kohta, mida ta kavatseb edastada/jagada, põhjuste ja eesmärkide kohta, miks ta peab vajalikuks isikuandmeid edastada/jagada, ning – andmete edasisaatmise korral – riikide või rahvusvaheliste organisatsioonide kohta, kellele ta kavatseb isikuandmeid edasi saata, et saaks hinnata kolmanda riigi õigusakte või rahvusvahelise organisatsiooni suhtes kohaldatavat sise-eeskirja / reguleerivat raamistikku.
44. Juhul kui on vaja lubada jagada isikuandmeid kolmanda isikuga, kes asub andmeid saava avalik-õigusliku asutuse või rahvusvahelise organisatsiooniga samas riigis, võib andmete jagamist erijuhtudel lubada kas andmeid edastava avalik-õigusliku asutuse eelneval sõnaselgel loal või tingimusel, et andmeid saaval kolmandal isikul on siduv kohustus järgida rahvusvahelises lepingus sisalduvaid põhimõtteid ja tagatiseid.
45. Lisaks võiks rahvusvahelises lepingus kooskõlas isikuandmete kaitse üldmääruse artiklis 49 loetletud eranditega sätestada erandlikud asjaolud, mille korral võib andmete edasine jagamine toimuda ilma eelneva loata või eespool nimetatud kohustusteta, näiteks kui selline jagamine oleks vajalik andmesubjekti või muude isikute eluliste huvide kaitsmiseks või õigusnõuete koostamiseks, esitamiseks või kaitsmiseks. Sellised erandlikud asjaolud võivad tekkida ka siis, kui andmete edasisaatmine on andmeid saava lepinguosalise suhtes kohaldatava õiguse kohaselt nõutav, kuna see on vajalik otseselt seotud uurimiste/kohtumenetluste läbiviimiseks.
46. Eelmises punktis nimetatud juhtudel tuleks rahvusvahelises lepingus selgelt sätestada konkreetsed ja erandlikud asjaolud, mille korral on selline andmete jagamine lubatud. Lisaks peaks andmeid saav avalik-õiguslik asutus või rahvusvaheline organisatsioon olema kohustatud teavitama andmeid edastanud avalik-õiguslikku asutust enne nende andmete jagamist ning lisama teabe jagatavate andmete, andmeid saava kolmanda isiku ja andmete jagamise õigusliku aluse kohta. Andmeid edastav avalik-õiguslik asutus peaks omakorda säilitama andmeid saava avalik-õigusliku asutuse või rahvusvahelise organisatsiooni teated ning esitama taotluse korral selle teabe oma järelevalveasutusele. Kui selline teavitamine enne andmete jagamist on vastuolus seaduses sätestatud konfidentsiaalsuskohustustega, näiteks kohustusega säilitada uurimise konfidentsiaalsus, tuleks asjakohane teave esitada võimalikult kiiresti pärast andmete jagamist. Sellisel juhul tuleks andmeid edastavale asutusele korrapärase ajavahemike järel anda üldist teavet kindlaksmääratud ajavahemiku jooksul saadud taotluste liigi kohta, sealhulgas taotletud andmete liikide, andmeid taotlenud asutuse ja andmete avalikustamise õigusliku aluse kohta.
47. Kõigi eespool nimetatud stsenaariumide puhul peaks rahvusvaheline leping lubama avaldada isikuandmeid andmeid saava avalik-õigusliku asutusega samas kolmandas riigis asuvatele muudele avalik-õiguslikele asutustele üksnes juhul, kui see ei lähe kaugemale sellest, mis on demokraatlikus ühiskonnas vajalik ja proportsionaalne üldist avalikku huvi pakkuvate oluliste eesmärkide kaitsmiseks kooskõlas isikuandmete kaitse üldmääruse artikli 23 lõikes 1 loetletud eesmärkidega ja Euroopa Liidu Kohtu praktikaga. Hinnates kolmandate riikide ametiasutuste võimalikku juurdepääsu jälgimise eesmärgil, peaks andmeid edastav avalik-õiguslik asutus võtma arvesse Euroopa nelja olulise tagatise

elemente²¹. Need hõlmavad tõhusa õiguskaitsevahendi kättesaadavust andmesubjektidele andmeid saava avalik-õigusliku asutuse kolmandas riigis, kui ametiasutustel on nende isikuandmete juurdepääs²². Rahvusvahelistele organisatsioonidele isikuandmete edastamise korral peab selline juurdepääs olema kooskõlas rahvusvahelise avaliku õigusega ning ei tohi piirata rahvusvahelise organisatsiooni privileege ja immunitete.

48. Olenevalt konkreetsest juhtumist võib olla kasulik nõuda, et rahvusvahelisele lepingule lisataks lisa, milles loetletakse õigusaktid, mis reguleerivad andmete edasist jagamist sihtriigis teiste avalik-õiguslike asutustega, sealhulgas jälgimise eesmärgil. Sellise lisa võimalikud muudatused tuleb andmeid edastavale lepinguosalisele kindlaksmääratud aja jooksul teatavaks teha.

2.6 Tundlikud isikuandmed

49. Kui rahvusvahelise lepinguga nähakse ette isikuandmete kaitse üldmääruse artikli 9 lõike 1 tähenduses tundlike isikuandmete edastamine, tuleks lisada konkreetseid riske leevendavad täiendavad kaitsemeetmed, mida andmeid saav avalik-õiguslik asutus või rahvusvaheline organisatsioon peab rakendama. Need võivad hõlmata näiteks piiranguid, nagu juurdepääsupiirangud, teabe töötlemise eesmärgi piirangud, edasisaatmise piirangud jne, või konkreetseid kaitsemeetmeid, nagu täiendavad turvameetmed, mille kohaselt peavad teabele juurdepääsu omavad töötajad olema saanud eriväljaõppe.

2.7 Õiguskaitsemehhanismid

50. Andmesubjektide kohtulikult kaitstavate ja tõhusate õiguste tagamiseks tuleb rahvusvahelise lepinguga ette näha süsteem, mis võimaldab andmesubjektidel jätkuvalt tugineda õiguskaitsemehhanismidele pärast nende andmete edastamist EMP-välisele riigile või rahvusvahelisele organisatsioonile. Need õiguskaitsemehhanismid peavad pakkuma õiguskaitsevahendeid isikutele, keda valitud dokumendi sätete rikkumine mõjutab, ning seega võimaldama andesubjektidel, kelle isikuandmed on edastatud väljapoole EMPd, esitada sellise rikkumise kohta kaebusi ja lasta need kaebused lahendada. Eelkõige tuleb andmesubjektile tagada tõhus võimalus esitada kaebus avalik-õiguslikele asutustele, kes on rahvusvahelise lepingu osalised, ja sõltumatule järelevalvemehhanismile (kas otse või pärast asjaomase lepinguosalise poole pöördumist). Lisaks peaks põhimõtteliselt olema tagatud edasikaebeõigus.
51. Esiteks peaks andmeid saav avalik-õiguslik asutus võtma kohustuse sisse seada mehhanism, mille abil tõhusalt ja õigeaegselt käsitleda ja lahendada andmesubjektide kaebusi kokkulepitud andmekaitsemeetmete järgimise kohta. Samuti tuleks andmesubjektidele anda võimalus kasutada tõhusaid halduslikke õiguskaitsevahendeid sõltumatu järelevalveasutuse kaudu, sealhulgas võimaluse korral sõltumatu andmekaitseasutuse kaudu²³.
52. Teiseks peaks leping tagama edasikaebeõiguse, sealhulgas õiguse nõuda isikuandmete ebaseaduslikust töötlemisest tuleneva materiaalse ja mittemateriaalse kahju hüvitamist. Kui tõhusat edasikaebeõigust ei ole võimalik tagada, näiteks siseriikliku õiguse piirangute või andmeid saava avalik-õigusliku asutuse, nt rahvusvahelise organisatsiooni eristaatuse tõttu, tuleb rahvusvahelises lepingus ette näha alternatiivsed kaitsemeetmed. Need alternatiivsed kaitsemeetmed peavad pakkuma andmesubjektile

²¹ Vt Euroopa Andmekaitsekoostöögrupi soovitus 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis.

²² Vt Euroopa Andmekaitsekoostöögrupi soovitus 02/2020, „Tagatis D“, lk 13 jj.

²³ Vt ka jaotis 2.8 järelevalvemehhanismi kohta.

tagatise, mis on sisult samaväärsed Euroopa Liidu põhiõiguste harta (edaspidi „Eli põhiõiguste harta“) artiklis 47 nõutud tagatistega²⁴.

53. Sellisel juhul võiks rahvusvahelise lepinguga luua struktuuri, mis võimaldab andmesubjektil teostada oma õigusi väljaspool kohtuid, näiteks kohtulaadsete siduvate mehhanismide kaudu, nagu vahetamine või vaidluste kohtuvälise lahendamise mehhanism (nt vahendamine), mis tagab sõltumatu läbivaatamise ja mille otsus on andmeid saavale avalik-õiguslikule asutusele siduv²⁵. Lisaks sellele võib isikuandmeid edastav avalik-õiguslik asutus võtta kohustuse kahju hüvitada, kui sõltumatul läbivaatamisel leiab kinnitust, et isikuandmeid on töödeldud ebaseaduslikult.

Erandjuhul võib lepinguga kehtestada muud, sama sõltumatud ja tõhusad õiguskaitsemehhanismid, näiteks sellised tõhusad õiguskaitsemehhanismid, mida rakendavad rahvusvahelised organisatsioonid.

54. Kõigi eespool nimetatud õiguskaitsemehhanismide puhul peaks rahvusvaheline leping sisaldama lepinguosaliste kohustust teavitada üksteist menetluse tulemustest, eelkõige juhul, kui üksikisiku kaebus jäetakse rahuldamata või kui seda ei lahendata.
55. Õiguskaitsemehhanismiga peab kaasnema andmeid edastava avalik-õigusliku asutuse võimalus peatada või lõpetada isikuandmete edastamine rahvusvahelise lepingu alusel, kui lepinguosalistel ei õnnestu vaidlust rahumeelselt lahendada, kuni ta leiab, et andmeid saav avalik-õiguslik asutus on probleemi rahuldavalt lahendanud. Sellise peatamise või lõpetamisega, kui seda võimalust kasutatakse, peab kaasnema andmeid saava avalik-õigusliku asutuse kohustus isikuandmed tagastada või kustutada. Andmeid edastav avalik-õiguslik asutus peab andmete edastamise peatamisest või lõpetamisest teatama pädevale riiklikule järelevalveasutusele.

²⁴ Kohtuotsus, Euroopa Liidu Kohus, 16. juuli 2020, Data Protection Commissioner vs. Facebook Ireland Ltd ja Maximillian Schrems („Schrems II“), C-311/18, punktid 96, 186 jj.

²⁵ Kohtuotsus, Euroopa Liidu Kohus, 6. oktoober 2015, Maximillian Schrems vs. Data Protection Commissioner („Schrems“), C-362/14, punktid 41 ja 95; kohtuotsus, Euroopa Liidu Kohus, 16. juuli 2020, Data Protection Commissioner vs. Facebook Ireland Ltd ja Maximillian Schrems („Schrems II“), C-311/18, punktid 186, 187, 189, 195 jj.

2.8 Järelevalvemehhanismid

56. Selleks et tagada kõigi rahvusvahelisest lepingust tulenevate kohustuste täitmine, tuleb rahvusvahelise lepinguga ette näha sõltumatu järelevalve lepingu nõuetekohase kohaldamise ja lepinguga ette nähtud õiguste riivete üle.
57. Esiteks tuleks lepinguga ette näha asutusesisene järelevalve lepingu täitmise tagamiseks. Kumbki lepinguosaline peaks korrapäraselt kontrollima kehtestatud menetlusi ja lepingus sätestatud kaitsemeetmete tõhusat kohaldamist. Korrapärase sisekontrollide käigus tuleks kontrollida ka õigusaktide võimalikke muudatusi, mis takistavad lepinguosalis(t)el järgida rahvusvahelises lepingus sätestatud andmekaitsepõhimõtteid ja kaitsemeetmeid. Lisaks võiks ette näha, et kumbki lepinguosaline võib taotleda teiselt lepinguosaliselt sellise läbivaatamise teostamist. Rahvusvahelises lepingus tuleb sätestada nõue, et lepinguosalisel peavad vastama teise lepinguosalise järelepärimistele lepingus sätestatud kaitsemeetmete tõhusa rakendamise kohta. Iga läbivaatamist teostav lepinguosaline peaks edastama läbivaatamise tulemused teis(t)ele lepinguosalis(t)ele. Ideaaljuhul tuleks selline teave edastada ka lepingu üle järelevalvet teostavale sõltumatule järelevalvemehhanismile.
58. Lisaks sellele tuleb rahvusvahelises lepingus sätestada lepinguosalise kohustus teavitada viivitamata teist lepinguosalist, kui ta mingil põhjusel ei suuda lepingus sätestatud kaitsemeetmeid tõhusalt rakendada. Selleks puhuks tuleb rahvusvahelise lepinguga näha andmeid edastavale avalik-õiguslikule asutusele ette võimalus peatada või lõpetada selle lepingu alusel isikuandmete edastamine andmeid saavale avalik-õiguslikule asutusele, kuni andmeid saav avalik-õiguslik asutus teatab andmeid edastavale avalik-õiguslikule asutusele, et ta suudab taas tegutseda viisil, mis on kaitsemeetmetega kooskõlas. Andmeid edastav asutus peab teavitama pädevat riiklikku järelevalveasutust nii olukorra muutumisest kui ka andmete edastamise peatamisest või lepingu lõpetamisest.
59. Teiseks tuleb lepinguga ette näha sõltumatu järelevalve, mille eesmärk on tagada, et lepinguosalisel järgivad lepingu sätteid. See nõue tuleneb otseselt ELi põhiõiguste hartast²⁶ ja Euroopa inimõiguste ja põhivabaduste kaitse konventsioonist²⁷ vastavalt Euroopa Inimõiguste Kohtu praktikale ning esmase õiguse sätetest²⁸ ja asjaomasest kohtupraktikast.
60. Euroopa Liidu Kohus on alates 2015. aastast²⁹ korduvalt sedastanud vajadust sõltumatu õiguskaitse- ja järelevalvemehhanismi järele³⁰. Ka Euroopa Inimõiguste Kohus on oma otsustes sageli rõhutanud, et

²⁶ ELi põhiõiguste harta artiklid 7, 8 ja 47.

²⁷ Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 8.

²⁸ Lissaboni lepingu artikkel 6:

„1. Liit tunnustab 7. detsembri 2000. aasta Euroopa Liidu põhiõiguste hartas, nagu seda on kohandatud 12. detsembril 2007. aastal Strasbourgis, sätestatud õigusi, vabadusi ja põhimõtteid, millel on aluslepingutega võrreldes samaväärne õigusjõud.

Harta sätteid ei laienda mingil viisil liidu pädevust, mis on määratletud aluslepingutega.

Hartas esitatud õigusi, vabadusi ja põhimõtteid tõlgendatakse vastavalt harta VII jaotise üldsätetele, mis reguleerivad selle tõlgendamist ja kohaldamist, võttes nõuetekohaselt arvesse hartas osutatud selgitusi, milles on esitatud asjaomaste sätete allikad.

2. Liit ühineb Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga. Sellega ühinemine ei mõjuta liidu pädevust, mis on määratletud aluslepingutega.

3. Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga tagatud ja liikmesriikide ühistest põhiseaduslikest tavadest tulenevad põhiõigused on liidu õiguse üldpõhimõtted“.

²⁹ Kohtuotsus, Euroopa Liidu Kohus, 6. oktoober 2015, Maximilian Schrems vs. Data Protection Commissioner („Schrems“), C-362/14, punktid 41 ja 95.

³⁰ Euroopa Liidu Kohtu 27. juuli 2017. aasta arvamus 1/15 Euroopa Liidu ja Kanada vahelise broneeringuinfo edastamist käsitleva kavandatava lepingu kohta, 26. juuli 2017, punkt 228 jj; Euroopa Liidu Kohtu 30. aprilli

igasuguse sekkumise korral Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 8 sätestatud õigusesse eraelu austamisele tuleb rakendada tõhusat, sõltumatut ja erapooletut järelvalvesüsteemi³¹.

61. Lepingus võiks näiteks ette näha järelvalve pädeva järelvalveasutuse poolt, kui selline asutus on EMPst isikuandmeid saava avalik-õigusliku asutuse riigis olemas, isegi kui isikuandmete kaitse üldmääruses ei ole sätestatud, et pädev järelvalveasutus peab olema väline järelvalveasutus. Lisaks võiks leping sisaldada andmeid saava lepinguosalise vabatahtlikku kohustust teha EMP järelvalveasutustega koostööd.
62. Kui kolmandas riigis või rahvusvahelises organisatsioonis puudub konkreetselt andmekaitseõiguse järelvalve eest vastutav järelvalveasutus või isik, tuleb sõltumatu, tõhusa ja erapooletu järelvalvemehhanismi vajadus täita muude vahenditega. Sõltumatu järelvalvemehhanismi liik võib sõltuda konkreetselt juhtumist.
63. Lepingus võib näiteks viidata kolmanda riigi olemasolevatele järelvalveasutustele, mis ei ole andmekaitse valdkonna järelvalveasutused. Kui ei ole võimalik tagada struktuuriliselt või institutsionaalselt sõltumatut välist järelvalvet, näiteks teatavate rahvusvaheliste organisatsioonide privileegide ja immuuniteetide tõttu, võiks järelvalve tagada ka funktsionaalselt sõltumatute mehhanismide abil. Sel juhul peaks järelvalvet teostama üksus, mis ei ole küll väline, kuid täidab oma ülesandeid sõltumatult, st juhiseid saamata ning piisavate inim-, tehniliste ja rahaliste ressursidega jne. Järelvalvet teostava üksuse otsused peavad olema andmeid saavale lepinguosalisele siduvad.

2.9 Lõpetamisklausel

64. Rahvusvahelise lepinguga tuleks ette näha, et kõiki EMPst rahvusvahelise lepingu alusel enne lepingu tegelikku lõpetamist edastatud isikuandmeid töödeldakse jätkuvalt kooskõlas rahvusvahelise lepingu sätetega.

2019. aasta arvamus 1/17 Kanada ja Euroopa Liidu vahelise ulatusliku majandus- ja kaubanduslepingu kohta, punkt 190 jj.

³¹ Kohtuotsus, Euroopa Inimõiguste Kohus, 6. september 1978, Klass vs. Saksamaa, punktid 55 ja 56. Euroopa Inimõiguste Kohtu praktikast tulenev nõue kehtib ka ELi põhiõiguste harta artiklite 7 ja 8 rikkumise suhtes, kuna ELi põhiõiguste harta artikli 52 lõike 3 kohaselt on nende põhiõiguste tähendus ja ulatus samad, mis on sätestatud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 8.

3 KONKREETNE TEAVE ISIKUANDMETE KAITSE ÜLDMÄÄRUSE ARTIKLI 46 KOHTA

3.1 Konkreetne teave õiguslikult siduvate ja täitmisele pööratavate dokumentide kohta

– isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkt a

65. Isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkt a võimaldab EMP avalik-õiguslikul asutusel ilma järelevalveasutuse eelneva loata võtta kolmanda riigi avalik-õiguslikele asutustele või rahvusvahelisele organisatsioonile andmete edastamiseks vastastikku sõlmitud dokumendid. Sellised dokumendid peavad olema õiguslikult siduvad ja täitmisele pööratavad. Selle sätte alusel võib seega kasutada rahvusvahelisi lepinguid, avalikul õigusel põhinevaid lepinguid või vahetult kohaldatavaid halduslepinguid.
66. Mis tahes õiguslikult siduv ja täitmisele pööratav dokument peaks hõlmama peamisi andmekaitsepõhimõtteid ja andmesubjektide õigusi, nagu on nõutud isikuandmete kaitse üldmääruses.
67. Lepinguosalised peavad võtma kohustuse kehtestada andmete edastamiseks piisavad andmekaitsemeetmed. Sellest tulenevalt tuleks lepingus sätestada ka viis, kuidas andmeid saav avalik-õiguslik asutus kohaldab peamisi andmekaitsepõhimõtteid ja andmesubjektide õigusi kõigi edastatud isikuandmete suhtes, tagamaks, et isikuandmete kaitse üldmääruse kohast füüsiliste isikute kaitse taset ei kahjustata.
68. Kui õiguslikult siduvate ja täitmisele pööratavate dokumentidega ei ole võimalik tagada tõhusat edasikaebeõigust, mistõttu tuleb kokku leppida alternatiivses õiguskaitsemehhanismis, peaksid EMP avalik-õiguslikud asutused enne selliste dokumentide sõlmimist konsulteerima pädeva järelevalveasutusega.
69. Kuigi dokumendi vorm ei ole otsustava tähtsusega ning oluline on, et see oleks õiguslikult siduv ja täitmisele pööratav, leiab Euroopa Andmekaitsekoostöögrupp, et parim valik oleks sätestada üksikasjalikud andmekaitseklauslid vahetult dokumendis endas. Kui see lahendus ei ole konkreetsete asjaolude tõttu siiski teostatav, soovib andmekaitsekoostöögrupp tungivalt lisada andmekaitsepõhimõtteid sisaldava üldklausli vahetult dokumendi teksti ning esitada üksikasjalikumad sätted ja kaitsemeetmed dokumendi lisas.

3.2 Konkreetne teave halduskokkulepete kohta – isikuandmete kaitse üldmääruse artikli 46 lõike 3 punkt b

70. Isikuandmete kaitse üldmääruse artikli 46 lõike 3 punktiga b on ette nähtud ka alternatiivsed vahendid, st halduskokkulepped (nt vastastikuse mõistmise memorandum), mis tagavad kaitse kohustuste kaudu, mille kumbki osaline kokkuleppe jõustamiseks endale võtab.
71. Sellega seoses on isikuandmete kaitse üldmääruse artikli 46 lõikes 1 ja põhjenduses 108 sätestatud, et niisugused kokkulepped peavad tagama andmesubjektide kohtulikult kaitstavate õiguste ja tõhusate õiguskaitsevahendite. Kui kaitsemeetmed nähakse ette halduskokkuleppega, mis ei ole õiguslikult siduv, tuleb selleks saada pädeva järelevalveasutuse luba.

72. Õiguslikult mittesiduvate halduskokkulepete kasutamist avalikus sektoris kaitsemeetmete tagamiseks tuleks hoolikalt hinnata, pidades silmas töötlemise eesmärki ja töödeldavate andmete laadi. Kui EMP üksikisikute andmekaitsealased õigused ja õiguskaitsevahendid ei ole kolmanda riigi siseriiklikus õiguses või rahvusvahelise organisatsiooni sise-eeskirjas / reguleerivas raamistikus sätestatud, tuleks eelistada õiguslikult siduva lepingu sõlmimist. Kasutatava dokumendi liigist olenemata peavad kehtestatud meetmed olema tõhusad, et tagada nõuetekohane rakendamine, täitmisele pööramine ja järelevalve.
73. Halduskokkulepete korral tuleb üksikisikute tõhusate õiguste, õiguskaitse ja järelevalve tagamiseks rakendada konkreetseid meetmeid. Eelkõige peaks mittesiduv dokument sisaldama tõhusate ja kohtulikult kaitstavate õiguste tagamiseks EMPst isikuandmeid saava avalik-õigusliku asutuse kinnitust selle kohta, et isikute õigused on täielikult tagatud tema riigi siseriikliku õigusega ja et EMP üksikisikud saavad neid teostada samadel tingimustel nagu asjaomase kolmanda riigi kodanikud ja elanikud. Sama kehtib siis, kui EMP üksikisikutel on andmeid saava avalik-õigusliku asutuse riigi siseriikliku õigusraamistiku alusel võimalik kasutada halduslikke ja kohtulikke õiguskaitsevahendeid. Ka rahvusvahelised organisatsioonid peaksid andma kinnituse üksikisikute õiguste kohta, mis on nende sise-eeskirjadega tagatud, ning olemasolevate õiguskaitsemehhanismide kohta.
74. Kui eeltoodud kinnitusi ei ole võimalik anda, tuleks üksikisikute õigused tagada kokkuleppeosaliste konkreetsete kohustustega, millele lisanduvad menetluslikud mehhanismid, et tagada nende kohustuste täitmine ja üksikisikute õiguskaitse. Need konkreetsete kohustused ja menetluslikud mehhanismid peavad praktikas võimaldama tagada vastavuse kaitsetasemele, mis on sisuliselt samaväärne sellega, mis on ELis tagatud isikuandmete kaitse üldmäärusega.

Sellised menetluslikud mehhanismid võivad hõlmata näiteks kokkuleppeosaliste kohustust teavitada üksteist EMP üksikisikute taotlustest ning lahendada õigeaegselt vaidlused või nõuded.

75. Kui vaidlusi või nõudeid ei õnnestu kokkuleppeosaliste vahel rahumeelselt lahendada, tuleb üksikisikule tagada sõltumatu ja tõhus õiguskaitse alternatiivsete mehhanismide kaudu, näiteks võimaldades tal kasutada alternatiivset vaidluste lahendamise mehhanismi, nagu vahetamine või vahendamine. Selline alternatiivne vaidluste lahendamise mehhanism peab olema siduv³².
76. Olenevalt konkreetsest juhtumist tuleks tõhusa õiguskaitse tagamiseks näha halduskokkuleppes ette kõigi või mõnede eespool nimetatud meetmete kombinatsioon. Vastuvõetavad võivad olla ka muud meetmed, mida käesolevates suunistes ei käsitleta, kui need meetmed tagavad sõltumatu ja tõhusa õiguskaitse.
77. Pädev järelevalveasutus vaatab kõik isikuandmete kaitse üldmääruse artikli 46 lõike 3 punkti b kohaselt koostatud halduskokkulepped igal üksikjuhul eraldi läbi ja vajaduse korral järgneb sellele läbivaatamisele asjakohane Euroopa Andmekaitsekoostöö menetlus. Pädev järelevalveasutus lähtub kokkuleppe kontrollimisel käesolevates suunistes esitatud üldistest soovitustest, kuid võib sõltuvalt konkreetsest juhtumist nõuda ka rohkem tagatisi.

³² Kohtuotsus, Euroopa Liidu Kohus, 16. juuli 2020, Data Protection Commissioner vs. Facebook Ireland Ltd ja Maximilian Schrems („Schrems II“), C-311/18, punktid 189, 196 jj.

4 MENETLUSLIKUD KÜSIMUSED

78. Pädev järelevalveasutus vaatab isikuandmete kaitse üldmääruse artikli 46 lõike 3 punkti b alusel koostatud halduskokkulepped igal üksikjuhul eraldi läbi, kuna selliste kokkulepete korral on nõutav pädeva järelevalveasutuse luba; pädev järelevalveasutus kohaldab vastavalt isikuandmete kaitse üldmääruse artikli 46 lõikele 4 järjepidevuse mehhanismi kooskõlas kõnealuse määruse artikli 64 lõikega 2. Juhul kui siduvates ja täitmisele pööratavates dokumentides nähakse ette alternatiivsed õiguskaitsemehhanismid vastavalt isikuandmete kaitse üldmääruse artikli 46 lõike 2 punktile a, soovitab Euroopa Andmekaitsekoostöögrupi pidada nõu ka pädeva järelevalveasutusega. Euroopa Andmekaitsekoostöögrupi tungiv soovitus on konsulteerida pädeva järelevalveasutusega varases etapis.

Euroopa Andmekaitsekoostöögrupi nimel

eesistuja

(Andrea Jelinek)