Suunised

Suunised 07/2022 sertifitseerimise kui andmeedastusvahendi kohta

Versioon 2.0

Vastu võetud 14. veebruaril 2023

VERSIOONID

Versioon 1.0	14. juuni 2022	Suuniste vastuvõtmine avalikuks konsultatsiooniks
Versioon 2.0	14. veebruar 2023	Suuniste vastuvõtmine pärast avalikku konsultatsiooni

KOKKUVÕTE

Isikuandmete kaitse üldmääruse artiklis 46 on sätestatud, et andmeeksportijad peavad kehtestama asjakohased kaitsemeetmed isikuandmete edastamiseks kolmandatele riikidele või rahvusvahelistele organisatsioonidele. Sellega seoses on asjakohaseid kaitsemeetmeid, mida andmeeksportijad võivad kasutada artikli 46 alusel andmete edastamisel kolmandatele riikidele, isikuandmete kaitse üldmäärusega mitmekesistatud, lisatud on muu hulgas sertifitseerimine kui uus andmeedastusmehhanism (isikuandmete kaitse üldmääruse artikli 42 lõige 2 ja artikli 46 lõike 2 punkt f).

Käesolevates suunistes antakse juhised isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkti f kohaldamiseks isikuandmete edastamisel kolmandatesse riikidesse või rahvusvahelistele organisatsioonidele sertifikaadi alusel. Dokument on jaotatud neljaks osaks ja sellel on üks lisa.

Esimeses osas („ÜLDINE TAUST“) selgitatakse, et suunised täiendavad juba olemasolevaid üldisi suuniseid 1/2018 sertifitseerimise kohta ja käsitlevad isikuandmete kaitse üldmääruse V peatüki erinõudeid, kui sertifitseerimist kasutatakse andmeedastusvahendina. Isikuandmete kaitse üldmääruse artikli 44 kohaselt peab igasugune isikuandmete edastamine kolmandatele riikidele või rahvusvahelistele organisatsioonidele vastama lisaks isikuandmete kaitse üldmääruse V peatükile ka määruse muude sätete tingimustele. Seetõttu tuleb esimese sammuna tagada isikuandmete kaitse üldmääruse üldsätete täitmine ja teise sammuna vastavus isikuandmete kaitse üldmääruse V peatüki sätetele. Kirjeldatakse osalejaid, kes selles kontekstis on kaasatud, ja nende peamisi rolle, keskendudes eriti rollile, mida täidab andmeimportija, kellele sertifikaat antakse, ja rollile, mida täidab andmeeksportija, kes kasutab sertifikaati oma andmeedastuse vahendina (arvestades, et vastutus andmetöötluse nõuetele vastavuse eest jääb andmeeksportijale). Selles kontekstis võib sertifitseerimine hõlmata ka meetmeid, mis täiendavad edastamisvahendeid, et tagada vastavus ELi isikuandmete kaitse tasemele. Suuniste esimene osa sisaldab ka teavet andmeedastusvahendina kasutatava sertifikaadi saamise protsessi kohta.

Käesolevate suuniste teises osas („AKREDITEERIMISNÕUETE RAKENDAMISE JUHISED“) tuletatakse meelde, et sertifitseerimisasutuse akrediteerimise nõuded on sätestatud standardis ISO 17065 ja need tulenevad ka isikuandmete kaitse üldmääruse artikli 43 kohast sertifitseerimisasutuste akrediteerimist käsitlevate suuniste 4/2018 ja nende lisa tõlgendamisest V peatüki taustal. Siiski selgitatakse käesolevates suunistes andmete edastamise kontekstis täiendavalt mõningaid sertifitseerimisasutusele kohaldatavaid akrediteerimisnõudeid.

Käesolevate suuniste kolmandas osas („SERTIFITSEERIMISE ERIKRITEERIUMID“) antakse juhiseid sertifitseerimise kriteeriumide kohta, mis on juba loetletud suunistes 1/2018, ja kehtestatakse täiendavad erikriteeriumid, mis tuleks lisada sertifitseerimismehhanismi, mida kasutatakse edastusvahendina andmete edastamisel kolmandatele riikidele. Nende kriteeriumide hulgas on kolmanda riigi õigusnormide hindamine, andmeeksportijate ja -importijate üldised kohustused, andmete edasisaatmise, hüvitamise ja täitmise tagamise eeskirjad, protsess ja meetmed olukordades, kus siseriiklikud õigusaktid ja tavad takistavad sertifitseerimise ja kolmanda riigi ametiasutuste andmetele juurdepääsu taotluste osana võetud kohustuste täitmist.

Suuniste neljandas osas („SIDUVAD JA TÄITMISELE PÖÖRATAVAD KOHUSTUSED, MIS TULEB RAKENDADA“) on esitatud elemendid, mida tuleks käsitleda siduvates ja täitmisele pööratavates kohustustes, mida vastutavad töötlejad või volitatud töötlejad, kelle suhtes isikuandmete kaitse üldmäärust ei kohaldata, peaksid võtma, et tagada kolmandatele riikidele edastatud andmete jaoks asjakohased kaitsemeetmed. Need kohustused, mis võivad olla sätestatud eri dokumentides, sealhulgas lepingutes,

hõlmavad eelkõige garantiid, et andmeimportijal ei ole mingit põhjust arvata, et kolmandas riigis asjaomase töötlemise suhtes kohaldatavad õigusnormid ja tavad, sealhulgas mis tahes nõuded isikuandmete avalikustamiseks või meetmed, millega antakse ametiasutustele juurdepääs andmetele, takistaksid tal täitmast tema sertifitseerimisest tulenevaid kohustusi.

Suuniste LISA sisaldab näiteid lisameetmete kohta, mis on kooskõlas soovituste 01/2020 („Soovitused 01/2020 edastusvahendeid täiendavate meetmete kohta, et tagada vastavus isikuandmete kaitse ELi tasemega“) II lisas loetletud lisameetmetega sertifitseerimise kasutamisel andmeedastusvahendina. Näited on koostatud eesmärgiga juhtida tähelepanu kriitilistele olukordadele.

SISUKORD

Euroopa Andmekaitsenõukogu,

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 protokolli nr 37, mida on muudetud EMP ühiskomitee 6. juuli 2018. aasta otsusega nr 154/2018[1],

võttes arvesse oma kodukorra artiklit 12 ja artiklit 22,

ON VASTU VÕTNUD JÄRGMISED SUUNISED

1 ÜLDINE TAUST

1.1 Eesmärk ja kohaldamisala

1. Käesoleva dokumendi eesmärk on anda juhiseid isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkti f kohaldamiseks isikuandmete edastamisel kolmandatesse riikidesse või rahvusvahelistele organisatsioonidele sertifikaadi alusel. Euroopa Andmekaitsenõukogu on juba avaldanud üldised suunised isikuandmete kaitse üldmääruse alusel sertifitseerimise[2] ja akrediteerimise[3] kohta. Seetõttu kajastavad käesolevad uued suunised ainult sertifitseerimise kui andmeedastusvahendi konkreetseid aspekte. Suunistes täpsustatakse isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkti f ja artikli 42 lõike 2 kohaldamist, pakkudes selle kohta praktilisi juhiseid ja lisades juba avaldatud suunistesse uusi elemente.

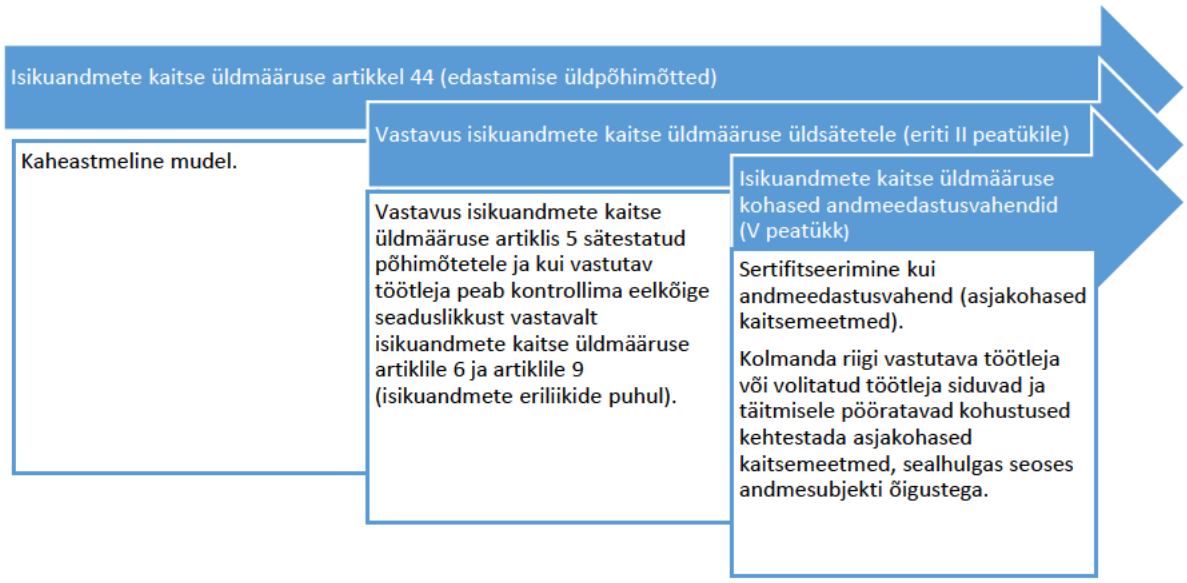
2. Euroopa Andmekaitsenõukogu hindab käesolevate suuniste toimimist nende praktilisel kohaldamisel saadud kogemuste valguses ja annab lisajuhiseid, et selgitada allpool loetletud elementide kohaldamist, sealhulgas sertifitseerimislepingu rolli seoses siduvate ja täitmisele pööratavate kohustustega, millele osutatakse isikuandmete kaitse üldmääruse artikli 46 lõike 2 punktis f.

1.2 Andmete rahvusvahelise edastamise suhtes kohaldatavad üldeeskirjad

3. Isikuandmete kaitse üldmääruse artikli 44 kohaselt peab igasugune isikuandmete edastamine kolmandatele riikidele[4] või rahvusvahelistele organisatsioonidele vastama lisaks isikuandmete kaitse üldmääruse V peatükile ka määruse muude sätete tingimustele. Seetõttu peab iga edastamine vastama muu hulgas 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. Esimese sammuna tuleb tagada isikuandmete kaitse

[1] Käesoleva dokumendi viiteid liikmesriikidele tuleks käsitada viidetena EMP liikmesriikidele.
[2] Suunised 1/2018 määruse (EL) 2016/679 artiklite 42 ja 43 kohase sertifitseerimise ja sertifitseerimiskriteeriumide kindlaksmääramise kohta.
[3] Suunised 4/2018 isikuandmete kaitse üldmääruse (2016/679) artikli 43 kohase sertifitseerimisasutuste akrediteerimise kohta.
[4] Suunised 05/2021 isikuandmete kaitse üldmääruse artikli 3 ja V peatüki rahvusvahelist edastamist käsitlevate sätete koostoime kohta, lk 4.

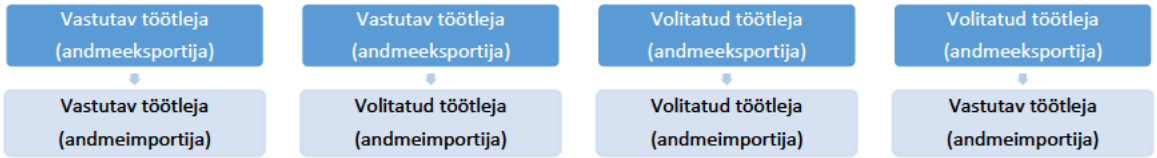
üldmääruse üldsätete täitmine ja teise sammuna vastavus isikuandmete kaitse üldmääruse V peatüki sätetele.



4. 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“. Isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkti f kohaselt võib sellised asjakohased kaitsemeetmed ette näha heakskiidetud sertifitseerimismehhanismiga, koos kolmanda riigi vastutava töötleja või volitatud töötleja siduvate ja täitmisele pööratavate kohustustega kehtestada asjakohased kaitsemeetmed, sealhulgas andmesubjekti õiguste osas.

5. Selle tulemusena võib andmeeksportija otsustada tugineda andmeimportijalt saadud sertifikaadile kui elemendile, mis tõendab tema kohustuste täitmist, nt vastavalt isikuandmete kaitse üldmääruse artikli 24 lõikele 3 või artikli 28 lõikele 5. Andmeimportija võib otsustada taotleda sertifikaati, tõendamaks et ta on kehtestanud asjakohased kaitsemeetmed.

6. Nii andmeeksportija kui ka andmeimportija võivad täita erinevaid rolle (näiteks vastutav töötleja või volitatud töötleja),[5] olenevalt V peatükis sätestatud töötlemisest, mis toob kaasa erinevad kohustused:



7. Lisaks sertifitseerimise või muude artiklites 45 ja 46 osutatud andmeedastusvahendite või -mehhanismide kasutamisele on isikuandmete kaitse üldmääruse artiklis 49 sätestatud, et piiratud arvul konk-

[5] Vt allpool: SERTIFITSEERIMISKRITEERIUMIDE RAKENDAMISE JUHISED

reetsetel juhtudel võib rahvusvaheline andmeedastus toimuda ka siis, kui ei järgita ühtegi muud V peatükis sätestatud mehhanismi[6]. Nagu on aga Euroopa Andmekaitsenõukogu varasemates suunistes selgitatud, tuleb isikuandmete kaitse üldmääruse artiklis 49 sätestatud erandeid tõlgendada kitsendavalt ja need on peamiselt seotud töötlemistoimingutega, mis on juhtumipõhised ja mittekorduvad[7].

1.3 Kes on kaasatud osalejad ja milline on nende roll sertifitseerimise kui andmeedastusvahendi puhul?

8. Järjepidevuse tagamiseks on **Euroopa Andmekaitsenõukogule** antud õigus kiita heaks kogu EMPd hõlmavaid sertifitseerimiskriteeriume (Euroopa andmekaitsepitser) ning esitada arvamusi järelevalveasutuste sertifitseerimiskriteeriume ja sertifitseerimisasutuste akrediteerimisnõudeid käsitlevate otsuse eelnõude kohta. Ka on andmekaitsenõukogu pädevuses koondada kõik sertifitseerimismehhanismid ning andmekaitsepitserid ja -märgised registrisse ja teha need üldsusele kättesaadavaks[8].

9. **Järelevalveasutused** kiidavad sertifitseerimiskriteeriumid heaks, kui sertifitseerimismehhanism ei ole Euroopa andmekaitsepitser[9]. Ka võivad järelevalveasutused akrediteerida sertifitseerimisasutuse, kavandada sertifitseerimiskriteeriumid ja väljastada sertifikaate, kui see on nende liikmesriigi õigusega ette nähtud[10].

10. **Riiklik akrediteerimisasutus** võib akrediteerida kolmandate poolte sertifitseerimisasutusi, kasutades ISO 17065 ja järelevalveasutuste täiendavaid akrediteerimisnõudeid, mis peaksid olema kooskõlas käesolevate suuniste 2. jaoga. Mõnes liikmesriigis võivad akrediteerimist pakkuda nii pädev järelevalveasutus kui ka riiklik akrediteerimisasutus või mõlemad.

11. **Sertifitseerimisskeemi omanik** on organisatsioon, kes on kehtestanud sertifitseerimiskriteeriumid ja metodoloogilised nõuded, mille järgi vastavust hinnatakse. Hindamisi tegev organisatsioon võib olla sama organisatsioon, kes on süsteemi välja töötanud ja kes on selle omanik, kuid võib kehtida ka kord, kus üks organisatsioon on skeemi omanik ja teine (või teised) teeb (teevad) hindamisi sertifitseerimisasutusena.

12. Olenevalt liikmesriigi õigusest võib järelevalveasutuste asemel sertifikaate väljastada eespool nimetatud viisil akrediteeritud **sertifitseerimisasutus**[11]. Ta võib koostada sertifitseerimiskriteeriumid ja olla seega skeemi omanik (vt punkt 11 eespool). Tema asukoht peab olema EMPs, eelkõige selleks, et võimaldada isikuandmete kaitse üldmääruse artikli 58 lõike 2 punktis f sätestatud parandusvolituste tõhusat kasutamist. Sertifitseerimisasutus võib aga tellida alltöövõttu kohalikelt ekspertidelt või väljaspool EMPd asuvatelt asutustelt, kes teevad siis auditeerimistoiminguid tema nimel[12]. Siiski ei või sertifitseerimisasutus tellida sertifikaadi andmise või andmata jätmise otsustamist alltöövõtu korras.

---

[6] Lisateave artikli 49 ja selle üldise koosmõju kohta artikliga 46 on kättesaadav suunistes 2/2018 määruse 2016/679 artiklis 49 sätestatud erandite kohta.
[7] Suunised 2/2018 määruse 2016/679 artiklis 49 sätestatud erandite kohta, lk 5.
[8] Isikuandmete kaitse üldmääruse artikli 42 lõige 8.
[9] Suunised 1/2018 määruse (EL) 2016/679 artiklite 42 ja 43 kohase sertifitseerimise ja sertifitseerimiskriteeriumide kindlaksmääramise kohta, punkt 2.2.
[10] Isikuandmete kaitse üldmääruse artikli 42 lõige 5 ja artikli 43 lõige 1.
[11] Isikuandmete kaitse üldmääruse artikli 42 lõige 5.
[12] Sertifitseerimisasutused peavad hindama oma kohalikke eksperte kooskõlas standardiga ISO 17065 ja järelevalveasutuse kehtestatud täiendavate nõuetega (isikuandmete kaitse üldmääruse artikli 43 lõike 1 punkt b).

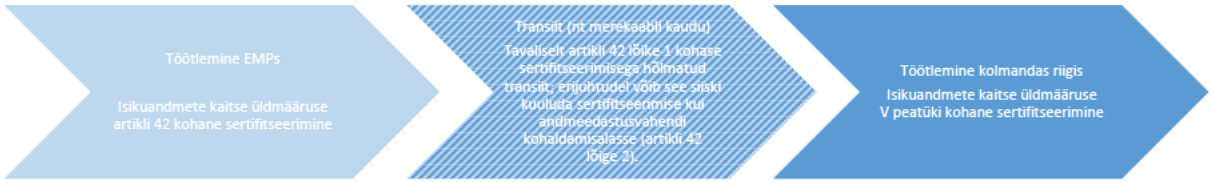
13. **Andmeimportija** on kolmanda riigi üksus (vastutav töötleja või volitatud töötleja), kes saab andmed andmeeksportijalt.

14. **Andmeeksportija** on üksus (vastutav töötleja või volitatud töötleja), kes edastab andmed EMPst andmeimportijale. Andmeeksportija peab tagama vastavuse V peatükile.

1.4 Mis on sertifitseerimise kui andmeedastusvahendi kohaldamisala ja objekt?

15. Sertifitseerimismehhanismi kui artikli 42 lõike 2 kohase andmeedastusvahendi eesmärk on tagada asjakohased kaitsemeetmed isikuandmete töötlemisel artikli 46 lõike 2 punkti f kohaselt. Sertifikaat tõendab asjakohaste kaitsemeetmete olemasolu, mille on taganud vastutavad töötlejad või volitatud töötlejad väljaspool EMPd või EMP vastutavatelt või volitatud töötlejatelt andmeid vastu võttev rahvusvaheline organisatsioon isikuandmete edastamisega kaasnevate spetsiifiliste riskide tõrjumiseks.

16. Üldiselt kujutab isikuandmete edastamine liikmesriigist kolmandasse riiki iseenesest isikuandmete töötlemist isikuandmete kaitse üldmääruse artikli 4 punkti 2 tähenduses, mis toimub liikmesriigis[13] ja on seetõttu isikuandmete kaitse üldmääruse artikli 4 lõike 1 kohaselt sertifitseeritav. Siiski võib mõnes olukorras, olenevalt kontekstist, olla tegemist andmete transiidiga sertifitseerimise kui andmeedastusvahendi kohaldamisalas. Järelikult peaks sertifitseerimise objekt – mis langeb kokku sertifitseerimisaegse hindamise objektiga[14] – üldjuhul olema EMPst saadud andmete töötlemine, mida teeb andmeimportija kolmandas riigis, ja andmete transiit, kui see toimub andmeimportija kontrolli all.



17. Sertifitseerimise objekt võib olla üks töötlemistoiming või -toimingute kogum. Need võivad sisaldada korralduslikes meetmetes väljenduvaid juhtimisprotsesse, mis moodustavad töötlemistoimingu lahutamatu osa[15].

18. Seetõttu oleks taotlev üksus seoses oma sertifitseerimise objektiga andmeimportija kolmandas riigis.

1.5 Milline peaks olema eksportija roll sertifitseerimise kui andmeedastusvahendi kasutamisel?

19. Andmeeksportija poolne andmete edastamine kuulub iseenesest üldiselt otse isikuandmete kaitse üldmääruse alla. See tähendab, et eksportija on kohustatud täitma oma kohustusi, mis tulenevad isikuandmete kaitse üldmäärusest, ja eelkõige tagama andmete turvalise edastamise kooskõlas artikliga 32 ja V peatükiga, kindlustamaks, et määrusega tagatud füüsiliste isikute kaitse taset ei kahjustata

---

[13] Kohtuotsus, Euroopa Liidu Kohus, C-311/18, Data Protection Commissioner *versus* Facebook Ireland Limited ja Maximillian Schrems, punkt 83.

[14] Suunised 1/2018 määruse (EL) 2016/679 artiklite 42 ja 43 kohase sertifitseerimise ja sertifitseerimiskriteeriumide kindlaksmääramise kohta, lk 17.

[15] Suunised 1/2018 määruse (EL) 2016/679 artiklite 42 ja 43 kohase sertifitseerimise ja sertifitseerimiskriteeriumide kindlaksmääramise kohta, lk 16 (nt kaebuste käsitlemise mehhanism).

(isikuandmete kaitse üldmääruse artikkel 44)[16]. Mõistagi saab seda sertifitseerida artikli 42 lõike 1 alusel.

20. Peale selle on andmeeksportija, kes soovib kasutada sertifikaati asjakohase kaitsemeetmena vastavalt isikuandmete kaitse üldmääruse artikli 46 lõike 2 punktile f, eelkõige kohustatud kontrollima, kas sertifikaat, millele ta kavatseb tugineda, on kavandatava töötlemise omaduste seisukohalt tõhus. Selleks peab andmeeksportija väljastatud sertifikaati kontrollima, et uurida, kas sertifikaat on kehtiv ega ole aegunud, kas see hõlmab konkreetset edastamist ja kas isikuandmete transiit kuulub sertifitseerimise kohaldamisalasse, samuti seda, kas tegemist on andmete edasisaatmisega ja kas selle kohta on esitatud piisav dokumentatsioon. Lisaks peab andmeeksportija kontrollima, et riiklik akrediteerimisasutus või pädev järelevalveasutus on sertifikaadi väljastanud sertifitseerimisasutuse akrediteerinud. Lisaks peaks andmeeksportija viitama sertifikaadi kasutamisele andmeedastusvahendina vastavalt isikuandmete kaitse üldmääruse artiklile 28, kui vastutav töötleja edastab andmeid volitatud töötlejale, või andmeimportijaga sõlmitud andmete jagamise lepingule, kui vastutav töötleja edastab andmeid vastutavale töötlejale.

21. Arvestades, et eksportija vastutab kõigi V peatüki sätete kohaldamise eest, peab ta hindama ka seda, kas sertifikaat, millele ta kavatseb tugineda kui andmeedastusvahendile, on kolmandas riigis asjaomase andmeedastuse suhtes asjakohaseid kehtivaid õigusakte ja tavasid silmas pidades tõhus. Selle hindamise jaoks ja olulise elemendina, millega tõendada oma kohustuste täitmist, võib andmeeksportija tugineda sertifitseerimisasutuse kontrollile, mille puhul sertifitseerimisasutus on kontrollinud importija dokumenteeritud hinnangut kolmanda riigi õigusaktide ja tavade kohta.

22. Kui andmeimportija hinnangul on selgunud, et tal ja/või andmeeksportijal võib olla vaja võtta sertifikaadiga ette nähtud lisameetmeid, et tagada EMPs tagatuga sisuliselt samaväärne kaitsetase, peab andmeeksportija kontrollima sertifikaadi saanud andmeimportija ettenähtud lisameetmeid ja seda, kas ta suudab võtta andmeimportija nõutud tehnilisi ja lisameetmeid (kui neid on).

23. Kui neid nõudeid ei täideta, peab andmeeksportija nõudma importijalt kohandatud lisameetmete võtmist või need ise kehtestama.

1.6 Milline on sertifitseerimise kui andmete edastamise vahendi puhul kasutatav protsess?

24. Sertifitseerimine on vabatahtlik, kuid kui seda taotletakse, tuleb sertifitseerimine teha läbipaistva protsessi abil, mis põhineb kohustuslikel normidel. Isikuandmete kaitse üldmääruses on erasektori sertifitseerimismehhanismid pälvinud märkimisväärse usalduse kui „reguleeritud iseregulatsioon“. Sellest tulenevalt peavad need mehhanismid tagama, et sertifikaadid vastavad sisuliselt isikuandmete kaitse üldmääruse artiklis 46 määratletud asjakohaste kaitsemeetmete nõuetele.

[16] Sellega seoses on oluline märkida, et isikuandmete kaitse üldmääruse artikkel 44 näeb selgelt ette, et andmeid ei pruugi edastada mitte ainult vastutav töötleja, vaid ka volitatud töötleja. Seetõttu tekib andmete edastamise puhul olukord, kus volitatud töötleja saadab andmed teisele volitatud töötlejale või isegi kolmandas riigis asuvale vastutavale töötlejale vastutava töötleja juhiste alusel (isikuandmete kaitse üldmääruse artikli 28 lõike 3 punkt a). Sellistel juhtudel tegutseb volitatud töötleja andmete eksportijana vastutava töötleja nimel ja peab tagama V peatüki sätete järgimise asjaomase edastamise puhul vastutava töötleja juhiste alusel, sealhulgas selle, et kasutatakse asjakohast edastusvahendit. Arvestades, et andmete edastamine on vastutava töötleja nimel tehtav töötlemistoiming, vastutab vastutav töötleja ning teda võib pidada vastutavaks ka V peatüki kohaselt, samuti peab ta tagama, et volitatud töötleja annab artikli 28 alusel piisavad tagatised.

25. Seetõttu peab sertifitseerimine põhinema sertifitseerimiskriteeriumide hindamisel kohustusliku auditimetoodika alusel. Need kriteeriumid kiidavad heaks riiklikud järelevalveasutused või Euroopa Andmekaitsenõukogu, nagu on kirjeldatud isikuandmete kaitse üldmääruse artikli 42 lõikes 5. Sertifitseerimiskriteeriumid peavad sisaldama nõudeid andmeimportija poolse töötlemise, sealhulgas andmete edasisaatmise ja kolmanda riigi asjakohase õigusraamistiku hindamiseks, et vältida olukorda, kus kolmanda riigi normid ja tavad takistavad andmeimportijal sertifikaadist tulenevate kohustuste täitmist.

26. Sertifitseerimisprotsessi kestel kontrollib riikliku akrediteerimisasutuse või pädeva järelevalveasutuse akrediteeritud sertifitseerimisasutus hindamise objekti sertifitseerimiskriteeriumide alusel[17].

27. Isikuandmete kaitse üldmääruse artikli 43 lõike 1 kohaselt väljastab sertifikaadi ja pikendab seda sertifitseerimisasutus, kellel on andmekaitse valdkonnas asjakohased eksperditeadmised, olles enne teavitanud järelevalveasutust, et see saaks vajaduse korral kasutada oma volitusi vastavalt artikli 58 lõike 2 punktile h.

28. Vastavalt isikuandmete kaitse üldmääruse artikli 43 lõikele 5 esitab sertifitseerimisasutus pädevale järelevalveasutusele taotletud sertifikaadi väljastamise või sertifikaadi tagasivõtmise põhjused. See ei tähenda, et sertifitseerimisasutus vajab sertifikaadi väljastamiseks järelevalveasutuse luba. Sertifitseerimisasutus hakkab jälgima, kas tema kliendid täidavad sertifitseerimiskriteeriume.

29. Järelevalveasutusel on parandusvolitused võtta sertifikaat tagasi või anda sertifitseerimisasutusele korraldus võtta tagasi isikuandmete kaitse üldmääruse artiklite 42 ja 43 alusel väljastatud sertifikaat või anda sertifitseerimisasutusele korraldus jätta sertifikaat väljastamata, kui sertifitseerimise nõuded ei ole enam täidetud.

30. Euroopa andmekaitsepitser rahvusvaheliseks andmeedastuseks võib olla vahend, mis hõlmab andmete edastamist kolmandatesse riikidesse, kui seda kasutatakse koos siduvate ja täitmisele pööratavate kohustustega[18].

31. Siiski saab andmeedastusvahendina kasutatavaid sertifikaate väljastada ka vastavalt EMP riikide heakskiidetud riiklikele sertifitseerimiskavadele. Sellisena kehtivad need ainult juhul, kui EMP liikmesriikide andmeeksportijad edastavad andmeid kolmandatesse riikidesse, kus sertifitseerimiskava on heaks kiidetud, sest EMP eri riikide sertifikaate vastastikku ei tunnustata. EMP eri riikides asuvad järelevalveasutused võivad aga andmete edastamiseks heaks kiita sama sertifitseerimismehhanismi[19].

---

[17] Suunised 4/2018 isikuandmete kaitse üldmääruse (2016/679) artikli 43 kohase sertifitseerimisasutuste akrediteerimise kohta, lk 9.

[18] Vt isikuandmete kaitse üldmääruse artikli 42 lõige 5 ning andmekaitsenõukogu suuniste 1/2018 (määruse (EL) 2016/679 artiklite 42 ja 43 kohase sertifitseerimise ja sertifitseerimiskriteeriumide kindlaksmääramise kohta) punkt 35.

[19] Kui järelevalveasutus juhib oma riigisisese algatusega sertifitseerimiskriteeriumide X vastuvõtmist ja pärast seda, võttes arvesse kava kriteeriume ja kohaldatavaid konkreetseid siseriiklikke norme, soovivad teised riigid võtta vastu samad sertifitseerimiskriteeriumid, võivad nad need vastu võtta, ilma et oleks vaja Euroopa Andmekaitsenõukogu isikuandmete kaitse üldmääruse artikli 64 kohast arvamust, ja tugineda isikuandmete kaitse üldmääruse artikli 64 lõike 3 kohaselt esimesele järelevalveasutusele antud arvamusele (vt selle kohta viide suuniste *addendum*'ile (Guidance – Addendum) (suuniste 1/2018 (määruse artiklite 42 ja 43 kohase sertifitseerimise ja sertifitseerimiskriteeriumide kindlaksmääramise kohta) lisa) punkt 66.

2 AKREDITEERIMISNÕUETE RAKENDAMISE JUHISED

32. Sertifitseerimisasutuse akrediteerimise nõuded seoses sertifitseerimise kui andmeedastusvahendiga on sätestatud standardis ISO 17065 ning suuniseid 4/2018[20] on tõlgendatud V peatüki taustal, nagu allpool selgitatud.

33. Euroopa Andmekaitsenõukogu hinnangul hõlmavad isikuandmete kaitse üldmääruse artikli 64 lõike 1 punkti c kohaselt vastu võetud suuniste 4/2018 ja standardi ISO 17065 alusel koostatud täiendavad akrediteerimisnõuded juba erinõudeid, mis on vajalikud sertifitseerimisasutuse akrediteerimiseks seoses sertifitseerimise kui andmeedastusvahendiga. Andmete edastamise stsenaariumi puhul on vaja mõnda nõuet seoses selgitavate märkuste ja tõlgendustega siiski täpsustada.

34. Mis puudutab vahenditega seotud nõudeid (vt suuniste 4/2018 nõue 6 – 1. lisa), peab sertifitseerimisasutus tagama, et tal on olemas vajalikud vahendid, et kontrollida, kas andmeimportija on vastavalt sertifitseerimiskriteeriumidele nõuetekohaselt ja korrektselt hinnanud selle kolmanda riigi või nende kolmandate riikide õiguslikku olukorda ja tavasid, kus ta on asutatud või tegutseb[21]. Selline hindamine tuleks teha nende töötlemistoimingute suhtes, mis tuleb sertifitseerida hindamise objekti osana, pidades silmas isikuandmete kaitse üldmääruse artiklis 46 sätestatud asjakohaseid kaitsemeetmeid, ning see peaks hõlmama andmeimportija kindlaks tehtud ja vajaduse korral võetud lisameetmeid. See hõlmab nt ka olulisi teadmisi asjakohastest kohalikest õigusaktidest ja tavadest ning piisavat keeleoskust seoses kolmanda riigiga / kolmandate riikidega.

35. Mis puudutab protsessi käsitlevaid nõudeid (vt suuniste 4/2018 1. lisa nõue 7), siis peab sertifitseerimisasutus tagama, et sertifitseerimisprotsessi saab toetada võimalike kohapealsete audititegа, et seda tehakse töötlemise suhtes, mis leiab aset kolmandas riigis / kolmandates riikides, ning et hindamine hõlmab ka kehtiva õiguse ja poliitika praktilist rakendamist kolmandas riigis / kolmandates riikides.

36. Mis puudutab sertifitseerimist mõjutavaid muudatusi käsitlevaid nõudeid (vt suuniste 4/2018 1. lisa nõue 7.10), jälgib sertifitseerimisasutus kolmanda riigi õigusaktide ja/või kohtupraktika muudatusi, mis võivad mõjutada hindamise objekti alla kuuluvat töötlemist.

3 SERTIFITSEERIMISE ERIKRITEERIUMID

37. Sertifitseerimise erikriteeriumide kaalumise kontekstis põhinevad käesolevad suunised suunistel 1/2018 määruse (EL) 2016/679 artiklite 42 ja 43 kohase sertifitseerimise ja sertifitseerimiskriteeriumide kindlaksmääramise kohta (versioon 3.0), vastaval 2. lisal sertifitseerimiskriteeriumide läbivaatamise ja hindamise kohta vastavalt artikli 42 lõikele 5 ja sertifitseerimiskriteeriumide hindamist käsitlevate suuniste *addendum*'ile.

38. Euroopa Andmekaitsenõukogu hinnangul hõlmavad suuniste 1/2018 2. lisa ja sertifitseerimiskriteeriumide hindamist käsitlevate suuniste *addendum*'i alusel koostatud sertifitseerimiskriteeriumid juba enamikku kriteeriume, mida tuleb andmeedastusvahendina kasutatava sertifitseerimise kava koostamisel arvesse võtta. Siiski võib tekkida vajadus mõnda neist olemasolevatest kriteeriumidest täpsustada, et neid konkreetse andmeedastusstsenaariumiga kohandada (vt punkt 3.1). Lisaks võib tekkida

[20] Suunised 4/2018 isikuandmete kaitse üldmääruse artikli 43 kohase sertifitseerimisasutuste akrediteerimise kohta ja nende lisa.
[21] Vt eespool punkt 12.

vajadus sõnastada lisakriteeriumid asjakohaste kaitsemeetmete kohaldamiseks, sealhulgas seoses andmesubjektide õigustega (vt punkt 3.2).

3.1 SERTIFITSEERIMISKRITEERIUMIDE RAKENDAMISE JUHISED

39. Mis puudutab sertifitseerimismehhanismi ja hindamise objekti (vt 2. lisa punkt 2.a), tuleks seda asjakohastes dokumentides selgelt kirjeldada, sealhulgas seoses isikuandmete edastamisega kolmandasse riiki, või seda, kas need hõlmavad ka isikuandmete transiiti.

40. Mis puudutab sertifitseerimismehhanismi ja hindamise objekti kohaldamisala (vt 2. lisa, punkt 2.b) tuleks asjakohastes dokumentides konkreetselt kirjeldada, mis liiki üksuse (nt vastutav töötleja ja/või volitatud töötleja) suhtes sertifitseerimismehhanismi kohaldatakse.

41. Mis puudutab sertifitseerimismehhanismi ja hindamise objekti kohaldamisala (vt 2. lisa, punkt 2.f), peaksid kriteeriumid nõudma, et vääritimõistmise vältimiseks oleks hindamise objekt määratletud konkreetselt. See peaks hõlmama vähemalt järgmist:

42. töötlemistoimingud, sealhulgas juhul, kui nähakse ette andmete edasisaatmist:

    a) eesmärk;

    b) üksuse liik (nt vastutav töötleja ja/või volitatud töötleja);

    c) edastatavate andmete liik, võttes arvesse seda, kas tegemist on isikuandmete kaitse üldmääruse artiklis 9 määratletud isikuandmete erikategooriatega;

    d) andmesubjektide kategooriad;

    e) riigid, kus andmete töötlemine toimub.

43. Mis puudutab läbipaistvust ja andmesubjektide õigusi (vt 2. lisa, punkt 8), tuleks sertifitseerimiskriteeriumides

    a) nõuda, et andmesubjektidele antaks teavet töötlemistoimingute kohta, sealhulgas vajaduse korral isikuandmete edastamise kohta kolmandale riigile või rahvusvahelisele organisatsioonile (vt isikuandmete kaitse üldmääruse artiklid 12, 13 ja 14);

    b) nõuda, et andmesubjektidele tagataks õigus tutvuda andmetega, õigus taotleda andmete parandamist, kustutamist või töötlemise piiramist, kohustus teatada isikuandmete parandamisest, kustutamisest või isikuandmete töötlemise piiramisest, õigus esitada vastuväiteid töötlemise suhtes, andmesubjekti õigus sellele, et tema kohta ei võetaks vastu otsust, mis põhineb üksnes automatiseeritud töötlusel, sealhulgas profiilianalüüsil, mis on sisuliselt samaväärsed isikuandmete kaitse üldmääruse artiklite 15–19, 21 ja 22 kohaselt antud õigustega;

    c) nõuda, et sertifikaadi saanud andmeimportija kehtestaks asjakohase kaebuste käsitlemise korra, et tagada andmesubjekti õiguste tõhus rakendamine;

    d) nõuda selle hindamist, kas ja mil määral on need õigused andmesubjektide jaoks asjaomases kolmandas riigis täitmisele pööratavad, ning kõiki asjakohaseid lisameetmeid, mida võib olla vaja nende täitmisele pööramiseks võtta, nt nõuda, et andmeimportija nõustuks alluma andmeeksportija(te) suhtes pädeva järelevalveasutuse jurisdiktsioonile ja sellega koostööd tegema kõigis menetlustes, mille eesmärk on tagada nende õiguste järgimine, ning eelkõige, et ta nõustuks vastama järelepärimistele, alluma auditeerimisele ja järgima eespool nimetatud järelevalveasutuse võetud meetmeid, sealhulgas parandus- ja kompenseerivaid meetmeid.

44. Mis puudutab kaitset tagavaid tehnilisi ja korralduslikke meetmeid (2. lisa punkt 10.q), tuleks sertifitseerimiskriteeriumides nõuda, et andmeimportija teavitaks eksportijat, ja kui importija tegutseb vastutava töötlejana, teavitaks kooskõlas isikuandmete kaitse üldmääruse artikli 34 nõuetega andmeeksportija(te) suhtes pädevat EMP järelevalveasutust andmetega seotud rikkumistest, ning teavitaks nendest andmesubjekte, kui rikkumine võib tõenäoliselt kaasa tuua suure ohu nende õigustele ja vabadustele.

3.2 TÄIENDAVAD SERTIFITSEERIMISE ERIKRITEERIUMID

45. Võttes arvesse isikuandmete kaitse üldmääruse artikli 46 alusel muude edastusvahendite jaoks kindlaks määratud kaitsemeetmeid (nagu siduvad kontsernisisesed eeskirjad või käitumisjuhendid) ja selleks, et tagada ühtne kaitsetase, ning võttes arvesse Euroopa Kohtu otsust kohtuasjas Schrems II, on Euroopa Andmekaitsenõukogu seisukohal, et sertifitseerimismehhanism, mida kasutatakse andmete kolmandatesse riikidesse edastamise vahendina, peaks hõlmama ka allpool loetletud kriteeriume.

1. Kolmanda riigi õigusaktide hindamine

a) Kas kriteeriumid nõuavad, et andmeimportija oleks hinnanud selle kolmanda riigi norme ja tavasid, kus ta tegutseb, ja seda, kas need takistavad importijal sertifitseerimisest tulenevaid kohustusi täita?
b) Kas kriteeriumid nõuavad, et andmeimportija dokumenteeriks selle kolmanda riigi normide ja tavade hinnangu, kus ta tegutseb, ning hoiaks dokumendid sertifitseerimisasutuse ja taotluse korral andmeeksportija suhtes pädeva EMP järelevalveasutuse ning andmeeksportija jaoks kättesaadavana?
c) Kas kriteeriumid nõuavad, et andmeimportija oleks määratlenud ja rakendanud korralduslikud ja tehnilised meetmed, et tagada isikuandmete kaitse üldmääruse artikli 46 kohased kaitsemeetmed, võttes arvesse soovitusi 01/2020 edastusvahendeid täiendavate meetmete kohta, et tagada vastavus isikuandmete kaitse ELi tasemega?
d) Kas kriteeriumid nõuavad, et andmeimportija dokumenteeriks tegelikult rakendatud korralduslikud ja tehnilised meetmed, et tagada isikuandmete kaitse üldmääruse artikli 46 kohased asjakohased kaitsemeetmed, ning hoida dokumendid sertifitseerimisasutuse ning taotluse korral pädevate andmekaitseasutuste ja andmeeksportija jaoks kättesaadavana?
e) Kas kriteeriumid nõuavad, et andmeimportija oleks määratlenud ja rakendanud korralduslikud ja tehnilised meetmed, et tagada edastatavate isikuandmete turvalisus, võttes arvesse soovitusi 01/2020 edastusvahendeid täiendavate meetmete kohta, et tagada vastavus isikuandmete kaitse ELi tasemega, kui transiit kuulub sertifitseerimise kui andmeedastusvahendi kohaldamisalasse?
f) Kas kriteeriumid nõuavad sertifitseerimisasutusele ja andmeeksportijale tagatise andmist selle kohta, et andmeimportijal ei ole põhjust arvata, et tema suhtes kohaldatavad õigusaktid ja tavad võivad takistada tal sertifitseerimisest tulenevate kohustuste täitmist?

2. Andmete eksportijate ja importijate üldised kohustused

a) Kas kriteeriumid nõuavad andmeeksportijate ja -importijate vahelistes kokkulepetes (nt olemasolevas teenuslepingus) selle konkreetse andmeedastuse kirjeldamist, mille suhtes sertifitseerimist kohaldatakse, ja seda, et asjaomaste andmesubjektide suhtes tunnustatakse soodustatud kolmanda isiku õigusi?

b) Kui kriteeriumid nõuavad nende lepinguliste kokkulepete või vahendite puhul konkreetset sisu ja selleks on ette nähtud vorm, siis kas nad nõuavad samuti, et ka need oleksid hindamise objektid?

3. Andmete edasisaatmise reeglid

a) Kas kriteeriumid nõuavad, et edasisaatmise suhtes kohaldataks konkreetseid kaitsemeetmeid kooskõlas isikuandmete kaitse üldmääruse V peatüki nõuetega, eesmärgiga kindlustada, et EMPs tagatud kaitsetaset ei kahjustata, ning kas kriteeriumid nõuavad, et asjakohased dokumendid hoitakse sertifitseerimisasutuse ja andmeeksportija(te) suhtes pädeva EMP järelevalveasutuse ja taotluse korral andmeeksportija jaoks kättesaadavana?

4. Heastamine ja täitmise tagamine

a) Kas kriteeriumidega nähakse ette, et andmesubjekt saab kaitsta oma õigusi soodustatud kolmanda isikuna andmeimportija vastu oma EMPs asuva alalise elukoha järgses kohtus või rahvusvahelises organisatsioonis, sealhulgas talle tekitatud kahju hüvitamiseks juhul, kui importija ei vasta asjaomasele sertifitseerimiskavale?
b) Kas kriteeriumid võimaldavad asjakohaselt hinnata, kas andmeimportija vastutab EMPs andmesubjektile tekitatud kahju eest asjaomase sertifitseerimiskavale mittevastavuse korral?
c) Kas kriteeriumid nõuavad, et andmesubjekt saaks esitada andmeimportija vastu kaebuse EMP järelevalveasutusele, eelkõige selles EMP riigis, kus on andmesubjekti alaline elukoht, töökoht või mis on andmeeksportija(te) suhtes pädev?
d) Kas kriteeriumid nõuavad, et andmeimportija teeks koostööd andmeeksportija(te) suhtes pädeva EMP järelevalveasutusega ning nõustuks tema (nende) auditite ja kontrollidega, võtaks arvesse tema (nende) nõuandeid ja täidaks tema (nende) otsuseid?

5. Protsess ja meetmed olukordade puhuks, kus siseriiklikud õigusaktid takistavad sertifitseerimise raames võetud kohustuste täitmist

a) Kas kriteeriumidega nähakse ette, et kui kolmandas riigis asuval andmeimportijal või rahvusvahelisel organisatsioonil on põhjust arvata, et muudatused tema suhtes kohaldatavates õigusaktides ja tavades võivad takistada tal täitmast sertifitseerimisest tulenevaid kohustusi, teavitab ta sellest viivitamatult sertifitseerimisasutust ja andmeeksportijat, et viimane saaks hinnata, kas andmete edastamine tuleb kohe peatada?
b) Kas kriteeriumide kohaselt on nõutav nende sammude kirjeldus (sealhulgas EMPs asuva andmeeksportija teavitamine ja asjakohaste lisameetmete võtmine), mis astutakse, kui andmeimportija saab teada kolmanda riigi õigusaktidest või tavadest, mis takistavad sertifitseerimisest tulenevate kohustuste täitmist, samuti nende meetmete kirjeldus, mis tuleb võtta, kui kolmanda riigi ametiasutused esitavad teabenõudeid (sealhulgas kohustus kontrollida teabenõude seaduslikkust ja see vajaduse korral vaidlustada ning minimeerida avaldatavat teavet)?

6. Kolmandate riikide ametiasutuste andmetele juurdepääsu taotluste käsitlemine

a) Kas kriteeriumidega nähakse ette, et andmeimportija teavitaks viivitamata andmeeksportijat, kui kolmanda riigi ametiasutused taotlevad juurdepääsu andmetele, ja võtaks asjakohaseid lisameetmeid?

b) Kas kriteeriumidega nähakse ette, et kolmandate riikide ametiasutuste ebaproportsionaalsetest juurdepääsutaotlustest, eelkõige taotlustest, mis nõuavad isikuandmete massilist ja valimatut edastamist, tulenevaid andmeedastusi ei tohiks teha?

7. Andmeeksportijaga seotud lisakaitsemeetmed

46. Kas kriteeriumidega nähakse ette, et andmeimportija peaks tagama ettenähtud juhtudel, ka andmeeksportija suhtes siduvate nõuete kaudu, et tema kindlaksmääratud lisameetmed on vastavuses andmeeksportija vastavate lisameetmetega, võttes arvesse Euroopa Andmekaitsenõukogu soovitusi 01/2020 ja kasutusjuhtumite näiteid, et tagada andmeimportija lisameetmete tõhus rakendamine?

4 SIDUVAD JA TÄITMISELE PÖÖRATAVAD KOHUSTUSED, MIS TULEB RAKENDADA

47. Isikuandmete kaitse üldmääruse artikli 42 lõikega 2 on ette nähtud, et andmete edastamiseks mõeldud sertifitseerimismehhanismi järgivad vastutavad töötlejad ja volitatud töötlejad, kelle suhtes isikuandmete kaitse määrust ei kohaldata, peavad võtma lepingu või muu õiguslikult siduva dokumendi[22] alusel täiendavad siduvad ja täitmisele pööratavad kohustused sertifitseerimismehhanismis ette nähtud asjakohaste kaitsemeetmete, sealhulgas õigustega seotud kaitsemeetmete kohaldamiseks.

48. Nagu on sätestatud isikuandmete kaitse üldmääruses, võib selliste kohustuste võtmiseks kasutada lepingut, mis tundub olevat kõige lihtsam lahendus. Kasutada võib ka muid dokumente, tingimusel et sertifitseerimismehhanismi järgiv vastutav töötleja / volitatud töötleja suudab tõestada asjaomase dokumendi siduvust ja täitmisele pööratavust.

49. Igal juhul peab siduvus ja täitmisele pööratavus olema tagatud liidu õigusega ning kohustused peaksid olema siduvad ja täitmisele pööratavad ka andmesubjektide kui soodustatud kolmandate isikute jaoks.

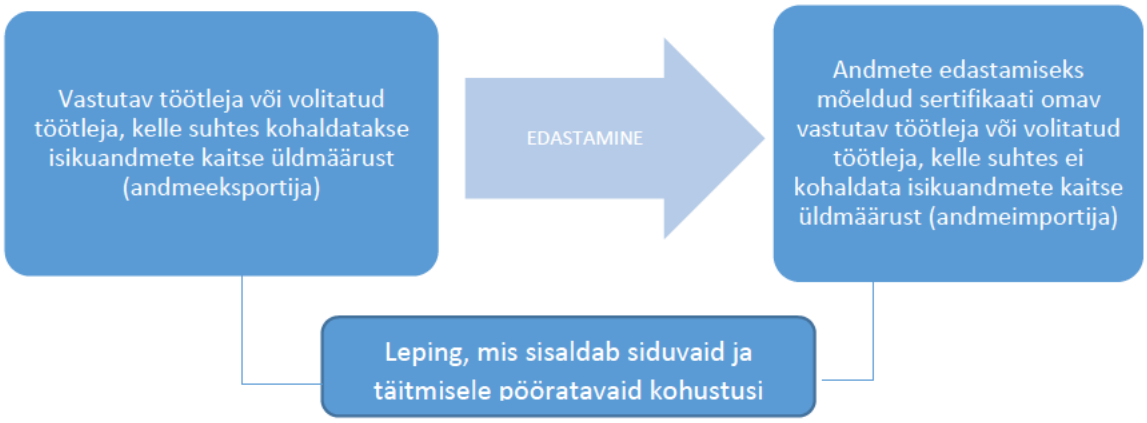
50. Otsene võimalus oleks lisada siduvad ja täitmisele pööratavad kohustused andmeeksportija ja -importija vahelisse lepingusse. Praktikas võiksid pooled kasutada olemasolevat lepingut (nt andmeeksportija ja -importija vaheline teenusleping, vastutavate töötlejate ja volitatud töötlejate vaheline andmetöötlusleping kooskõlas isikuandmete kaitse üldmääruse artikliga 28 või eraldiseisvate vastutavate töötlejate vaheline andmete jagamise leping), millesse võib lisada siduvad ja täitmisele pööratavad kohustused. Need kohustused tuleks kõigist muudest klauslitest selgelt eristada. Teine võimalus on kasutada eraldi lepingut, näiteks andmete edastamiseks mõeldud sertifitseerimismehhanismile võib lisada näidislepingu, millele kolmandas riigis asuvad vastutavad töötlejad / volitatud töötlejad ja kõik andmeeksportijad peavad alla kirjutama.

51. Peaks olema võimalik valida kõige sobivam lahendus sõltuvalt konkreetsest olukorrast.

52. Kui sertifitseerimismehhanismi kasutatakse andmete edastamisel ja andmete edasisaatmisel andmete volitatud töötlejalt alamtöötlejatele, tuleks sertifitseerimismehhanismile ja dokumendile, millega võetakse siduvad ja täitmisele pööratavad kohustused, osutada ka volitatud töötleja ja vastutava töötleja vahelises andmete töötlemise lepingus.

[22] See õiguslikult siduv dokument ei tohi olla muu V peatükis ette nähtud vahend (näiteks lepingu tüüptingimused), sest need artikli 46 lõike 2 punktis f osutatud siduvad ja täitmisele pööratavad kohustused peavad olema kavandatud nii, et tagada andmeimportija sertifitseerimiskriteeriumide täitmine.

Andmeeksportija ja -importija lepingus sisalduvate siduvate ja täitmisele pööratavate kohustuste näide:



53. Üldjuhul peab lepingus või muus õiguslikult siduvas dokumendis olema sätestatud, et andmeimportijana tegutsev sertifitseeritud vastutav töötleja / volitatud töötleja kohustub EMPst saadud asjakohaste andmete töötlemisel järgima edastamiseks mõeldud sertifikaadis sätestatud reegleid ja garanteerib, et tal ei ole põhjust arvata, et kõnealuse töötlemise suhtes kohaldatavad kolmanda riigi õigusaktid ja tavad, sealhulgas isikuandmete avalikustamise nõuded või ametiasutustele andmetele juurdepääsu lubavad meetmed, takistavad tal täitmast sertifitseerimisest tulenevaid kohustusi ning et ta teavitab andmeeksportijat kõigist asjakohastest muudatustest õigusaktides või tavades.

54. Lepingus või muus dokumendis tuleb kindlaks määrata ka mehhanismid, mis võimaldavad pöörata sellised kohustused täitmisele, juhul kui andmeimportijana tegutsev vastutav töötleja / volitatud töötleja ei järgi sertifikaadi reegleid, eelkõige kui ta rikub nende andmesubjektide õigusi, kelle andmeid sertifikaadi alusel edastatakse.

55. Konkreetsemalt tuleks lepingus või muus dokumendis sätestada järgmine.

- Andmesubjektide õigus: andmesubjektidel, kelle andmeid sertifikaadi alusel edastatakse, on õigus pöörata soodustatud kolmanda isikuna sertifitseeritud andmeimportija sertifitseerimise alusel võetud kohustused täitmisele.

- Vastutus väljaspool EMPd sertifikaadi saanud andmeimportija sertifitseerimiseeskirjadele mittevastavuse korral. Kui väljaspool EMPd sertifikaati omav andmeimportija ei täida sertifitseerimise eeskirju, on andmesubjektil võimalik esitada soodustatud kolmanda isiku õigust kasutades asjaomase üksuse vastu hagi, sealhulgas hüvitise saamiseks, EMP järelevalveasutuse ja enda alalises elukohas asuvale EMP kohtule. Väljaspool EMPd sertifikaati omav andmeimportija peab aktsepteerima sellist andmesubjekti otsust. Samuti on andmesubjektil võimalik esitada juhul, kui andmeimportija mittevastavus võib kaasa tuua andmeeksportija vastutuse, järelevalveasutusele, andmeeksportija asukoha kohtule või enda alalise elukoha kohtule hagi andmeeksportija vastu23. Andmeimportija ja andmeeksportija peaksid nõustuma ka sellega, et andmesubjekti võib isikuandmete kaitse üldmääruse artikli 80 lõikes 1 sätestatud tingimustel esindada mittetulunduslik asutus, organisatsioon või ühendus.

[23] See vastutus ei tohiks mõjutada sertifitseerimise puhul ette nähtud sertifitseerimisasutuse võimalusi võtta sertifitseeritud vastutavate töötlejate / volitatud töötlejate suhtes sertifikaadi kohaselt parandusmeetmeid.

- Andmeeksportija õigus nõuda soodustatud kolmanda isikuna sertifikaati omavalt andmeimportijalt sertifikaadis sätestatud eeskirjade täitmist.
- Sertifikaati omava andmeimportija kohustus teavitada andmeeksportijat ja andmeeksportija järelevalveasutust kõigist meetmetest, mida sertifitseerimisasutus on võtnud vastuseks sama andmeimportija puhul avastatud sertifitseerimiseeskirjade rikkumisele.

LISA

A. NÄITED LISAMEETMETEST, MIDA ANDMEIMPORTIJA RAKENDAB, KUI TRANSIIT KUULUB SERTIFITSEERIMISE KOHALDAMISALASSE

1. näide. Andmete talletamine varundamiseks ja muudel eesmärkidel, milleks ei ole vaja juurdepääsu krüptimata andmetele

Tuleb kehtestada krüptimisstandardite ja dekrüptimisvõtme turvalisuse kriteeriumid, eelkõige kolmanda riigi õigusliku olukorraga seotud kriteeriumid. Kui importijat saab sundida dekrüptimisvõtmeid edasi andma, ei saa lisameedet tõhusaks pidada[24].

2. näide. Pseudonüümitud andmete edastamine

Pseudonüümitud andmete puhul kehtestatakse edastatavate andmete tuvastatud või tuvastatavale isikule omistamiseks vajaliku lisateabe kohta turvalisuse kriteeriumid, eelkõige järgmised:

– kolmanda riigi õigusliku olukorra kriteeriumid. Kui andmeimportijat saab sundida lisaandmeid vaatama või neid kasutama, et omistada andmed tuvastatud või tuvastatavale isikule, ei saa meedet tõhusaks pidada[25];

– kolmandate riikide ametiasutustele kättesaadava lisateabe kindlaksmääramise kriteeriumid, mis võivad olla piisavad, et omistada andmed tuvastatud või tuvastatavale isikule.

3. näide. Andmete krüptimine, et kaitsta neid importija kolmanda riigi ametiasutuste juurdepääsu eest eksportija ja tema importija vahelise transiidi ajal

Krüptitud andmete puhul tuleb lisada kõik transiidi turvalisuse kriteeriumid. Kui importijat saab sundida dekrüptimiseks või autentimiseks krüptovõtmeid edasi andma või transiidiks kasutatavat komponenti muutma nii, et selle turvaomadusi kahjustatakse, ei saa lisameedet tõhusaks pidada[26].

4. näide. Kaitstud vastuvõtja

Kaitstud vastuvõtjate puhul tuleb määratleda privileegi piiride kriteeriumid. Andmetöötlus peab jääma seadusest tuleneva kutsesaladuse piiresse. See kehtib ka volitatud (alam)töötleja poolse töötlemise ja edastamise kohta, mille vastuvõtjad peavad samuti olema privilegeeritud[27].

B. NÄITED LISAMEETMETEST, KUI SERTIFITSEERIMINE EI HÕLMA TRANSIITI JA NEED MEETMED PEAB TAGAMA EKSPORTIJA

2. näide. Pseudonüümitud andmete edastamine

[24] 2. lisa, soovitused 01/2020 edastusvahendeid täiendavate meetmete kohta, et tagada vastavus isikuandmete kaitse ELi tasemega, versioon 2.0, 1. näide: andmete talletamine varundamiseks ja muudel eesmärkidel, milleks ei ole vaja juurdepääsu krüptimata andmetele, lk 85; https://https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_et_0.pdf.
[25] Vt eespool, punktid 86–89.
[26] Vt eespool, punktid 90.
[27] Vt eespool, punktid 91.

Esitatakse kriteeriumid kolmandate riikide ametiasutustele kättesaadava lisateabe kohta, mis võib olla piisav andmete omistamiseks tuvastatud või tuvastatavale isikule.

3. näide. Andmete krüptimine, et kaitsta neid importija kolmanda riigi ametiasutuste juurdepääsu eest eksportija ja tema importija vahelise transiidi ajal

Esitatakse kriteeriumid, mis käsitlevad kasutatava avaliku võtme sertifitseerimisasutuse või taristu usaldusväärsust, autentimiseks või dekrüptimiseks kasutatavate krüptovõtmete turvalisust ja võtmehalduse usaldusväärsust ning sellise nõuetekohaselt hooldatud tarkvara kasutamist, millel ei ole teadaolevaid nõrku kohti.

Kui importijat saab sundida avalikustama dekrüptimiseks või autentimiseks sobivaid krüptovõtmeid või muutma transiidiks kasutatavat komponenti, et selle turvaomadusi kahjustada, ei saa meedet tõhusaks pidada[28].

4. näide. Kaitstud vastuvõtja

Kaitstud vastuvõtjate puhul tuleb määratleda privileegi piiride kriteeriumid. Andmetöötlus peab jääma seadusest tuleneva kutsesaladuse piiresse. See kehtib ka volitatud (alam)töötleja poolse töötlemise ja edastamise kohta, mille vastuvõtjad peavad samuti olema privilegeeritud[29].

[28] Vt eespool soovitused, punkt 90.
[29] Vt eespool soovitused, punkt 91.