

# Soovitused



Translations proofread by EDPB Members.  
This language version has not yet been proofread.

## **Soovitused 01/2020 edastusvahendeid täiendavate meetmete kohta, et tagada vastavus isikuandmete kaitse ELi tasemega**

**Vastu võetud 10. novembril 2020**

## Kommenteeritud kokkuvõte

Euroopa Liidu isikuandmete kaitse üldmäärus võeti vastu kahel eesmärgil: soodustada isikuandmete vaba liikumist Euroopa Liidus ning ühtlasi kaitsta üksikisikute põhiõigusi ja vabadusi, eriti õigust isikuandmete kaitsele.

Euroopa Liidu Kohus tuletab meelde oma hiljutises otsuses kohtuasjas C-311/18 (Schrems II), et isikuandmetele Euroopa Majanduspiirkonnas (EMP) antud kaitse peab liikuma andmetega kaasa kõikjale, kuhu need liiguvad. Isikuandmete edastamine kolmandatesse riikidesse ei tohi olla vahend, millega neile EMPs antud kaitset õõnestada või lõdvendada. Kohus rõhutab seda täpsustades, et kolmandate riikide kaitsetase ei pea olema EMPs tagatuga identne, kuid peab sellele vastama sisuliselt. Kohus kinnitab ka lepingu tüüptingimuste kehtivust edastusvahendina, mis võib tagada kolmandatesse riikidesse edastatud andmetele lepingu alusel sisuliselt samaväärse kaitsetaseme.

Lepingu tüüptingimused ega muud isikuandmete kaitse üldmääruse artiklis 46 nimetatud edastusvahendid ei toimi vaakumis. Kohus märgib, et eksportijatena tegutsevad vastutavad töötajad ja volitatud töötajad vastutavad koostöös kolmandasse riiki importijaga vajaduse korral ja juhtumipõhiselt selle kontrollimise eest, kas kolmanda riigi õigus või praktika avaldab mõju isikuandmete kaitse üldmääruse artiklis 46 nimetatud edastusvahendites sisalduvate asjakohaste kaitsemeetmete tõhususele. Neil juhtudel jätab kohus eksportijatele endiselt võimaluse võtta nende lünkade täitmiseks täiendavaid meetmeid, et viia kaitse kooskõlla ELi õiguses nõutava tasemega. Kohus ei täpsusta, mis need meetmed võivad olla. Kohus siiski rõhutab, et eksportijad peavad määratlema need igal üksikjuhul eraldi. See on kooskõlas isikuandmete kaitse üldmääruse artikli 5 lõikes 2 sätestatud põhimõttega, mis nõuab, et vastutavad töötajad vastutaksid sama määruse isikuandmete töötlemisega seotud põhimõtete täitmise eest ja on võimelised seda tõendama.

Et abistada eksportijaid (vastutavad töötajad, volitatud töötajad, eraõiguslikud või avalik-õiguslikud isikud, kes töötlevad isikuandmeid isikuandmete kaitse üldmääruse reguleerimisalas) keerulises ülesandes hinnata kolmandaid riike ja tuvastada asjakohased täiendavad meetmed, on Euroopa Andmekaitsekoostöögrupi võtnud vastu käesolevad soovitusel. Soovitustes kirjeldatakse eksportijatele samme, millest lähtuda, ning tutvustatakse võimalikke teabeallikaid ja võimalike täiendavate meetmete näiteid.

**Esimese sammuna** soovitab Euroopa Andmekaitsekoostöögrupp teil eksportijatena **tunda oma edastustoiminguid**. Kõigi isikuandmete kolmandatesse riikidesse edastamise juhtude uurimine võib olla keerukas ülesanne. Isikuandmete sihtkoha teadmist on siiski vaja selle tagamiseks, et need oleksid mis tahes töötlemiskohas kaitstud sisuliselt samaväärsel tasemel. Peate samuti kontrollima, et teie edastatavad andmed oleksid piisavad, asjakohased ja piirduksid sellega, mida on nende kolmandasse riiki edastamise ja seal töötlemiseks vaja.

**Teine samm on kontrollida edastusvahendit, mida edastamiseks kasutate**, arvestades isikuandmete kaitse üldmääruse V peatükis loetletud vahendeid. Kui Euroopa Komisjon on juba tunnistanud riigi, piirkonna või sektori, millesse andmeid edastate, oma isikuandmete kaitse üldmääruse artikli 45 alusel tehtud kaitse piisavuse otsustega või varasema direktiivi 95/46/EÜ alusel tehtud kaitse piisavuse otsusega piisavaks, kui otsus on veel jõus, ei pea te astuma täiendavaid samme, v.a jälgima, et otsus on jõus. Kui kaitse piisavuse otsus puudub, peate kasutama regulaarsete ja korduvate edastustoimingute korral üht isikuandmete kaitse üldmääruse artiklis 46 loetletud edastusvahendit. Ainult mõnel episoodiliste ja mittekorduvate edastustoimingute juhul võib olla võimalik kasutada üht isikuandmete kaitse üldmääruse artiklis 49 sätestatud erandit, kui vastate tingimustele.

**Kolmanda sammuna** tuleb hinnata, kas kolmanda riigi õigusel või praktikas on midagi, mis võiks mõjutada teie kasutatavate edastusvahendite asjakohaste kaitsemeetmete tõhusust teie konkreetse edastustoimingu kontekstis. Keskenduge hinnangus eelkõige kolmanda riigi õigusaktidele, mis on olulised teie edastustoimingu ja kasutatava isikuandmete kaitse üldmääruse artikli 46 kohase edastusvahendi seisukohast ning võivad ohustada selle kaitsetaset. Et hinnata elemente, mida arvestada, kui hindate kolmanda riigi õigusakte, mis käsitlevad avaliku sektori asutuste juurdepääsu andmetele jälitustegevuse eesmärgil, tutvuge Euroopa Andmekaitseõukogu Euroopa oluliste tagatiste soovitustega. Eelkõige tuleb seda hoolikalt kaalutleda, kui avaliku sektori asutuste juurdepääsu andmetele reguleerivad õigusaktid on mitmeti mõistetavad või ei ole avalikult kättesaadavad. Kui puuduvad õigusaktid, mis asjaoludel võivad avaliku sektori asutused saada juurdepääsu isikuandmetele, ning soovite andmeid siiski edastada, uurige muid asjakohaseid ja objektiivseid tegureid, tuginemata subjektiivsetele teguritele, näiteks tõenäosusele, et avaliku sektori asutused kasutavad teie andmeid viisil, mis ei ole kooskõlas ELi standarditega. See hindamine tuleb teha vajaliku hoolikusega ja põhjalikult dokumenteerida, sest vastutate selle põhjal tehtava võimaliku otsuse eest.

**Neljas samm** on tuvastada ja võtta täiendavad meetmed, mida on vaja, et viia edastatud andmete kaitsetase ELi sisulise samaväärsuse standardi tasemele. Seda sammu on vaja ainult siis, kui teie hindamisel selgub, et kolmanda riigi õigusaktid kahjustavad isikuandmete kaitse üldmääruse artikli 46 kohase edastusvahendi tõhusust, mida kasutate või kavatsete kasutada oma edastustoimingu kontekstis. Siin soovitustes (2. lisa) on täiendavate meetmete näidete mitteammendav loetelu koos mõningate tingimustega, mis peavad olema täidetud nende tõhususe jaoks. Nagu artikli 46 kohastes edastusvahendites sisalduvate asjakohaste tagatiste korral, võib ka mõni täiendav meede olla tõhus teatud riikides, kuid mitte teistes. Teie ülesanne on hinnata nende tõhusust konkreetse edastamise kontekstis ning arvestades kolmanda riigi õigust ja kasutatavat edastusvahendit. Tehtava otsuse eest vastutate teie. Selleks võib teil olla vaja ka mitme täiendava meetme kombineerimist. Võite kokkuvõttes leida, et ükski täiendav meede ei saa tagada teie konkreetse edastustoimingu korral sisuliselt samaväärset kaitsetaset. Kui ükski täiendav meede ei sobi, peate edastamist vältima või selle peatama või lõpetama, et takistada isikuandmete kaitsetaseme rikkumist. Ka see täiendavate meetmete hindamine peab toimuma vajaliku hoolikusega ja see tuleb dokumenteerida.

**Viies samm** on läbida kõik ametlikud menetluse etapid, mida on teie täiendava meetme korral vaja, olenevalt kasutatavast isikuandmete kaitse üldmääruse artikli 46 kohasest edastusvahendist. Siin soovitustes täpsustatakse neid ametlikke nõudeid. Mõni võib vajada konsulteerimist pädevate järelevalveasutustega.

**Kuuenda ja viimase sammuna** tuleb teil sobivate ajavahemike järel taashinnata kolmandatesse riikidesse edastatavate andmete kaitsetaset ning jälgida, kas on toimunud või tulemas arenguid, mis võivad seda mõjutada. Vastutuse põhimõtte nõuab isikuandmete kaitsetaseme pidevat jälgimist.

Järelevalveasutused täidavad pidevalt oma volitusi isikuandmete kaitse üldmääruse kohaldamise järelevalvel ja jõustamisel. Järelevalveasutused arvestavad asjakohaselt meetmeid, millega eksportijad tagavad enda edastatavatele andmetele sisuliselt samaväärse kaitsetaseme. Nagu on Euroopa Kohus öelnud, peavad järelevalveasutused peatama või keelama andmete edastamise juhtudel, kui nad leiavad pärast uurimist või kaebust, et sisuliselt samaväärset kaitsetaset ei ole võimalik tagada.

Järelevalveasutused jätkavad eksportijate suuniste koostamist ning oma tegevuste koordineerimist Euroopa Andmekaitseõukogus, et tagada ELi andmekaitseõigusaktide järjekindel kohaldamine.

## Sisukord

1	Vastutus andmeedastusel .....	7
2	Tegevuskava: vastutuse põhimõtte kohaldamine andmeedastusele praktikas .....	8
2.1	1. samm. Tundke oma edastustoiminguid .....	8
2.2	2. samm. Tuvastage, mis edastusvahendeid kasutate .....	9
2.3	3. samm. Hinnake, kas teie kasutatav isikuandmete kaitse üldmääruse artikli 46 kohane edastusvahend on kõiki edastamise asjaolusid arvestades tõhus .....	12
2.4	4. samm. Võtke vastu täiendavad meetmed.....	15
2.5	5. samm. Menetluslikud sammud, kui olete tuvastanud tõhusad täiendavad meetmed ....	17
2.6	6. samm. Taashinnake olukorda asjakohaste ajavahemike järel .....	19
3	Kokkuvõte.....	20
1.	LISA. MÕISTED.....	21
2.	LISA. TÄIENDAVATE MEETMETE NÄITED.....	22
	Tehnilised meetmed.....	22
	Täiendavad lepingulised meetmed .....	28
	Korralduslikud meetmed.....	35
3.	LISA. VÕIMALIKUD TEABEALLIKAD kolmanda riigi HINDAMISEKS .....	39

## 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 154/2018,<sup>1</sup>

võttes arvesse töökorra artiklit 12 ja artiklit 22,

ning arvestades järgmist:

(1) Euroopa Liidu Kohus järeltab oma 16. juuli 2020. aasta otsuses kohtuasjas Data Protection Commissioner vs. Facebook Ireland Ltd ja Maximillian Schrems (C-311/18), et isikuandmete kaitse üldmääruse artikli 46 lõiget 1 ja artikli 46 lõike 2 punkti c tuleb tõlgendada nii, et nende sätetega nõutavad asjakohased kaitsemeetmed, kohtulikult kaitstavad õigused ja tõhusad õiguskaitsevahendid peavad andmesubjektidele, kelle isikuandmeid edastatakse kolmandasse riiki andmekaitse tüüptingimuste alusel, tagama õiguste kaitse, mille tase on sisuliselt samaväärne sellega, mis on Euroopa Liidus tagatud vastavalt kõnealusele määrusele, tõlgendatuna lähtuvalt Euroopa Liidu põhiõiguste hartast.<sup>2</sup>

(2) Nagu kohus on rõhutanud, tuleb Euroopa Liidus isikuandmete kaitse üldmäärusega tagatuga sisuliselt samaväärne füüsiliste isikute kaitsetase, tõlgendatuna harta alusel, tagada olenemata sellest, mis V peatüki sätte alusel isikuandmeid kolmandasse riiki edastatakse. V peatüki sätete eesmärk on tagada see kõrge kaitsetaseme pidevus isikuandmete kolmandasse riiki edastamisel.<sup>3</sup>

(3) Isikuandmete kaitse üldmääruse põhjenduses 108 ja artikli 46 lõikes 1 sätestatakse, et ELi kaitse piisavuse otsuse puudumise korral peaks vastutav või volitatud töötaja võtma meetmed, et korvata kolmanda riigi andmekaitse puudulik tase asjakohaste andmesubjekti kaitsmise meetmetega. Vastutav või volitatud töötaja võib tagada asjakohased kaitsemeetmed, ilma et selleks oleks vaja konkreetset järelevalveasutuse volitust, kasutades isikuandmete kaitse üldmääruse artikli 46 lõikes 2 loetletud edastusvahendit, näiteks andmekaitse tüüptingimusi.

(4) Kohus selgitab, et komisjoni poolt vastu võetud andmekaitse tüüptingimuste eesmärk on üksnes teha liidus asuvatele vastutavatele töötlejatele või nende volitatud töötlejatele kättesaadavaks lepingulised kaitsemeetmed, mis on kõigis kolmandates riikides ühtviisi kohaldatavad. Lepingulise olemuse tõttu ei saa andmekaitse tüüptingimused olla siduvad kolmandate riikide avaliku sektori

<sup>1</sup> Kõiki käesoleva dokumendi viiteid liikmesriikidele tuleb mõista kui viiteid EMP liikmesriikidele.

<sup>2</sup> Euroopa Liidu Kohtu 16. juuli 2020. aasta otsus kohtuasjas Data Protection Commissioner vs. Facebook Ireland Ltd ja Maximillian Schrems (C-311/18 (Schrems II)), teine järelalus.

<sup>3</sup> C-311/18 (Schrems II), punktid 92 ja 93.

asutustele, sest nad ei ole lepingu pooled. Seetõttu võib andmeeksportijatel olla vaja lisada nendes andmekaitse tüüptingimustes sisalduvatele tagatistele täiendavaid meetmeid, et tagada konkreetses kolmandas riigis vastavus ELi õigusega nõutavale kaitsetasemele. Kohus viitab isikuandmete kaitse üldmääruse põhjendusele 109, milles seda võimalust nimetatakse ning ergutatakse vastutavaid töötajaid ja volitatud töötajaid seda kasutama.<sup>4</sup>

(5) Kohus märkis, et eelkõige on andmeeksportija ülesanne kontrollida igal üksikjuhul eraldi ja vajaduse korral koostöös andmeimportijaga, kas liidu õiguse seisukohalt tagab sihtkohaks oleva kolmanda riigi õigus andmekaitse tüüptingimuste alusel edastatud isikuandmete sisuliselt samaväärse kaitsetaseme, ja vajaduse korral näha lisaks andmekaitse tüüptingimustes ettenähtule ette täiendavad kaitsemeetmed.<sup>5</sup>

(6) Kui Euroopa Liidus asuval vastutaval töötajal või tema volitatud töötajal ei ole võimalik võtta ELi õigusega nõutavaga sisuliselt samaväärse kaitsetaseme tagamiseks piisavaid täiendavaid meetmeid, peab ta või tema asemel pädev järelevalveasutus isikuandmete kolmandasse riiki edastamise peatama või lõpetama.<sup>6</sup>

(7) Isikuandmete kaitse üldmääruse ega kohus ei määratle ega täpsusta, mis on „täiendavad tagatised“, „lisameetmed“ või „täiendavad meetmed“ peale isikuandmete kaitse üldmääruse artikli 46 lõikes 2 loetletud edastusvahendite kaitsemeetmete, mida vastutavad töötajad ja volitatud töötajad võivad võtta, et tagada konkreetses kolmandas riigis kooskõla ELi õigusega nõutava kaitsetasemega.

(8) Euroopa Andmekaitseõukogu on otsustanud küsimust omal algatusel uurida ning anda eksportijatena tegutsevatele vastutavatele töötajatele ja volitatud töötajatele soovitusi täiendavate meetmete tuvastamise ja vastuvõtmise võimaliku protsessi kohta. Soovituste eesmärk on koostada eksportijate jaoks meetodika, mille alusel tuvastada, kas ja mis lisameetmeid on vaja nende edastustoimingute korral võtta. Eksportijate esmane ülesanne on tagada, et edastatavad andmed oleksid kolmandas riigis kaitstud ELis tagatuga sisuliselt samaväärsel tasemel. Käesolevate soovitude andmisega on Euroopa Andmekaitseõukogu eesmärk ergutada isikuandmete kaitse üldmääruse järjepidevat kohaldamist,<sup>7</sup>

## **ON VASTU VÕTNUD KÄESOLEVA ARVAMUSE:**

---

<sup>4</sup> C-311/18 (Schrems II), punktid 132 ja 133.

<sup>5</sup> C-311/18 (Schrems II), punkt 134.

<sup>6</sup> C-311/18 (Schrems II), punkt 135.

<sup>7</sup> Isikuandmete kaitse üldmääruse artikli 70 lõike 1 punkt e.

# 1 VASTUTUS ANDMEEDASTUSEL

1. ELi esmased õigusaktid käsitlevad õigust andmekaitsele põhiõigusena.<sup>8</sup> Vastavalt sellele on õigus andmekaitsele hästi kaitstud ning seda võib piiranguid või sellele seada ainult seadusega, arvestades nimetatud õiguse olemust ning juhul, kui need on proportsionaalsed, vajalikud ja vastavad tegelikult liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või kui on vaja kaitsta teiste isikute õigusi ja vabadusi.<sup>9</sup> Õigus isikuandmete kaitsele ei ole absoluutne õigus, vaid seda tuleb kaalutleda vastavalt selle ülesandele ühiskonnas ning tasakaalustada muude põhiõigustega vastavalt proportsionaalsuse põhimõttele.<sup>10</sup>
2. Andmetega, mis liiguvad kolmandasse riiki väljapoole EMPd, peab kaasnema ELis tagatuga sisuliselt samaväärse kaitsetaseme, et tagada isikuandmete kaitse üldmäärusega tagatud kaitsetaseme mittekahjustamine.
3. Õigus andmekaitsele on olemuselt aktiivne. Selleks on vaja, et eksportijad ja importijad (vastutavad ja/või volitatud töötajad) teeksid enam kui üksnes õiguse tunnustamine või passiivne järgimine.<sup>11</sup> Vastutavad töötajad ja volitatud töötajad peavad püüdma täita õigust andmekaitsele aktiivselt ja pidevalt, rakendades juriidilisi, tehnilisi ja korralduslikke meetmeid, mis tagavad selle tõhususe. Vastutavad töötajad ja volitatud töötajad peavad suutma ka tõendada seda tegevust andmesubjektidele, üldsusele ja andmekaitse järelevalveasutustele. Seda nimetatakse vastutuse põhimõtteks.<sup>12</sup>
4. Vastutuse põhimõtet on vaja isikuandmete kaitse üldmäärusega antava kaitse tõhusa kohaldamise tagamiseks ka andmete edastamisel kolmandatesse riikidesse<sup>13</sup>, sest ka see on andmetöötluse vorm.<sup>14</sup> Nagu rõhutas kohus otsuses, tuleb Euroopa Liidus isikuandmete kaitse üldmäärusega tagatuga sisuliselt samaväärne kaitsetase, tõlgendatuna lähtuvalt hartast, tagada olenemata sellest, mis selle peatüki sätte alusel isikuandmeid kolmandasse riiki edastatakse.<sup>15</sup>
5. Otsuses Schrems II rõhutab kohus eksportijate ja importijate ülesannet tagada, et isikuandmete töötlemine on toimunud ja toimub jätkuvalt kooskõlas ELi andmekaitseõigusega määratud kaitsetasemel, ning peatada andmete edastamine ja/või lõpetada leping, kui andmeimportija ei suuda või enam ei suuda järgida asjaomases eksportija ja importija vahelises lepingus sisalduvaid andmekaitse tüüptingimusi.<sup>16</sup> Eksportijana tegutsev vastutav või volitatud töötaja peab tagama, et importijad teevad vajaduse korral eksportijaga nende ülesannete täitmisel koostööd, hoides teda näiteks kursis importija asukohariigis vastu võetud isikuandmete kaitset mõjutavate arengutega.<sup>17</sup>

---

<sup>8</sup> Põhiõiguste harta artikli 8 lõige 1 ja Euroopa Liidu toimimise lepingu artikli 16 lõige 1, isikuandmete kaitse üldmääruse põhjendus 1, artikli 1 lõige 2.

<sup>9</sup> Euroopa Liidu põhiõiguste harta artikli 52 lõige 1.

<sup>10</sup> Isikuandmete kaitse üldmääruse põhjendus 4 ja otsus kohtuasjas C-507/17: Google LLC, Google Inc. õigusjärglane vs. Commission nationale de l'informatique et des libertés (CNIL), punkt 60.

<sup>11</sup> C-92/09 ja C-93/02, Volker und Markus Schecke GbR vs. Land Hessen, kohtujurist Sharpstoni ettepanek, 17. juuni 2010, punkt 71.

<sup>12</sup> Isikuandmete kaitse üldmääruse artikli 5 lõige 2 ja artikli 28 lõike 3 punkt h.

<sup>13</sup> Isikuandmete kaitse üldmääruse artikkel 44 ja põhjendus 101 ning isikuandmete kaitse üldmääruse artikli 47 lõike 2 punkt d.

<sup>14</sup> Euroopa Liidu Kohtu 6. oktoobri 2015. aasta otsus kohtuasjas Maximilian Schrems vs. Data Protection Commissioner (edaspidi C-362/14 (Schrems I)), punkt 45.

<sup>15</sup> C-311/18 (Schrems II), punktid 92 ja 93.

<sup>16</sup> C-311/18 (Schrems II), punktid 134, 135, 139, 140, 141 ja 142.

<sup>17</sup> C-311/18 (Schrems II), punkt 134.

Need ülesanded tähendavad isikuandmete kaitse üldmääruse vastutuse põhimõtte kohaldamist andmeedastusele.<sup>18</sup>

## 2 TEGEVUSKAVA: VASTUTUSE PÕHIMÕTTE KOHALDAMINE ANDMEEDASTUSELE PRAKTIKAS

6. Järgmiseks kirjeldatakse tegevuskava vajalikest sammudest, millega saate teada, kas peate andmeeksportijana võtma täiendavaid meetmeid, et edastada andmeid seaduslikult väljapoole EMPd. „Teie“ tähendab käesolevas dokumendis andmeeksportijana tegutsevat vastutavat või volitatud andmetöötajat, kes töötleb isikuandmeid isikuandmete kaitse üldmääruse kohaldamisalas. See hõlmab ka eraõiguslike asutuste ja avaliku sektori asutuste tehtavat töötlemist, kui andmeid edastatakse eraõiguslikele asutustele.<sup>19</sup> Seoses isikuandmete edastamisega avaliku sektori asutuste vahel on erisuunised *suunistes 2/2020 määruse 2016/679 artikli 46 lõike 2 punkti a ja artikli 46 lõike 3 punkti b kohta isikuandmete edastamisel EMP ja EMP-väliste riikide avaliku sektori asutuste ja organite vahel*.<sup>20</sup>
7. See hindamine ning valitud ja rakendatavad täiendavad meetmed tuleb sobivalt dokumenteerida ning teha vastavad dokumendid nõudmise korral kättesaadavaks pädevale järelevalveasutusele.<sup>21</sup>

### 2.1 1. samm. Tundke oma edastustoiminguid

8. Et teada, mida võidakse nõuda teilt (andmeeksportijalt), et jätkata või alustada uut isikuandmete edastamist<sup>22</sup>, on esimese sammuna vaja tagada, et olete oma edastustoimingutest täielikult teadlik (tunnete oma edastustoiminguid). Kõigi edastustoimingute registreerimine ja uurimine võib olla keerukas asutustele, kes edastavad kolmandatesse riikidesse regulaarselt palju mitmesuguseid andmeid ning kasutavad mitut volitatud töötajat ja alamtöötajat. Oma edastustoimingute tundmine on hädavajalik esimene samm vastutuse põhimõttest tulenevate kohustuste täitmisel.
9. Oma andmeedastustoimingutest täieliku ülevaate saamiseks võite lähtuda töötlemistoimingute kannetest, mille pidamise kohustus võib teil olla vastutava või volitatud töötlejana isikuandmete kaitse üldmääruse artikli 30 alusel.<sup>23</sup> Samuti võib teil abi olla varasematest tegevustest andmesubjektide

---

<sup>18</sup> Isikuandmete kaitse üldmääruse artikli 5 lõige 2 ja artikli 28 lõike 3 punkt h.

<sup>19</sup> Vt Euroopa Andmekaitseõukogu suunistes 3/2018 isikuandmete kaitse üldmääruse territoriaalse kohaldamisala kohta (artikkel 3) ([https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version\\_et](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_et)).

<sup>20</sup> Euroopa Andmekaitseõukogu suunistes 2/2020 määruse 2016/679 artikli 46 lõike 2 punkti a ja artikli 46 lõike 3 punkti b kohta isikuandmete edastamisel EMP ja EMP-väliste riikide avaliku sektori asutuste ja organite vahel (vt [https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en)).

<sup>21</sup> Isikuandmete kaitse üldmääruse artikli 5 lõige 2 ja artikli 24 lõige 1.

<sup>22</sup> NB! Edastamisena käsitatakse ka kolmandas riigis asuva isiku kaugjuurdepääsu EMPs asuvatele andmetele.

<sup>23</sup> Vt isikuandmete kaitse üldmääruse artikkel 30, eriti selle lõike 1 punkt e ja lõike 2 punkt c. Peale selle peaksid teie töötlemiskanded sisaldama töötlemistegevuste kirjeldust (sealhulgas andmesubjektide kategooriad, isikuandmete kategooriad ning töötlemise eesmärgid ja konkreetne teave andmeedastustoimingute kohta). Mõni vastutav töötaja ja volitatud töötaja on registri pidamise kohustusest vabastatud (isikuandmete kaitse üldmääruse artikli 30 lõige 5). Selle erandi suunistes: vt artikli 29 tööühma seisukohta erandite kohta isikuandmete kaitse üldmääruse artikli 30 lõike 5 kohase töötlemistoimingute registri pidamise kohustusest (Euroopa Andmekaitseõukogus 25. mail 2018 heaks kiidetud).



teavitamise kohustuste täitmisel vastavalt isikuandmete kaitse üldmääruse artikli 13 lõike 1 punktile f ja artikli 14 lõike 1 punktile f seoses nende andmete edastamisega kolmandatesse riikidesse.<sup>24</sup>

10. Ärge unustage edastustoimingute uurimisel arvestada ka edasi saatmist, näiteks seda, kas teie volitatud töötajad väljaspool EMPd saavad teilt neile usaldatud isikuandmeid edasi muus kolmandas riigis või samas kolmandas riigis asuvale alamtöötlejale.<sup>25</sup>
11. Kooskõlas isikuandmete kaitse üldmääruse võimalikult väheste andmete kogumise põhimõttega<sup>26</sup> peate kontrollima, et teie edastatavad andmed oleksid piisavad, asjakohased ja piirduksid sellega, mis on nende kolmandasse riiki edastamise ja seal töötlemise otstarbe seisukohalt vajalik.
12. Need toimingud tuleb teha enne iga andmeedastust ja ajakohastada enne edastamise taastamist andmeedastustoimingute peatamise järel: peate teadma, kus importijad võivad teie eksporditud andmeid hoida või töödelda (sihtkohtade kaart).
13. Pidage meeles, et edastamiseks loetakse ka kaugjuurdepääsu kolmandast riigist (näiteks tugitoimingute ajal) ja/või hoiustamist väljaspool EMPd asuvas pilves.<sup>27</sup> Täpsemalt peate rahvusvahelise pilvetaristu kasutamise korral hindama, kas teie andmeid edastatakse kolmandatesse riikidesse ja kuhu, v.a kui teie pilveteenuse osutaja ütleb oma lepingus selgelt, et andmeid ei edastata kolmandatesse riikidesse üldse.

## 2.2 2. samm. Tuvastage, mis edastusvahendeid kasutate

14. Teise sammuna peate tuvastama, mis edastusvahendeid isikuandmete kaitse üldmääruse V peatükis loetletute ja ette nähtute seast kasutate.

### Kaitse piisavuse otsused

15. Euroopa Komisjon võib kinnitada **kaitse piisavuse otsustega** seoses mõne või kõigi kolmandate riikidega, kuhu isikuandmeid edastate, et neis on isikuandmed piisavalt hästi kaitstud.<sup>28</sup>
16. Selline kaitse piisavuse otsus tähendab, et isikuandmed võivad liikuda EMPst vastavasse kolmandasse riiki, ilma et oleks vaja kasutada ühtki isikuandmete kaitse üldmääruse artikli 46 kohast edastusvahendit.

---

<sup>24</sup> Isikuandmete kaitse üldmääruse läbipaistvuseeskirjade kohaselt peate teavitama andmesubjekte sellest, kui isikuandmeid edastatakse kolmandatesse riikidesse (isikuandmete kaitse üldmääruse artikli 13 lõike 1 punkt f ja artikli 14 lõike 1 punkt f). Eelkõige peate teatama neile Euroopa Komisjoni kaitse piisavuse otsuse olemasolu või puudumise kohta või viitama isikuandmete kaitse üldmääruse artiklis 46 või 47 või artikli 49 lõikes 1 osutatud edastustoimingute korral asjakohastele ja sobivatele tagatistele ning nendest koopia saamise võimalustele või nende avaldamiskohale. Andmesubjektile esitatavad andmed peavad olema õiged ja ajakohased, pidades eriti silmas Euroopa Kohtu kohtupraktikat seoses edastamisega.

<sup>25</sup> Kui vastutav töötaja on andnud eelnevalt konkreetse või üldise kirjaliku nõusoleku kooskõlas isikuandmete kaitse üldmääruse artikli 28 lõikega 2.

<sup>26</sup> Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt c.

<sup>27</sup> Vt Euroopa Andmekaitsekoja vastus korduvale küsimusele nr 11 Euroopa Liidu Kohtu 23. juuli 2020. aasta otsuse kohta kohtuasjas C-311/18 (Data Protection Commissioner vs. Facebook Ireland Ltd ja Maximillian Schrems): „*tuleks pidada meeles, et isegi andmetele juurdepääsu andmine kolmandast riigist näiteks haldusotstarbel on samuti edastamine*“.

<sup>28</sup> Euroopa Komisjonil on õigus määrata isikuandmete kaitse üldmääruse artikli 45 alusel kindlaks, kas ELi mittekuuluv riik tagab isikuandmete piisava kaitse. Samuti on Euroopa Komisjonil õigus määrata, et rahvusvaheline organisatsioon tagab piisava kaitse.

17. Kaitse piisavuse otsused võivad hõlmata riiki tervikuna või piirduda mõne selle osaga. Kaitse piisavuse otsused võivad hõlmata kõiki andmeedastustoiminguid riiki või piirduda teatavat liiki edastamisega (näiteks ühes sektoris).<sup>29</sup>
18. Euroopa Komisjon avaldab oma kaitse piisavuse otsuste loetelu oma veebilehel.<sup>30</sup>
19. Kui edastate isikuandmeid komisjoni kaitse piisavuse otsusega hõlmatud kolmandatesse riikidesse, piirkondadesse või sektoritesse (kohaldatavas ulatuses), **ei pea te astuma täiendavaid siin soovitustes kirjeldatud samme**.<sup>31</sup> Peate siiski jälgima oma andmeedastustoimingute seisukohast oluliste kaitse piisavuse otsuste võimalikku tühistamist või kehtetuks tunnistamist.<sup>32</sup>
20. Kaitse piisavuse otsused ei takista siiski andmesubjekte kaebusi esitamast. Samuti ei keela need järelevalveasutustel pöörduda riiklikku kohtusse, kui neil on otsuse kehtivuse osas kahtlusi, et riiklik kohus saaks esitada Euroopa Kohtule eelotsusetaotluse selle kehtivuse kontrollimiseks.<sup>33</sup>

Näide. ELi kodanik Maximillian Schrems esitas 2013. aasta juunis lirimaa andmekaitsevolinikule kaebuse ja palus sellel järelevalveasutusel keelata või peatada oma isikuandmete edastamine ettevõttest Facebook Ireland Ltd Ameerika Ühendriikidesse, sest leidis, et Ameerika Ühendriikide õigus ja praktika ei taganud enda territooriumil hoitavatele isikuandmetele piisavat kaitset seal avaliku sektori asutuste sooritatava jälitustegevuse vastu. Andmekaitsevolinik lükkas kaebuse tagasi eelkõige põhjendusega, et Euroopa Komisjon on oma programmi Safe Harbor käsitleva otsusega 2000/520 leidnud, et Ameerika Ühendriigid tagavad sinna edastatud isikuandmetele piisava kaitse. M. Schrems vaidlustas andmekaitsevoliniku otsuse ning lirimaa kõrge kohus pöördus küsimusega otsuse 2000/520 kehtivuse kohta Euroopa Liidu Kohtu poole. Seejärel otsustas Euroopa Kohus tunnistada kehtetuks komisjoni otsuse 2000/520 piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega.<sup>34</sup>

<sup>29</sup> Isikuandmete kaitse üldmääruse artikli 45 lõige 1.

<sup>30</sup> [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_et](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_et)

<sup>31</sup> Kui teie ja andmeimportija olete võtnud meetmeid isikuandmete kaitse üldmäärusest tulenevate muude kohustuste täitmiseks; vastasel juhul rakendage nimetatud meetmed.

<sup>32</sup> Euroopa Komisjon peab vaatama kõik kaitse piisavuse otsuseid regulaarselt läbi ning jälgima, kas neist kasu saavad kolmandad riigid tagavad jätkuvalt piisaval tasemel kaitse (vt isikuandmete kaitse üldmääruse artikli 45 lõiked 3 ja 4). Samuti võib Euroopa Kohus kaitse piisavuse otsuseid kehtetuks tunnistada (vt otsused kohtuasjades C-362/14 (Schrems I) and C-311/18 (Schrems II)).

<sup>33</sup> C-311/18 (Schrems II), punktid 118–120. Järelevalveasutused ei tohi kaitse piisavuse otsust arvestamata jätta ega peatada või keelata isikuandmete edastamist sellistesse riikidesse, tuues põhjenduseks ainult kaitsetaseme ebapiisavuse. Nad võivad kasutada ainult oma volitusi peatada või keelata isikuandmete edastamist sellisesse kolmandasse riiki teistel põhjustel (näiteks ebapiisavad turbemeetmed, mis on vastuolus isikuandmete kaitse üldmääruse artikliga 32, või õigusliku aluse puudumine andmete töötlemiseks, mis on vastuolus isikuandmete kaitse üldmääruse artikliga 6). Järelevalveasutused võivad uurida täiesti sõltumatult, kas andmete edastamine on kooskõlas isikuandmete kaitse üldmääruses sätestatud nõuetega, ning pöörduda vajaduse korral riiklike kohtute poole, et viimased saaksid juhul, kui neil on kahtlusi komisjoni kaitse piisavuse otsuse kehtivuse suhtes, esitada Euroopa Kohtule eelotsusetaotluse selle kehtivuse kontrollimiseks.

<sup>34</sup> Kohtuotsus C-362/14 (Schrems I).

### Isikuandmete kaitse üldmääruse artikli 46 kohased edastusvahendid

21. Isikuandmete kaitse üldmääruse artiklis 46 on loetletud mitu „*asjakohaseid kaitsemeetmeid*“ sisaldavat edastusvahendit, mida eksportijad saavad kasutada isikuandmete edastamiseks kolmandatesse riikidesse, kui kaitse piisavuse otsused puuduvad. Artikli 46 kohaste edastusvahendite põhitüübid on
- andmekaitse tüüptingimused;
  - siduvad kontsernisisised eeskirjad;
  - toimimisjuhendid;
  - sertifitseerimismehhanismid;
  - spetsiaalsed lepingutingimused.
22. Olenemata sellest, mis isikuandmete kaitse üldmääruse artikli 46 kohase edastusvahendi valite, peate tagama, et kokkuvõttes on edastatavatel isikuandmetel sisuliselt samaväärne kaitsetase.
23. Peamiselt sisaldavad artikli 46 kohased edastusvahendid asjakohaseid lepingulisi kaitsemeetmeid, mida võib kohaldada kõigisse kolmandatesse riikidesse tehtavate edastustoimingute korral. Olukorras kolmandas riigis, kuhu andmeid edastate, võib siiski tuleneda vajadus täiendada neid edastusvahendeid ja neis sisalduvaid kaitsemeetmeid lisameetmetega (edaspidi „täiendavad meetmed“), et tagada sisuliselt samaväärne kaitsetase.<sup>35</sup>

### Erandid

24. Lisaks kaitse piisavuse otsustele ja isikuandmete kaitse üldmääruse artikli 46 kohastele edastusvahenditele sisaldab nimetatud määrus kolmandat võimalust teatud olukordades isikuandmete edastamiseks. Konkreetsetel tingimustel võib teil siiski olla võimalik edastada isikuandmeid isikuandmete kaitse üldmääruse artiklis 49 sätestatud erandi alusel.
25. Artikkel 49 on olemuselt erandlik. Selles sisalduvaid erandeid tuleb seega tõlgendada piiravalt ja need on peamiselt seotud töötlemistoimingutega, mis on juhuslikud ega kordu. Euroopa Andmekaitsekoostööühendus on andnud välja suunised 2/2018 määruse 2016/679 artikli 49 erandite kohta.<sup>36</sup>
26. Enne isikuandmete kaitse üldmääruse artiklis 49 sätestatud erandi kasutamist peate kontrollima, kas teie andmeedastus vastab rangetele tingimustele, mille täitmist see säte iga toiminguga korral nõuab.
- \*\*\*
27. Kui teie edastustoiming ei saa juriidiliselt põhineda kaitse piisavuse otsusel ega artikli 49 erandil, peate jätkama 3. sammuga.

<sup>35</sup> C-311/18 (Schrems II), punktid 130 ja 133. Vt ka punkt 2.3 allpool.

<sup>36</sup> Üksikasjalikumad suunised on dokumendis aadressil [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation\\_et](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_et).

### 2.3 3. samm. Hinnake, kas teie kasutatav isikuandmete kaitse üldmääruse artikli 46 kohane edastusvahend on kõiki edastamise asjaolusid arvestades tõhus

28. Isikuandmete kaitse üldmääruse artikli 46 kohase edastusvahendi valimine ei pruugi olla piisav. Edastusvahend peab tagama, et edastamine ei kahjustaks isikuandmete kaitse üldmäärusega tagatud kaitsetaset.<sup>37</sup> Teisisõnu peab teie edastusvahend olema praktikas tõhus.
29. Tõhus tähendab, et edastatud isikuandmed on kolmandas riigis kaitstud tasemel, mis on sisuliselt samaväärne EMPs tagatud kaitsega.<sup>38</sup> See ei ole nii, kui andmeimportijal ei saa täita enda valitud isikuandmete kaitse üldmääruse artikli 46 kohasest edastusvahendist tulenevaid kohustusi kolmandas riigis edastamisele kohaldatavate õigusaktide ja praktika tõttu.
30. Seetõttu tuleb hinnata, vajaduse korral koostöös importijaga, kas kolmanda riigi õiguses või praktikas on midagi, mis võiks kahjustada teie kasutatava isikuandmete kaitse üldmääruse artikli 46 kohase edastusvahendi asjakohaste kaitsemeetmete tõhusust teie konkreetse edastustoimingu kontekstis. Vajaduse korral peab teie andmeimportija esitama teile asjakohased allikad ja teabe kolmanda riigi kohta, kus ta asub, ja edastamisel kohaldatavate õigusaktide kohta. Samuti võite kasutada muid teabeallikaid, näiteks 3. lisa näitlikena loetletud allikaid.<sup>39</sup>
31. Teie hinnang peaks arvestama kõiki edastustoimingute uurimisel tuvastatud edastamises osalevaid pooli (näiteks vastutavaid töötlejaid, volitatud töötlejaid ja alamtöötlejaid, kes töötlevad andmeid kolmandas riigis). Mida rohkem vastutavaid töötlejaid, volitatud töötlejaid ja importijaid on asjaga seotud, seda keerukam on hindamine. Samuti peate hindamisel arvestama võimalikku hilisemat andmete edasisaatmist.
32. Selleks peate uurima iga edastustoimingu omadusi ja määrama, kuidas kohaldub neile edastustoimingutele kehtiv õiguskord riigis, kuhu andmeid edastatakse (või hiljem edasi saadetakse).
33. Kohalduv õiguslik kontekst sõltub edastamise asjaoludest – konkreetselt järgmisest:
  - eesmärk, milleks andmeid edastatakse ja töödeldakse (näiteks turundus, personalihaldus, talletamine, IT-tugi, kliinilised uuringud);
  - töötlemisel osalevate üksuste liigid (era- või avalik-õiguslik; vastutav/volitatud töötleja);
  - majandusharu, milles edastamine toimub (näiteks reklaamitehnika, side, finantsteenused);
  - edastatavate isikuandmete kategooriad (näiteks laste isikuandmed võivad kuuluda kolmandas riigis eriõigusaktide kohaldamisalasse);
  - kas andmeid hoitakse kolmandas riigis või antakse ainult kaugjuurdepääs ELis/EMPs hoitavatele andmetele;
  - edastatavate andmete vorm (lihttekstina / pseudonüümitud või krüptitud<sup>40</sup>);
  - võimalus, et andmeid võidakse kolmandast riigist muusse kolmandasse riiki edasi saata.<sup>41</sup>

<sup>37</sup> Isikuandmete kaitse üldmääruse artikkel 44.

<sup>38</sup> C-311/18 (Schrems II), punkt 105 ja teine järeldus.

<sup>39</sup> Vt ka punkt 43 allpool.

<sup>40</sup> Mõni kolmas riik ei luba krüptitud andmete importimist.

<sup>41</sup> Kui vastutav töötleja on andnud eelnevalt konkreetse või üldise kirjaliku nõusoleku kooskõlas isikuandmete kaitse üldmääruse artikli 28 lõikega 2.

34. Kohaldatavate õigusaktide seas tuleb hinnata, kas mõni neist kahjustab teie valitud isikuandmete kaitse üldmääruse artikli 46 kohases edastusvahendiga seotud kohustusi. Peate kontrollima, kas kohustusi, mis võimaldavad andmesubjektidel kasutada enda õigusi rahvusvahelise edastamise kontekstis (näiteks edastatud andmetega tutvumise, parandamise ja kustutamise taotlemine), saab praktikas tõhusalt täita ning ega sihtkohaks oleva kolmanda riigi õigus seda ei takista.
35. Peate hindama asjakohaseid üldisi eeskirju, sest neil on mõju isikuandmete kaitse üldmääruse artikli 46 kohases edastusvahendis sisalduvate kaitsemeetmete rakendamisele ning üksikisikute põhiõigustele (eriti andmesubjektile võimaldatava hüvituse õigusest juhul, kui kolmanda riigi ametiasutused saavad edastatud andmetele juurdepääsu).
36. Igal juhul pöörake erilist tähelepanu kõigile olulistele õigusaktidele, eriti neile, millega on kehtestatud nõudeid isikuandmete avaldamise kohta avaliku sektori asutustele või antud sellistele asutustele volitusi isikuandmetega tutvumiseks (näiteks kriminaalõiguse jõustamise, regulatiivjärelevalve ja riikliku julgeoleku eesmärgil). Kui need nõuded või volitused piirduvad sellega, mis on demokraatlikus ühiskonnas vajalik ja proportsionaalne<sup>42</sup>, ei pruugi need kahjustada kohustusi, mis sisalduvad teie kasutatavas isikuandmete kaitse üldmääruse artikli 46 kohases edastusvahendis.
37. Et hinnata, kas selline avaliku sektori asutuste juurdepääs piirduv demokraatlikus ühiskonnas vajaliku ja proportsionaalsega ning kas andmesubjektidel on tõhusad kaitsevõimalused, tuleb kasutada võrdluseks ELi standardeid, näiteks ELi põhiõiguste harta artikleid 47 ja 52.
38. Sellel hindamisel on olulised ka kolmanda riigi õigussüsteemi mitmesugused aspektid, näiteks isikuandmete kaitse üldmääruse artikli 45 lõikes 2 loetletud elemendid.<sup>43</sup> Näiteks võib valitsuse ebaseadusliku isikuandmetele juurdepääsu korral üksikisikutele kättesaadavate (õigus)kaitse mehhanismide tõhususe hindamisel olla oluline kolmanda riigi õigusriigi põhimõtete olukord. Valitsuse sekkumise proportsionaalsuse tagamisele võib kaasa aidata ka põhjaliku andmekaitse seaduse või sõltumatu andmekaitseasutuse olemasolu ning selliste rahvusvaheliste õigusaktide järgimine, milles on ette nähtud andmekaitsemeetmed.<sup>44</sup>

\*\*\*

39. Euroopa Andmekaitse nõukogu Euroopa oluliste tagatiste soovitusel kirjeldatakse elemente, mida tuleb hinnata, et määrata, kas kolmanda riigi avaliku sektori asutuste, nt riikliku julgeoleku asutuste või õiguskaitseasutuste juurdepääsu isikuandmetele reguleerivat õigusraamistikku võib käsitleda põhjendatud sekkumisena (ning seetõttu isikuandmete kaitse üldmääruse artikli 46 kohase edastusvahendiga võetavaid kohustusi mitte kahjustavana) või mitte. Eelkõige tuleb seda hoolikalt kaalutleda, kui avaliku sektori asutuste juurdepääsu andmetele reguleerivad õigusaktid on mitmeti mõistetavad või ei ole avalikult kättesaadavad.

---

<sup>42</sup> Vt ELi põhiõiguste harta artiklid 47 ja 52, isikuandmete kaitse üldmääruse artikli 23 lõige 1 ja Euroopa Andmekaitse nõukogu 10. novembri 2020. aasta soovitusel 02/2020 Euroopa oluliste tagatiste kohta seoses järelevalvemeetmetega, [https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential\\_et](https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_et).

<sup>43</sup> C-311/18 (Schrems II), punkt 104.

<sup>44</sup> Näide: konventsioon 108 (konventsioon üksikisikute kaitse kohta isikuandmete automatiseeritud töötlemisel, ETS nr 108) või konventsioon 108+ (moderniseeritud konventsioon üksikisikute kaitse kohta isikuandmete automatiseeritud töötlemisel, CETS nr 223) nähakse ette jõustatavad rahvusvahelised õiguskaitsemeetmed andmekaitserikkumiste korral ning nendega toetatakse isikuandmete kaitse miinimumtaseme ja eraelu puutumatuse tagamist.

40. Kui neid kohaldatakse artikli 46 kohastel edastusvahenditel põhinevate andmeedastustoimingutega seotud olukordadele, võivad Euroopa Andmekaitsekoogu Euroopa oluliste tagatiste soovitusel aidata andmeeksportijal ja andmeimportijal hinnata, kas need volitused takistavad andmeimportijal põhjendamatult sisulise samaväärsuse tagamise kohustuste täitmist.
41. Sisuliselt samaväärse kaitsetaseme puudumine on eriti ilmne, kui teie edastustoimingu mõistes asjakohase kolmanda riigi õigusaktid või praktika ei vasta Euroopa oluliste tagatiste nõuetele.
42. Hindamine peab põhinema eelkõige avalikult kättesaadavatel õigusaktidel. Mõnes olukorras sellest siiski ei piisa, sest kolmandates riikides võivad õigusaktid puududa. Kui soovite sellisel juhul siiski andmeid edastada, uurige muid asjakohaseid ja objektiivseid tegureid<sup>45</sup>, tuginemata subjektiivsetele teguritele, näiteks tõenäosusele, et avaliku sektori asutused kasutavad teie andmeid viisil, mis ei ole kooskõlas ELi standarditega. See hindamine tuleb teha vajaliku hoolikusega ja põhjalikult dokumenteerida, sest vastutate selle põhjal tehtava võimaliku otsuse eest.<sup>46</sup>
43. Võite täiendada hinnangut teistest allikatest saadud andmetega<sup>47</sup>, näiteks:
- tõendid, et kolmanda riigi ametiasutus püüaks saada juurdepääsu andmetele nii andmeimportija teadmisel kui ka ilma, pidades silmas teatatud pretsedente, õigusakte ja praktikat;
  - tõendid, et kolmanda riigi ametiasutusel oleks võimalik saada andmetele juurdepääs andmeimportija kaudu või sidekanali vahetult jälgides, pidades silmas teatatud pretsedente, juriidilisi volitusi ning tema käsutuses olevaid tehnilisi, rahalisi ja inimressursse.
44. Hindamisel võib lõpuks selguda, et teie kasutatav isikuandmete kaitse üldmääruse artikli 46 kohane edastusvahend ja selles sisalduvad asjakohased kaitsemeetmed on järgmiste omadustega.
- Tagavad tõhusalt, et edastatud isikuandmed on kolmandas riigis kaitstud tasemel, mis on sisuliselt samaväärne EMPs tagatud kaitsega. Kolmandas riigis andmeedastusele kohaldatavad õigusaktid ja tavad annavad andmeimportijale võimaluse täita enda valitud edastusvahendist tulenevaid kohustusi. Taashinnake olukorda sobivate ajavahemike järel või oluliste muutuste ilmnemisel (vt 6. samm).
  - Ei taga tõhusalt sisuliselt samaväärset kaitsetaset. Andmeimportija ei saa kolmandas riigis andmeedastusele kohaldatavate õigusaktide ja/või tavade tõttu enda kohustusi täita. Euroopa Kohus on rõhutanud, et kui isikuandmete kaitse üldmääruse artikli 46 kohane edastusvahend osutub ebapiisavaks, on andmeeksportija ülesanne võtta tõhusad täiendavaid meetmeid või isikuandmeid mitte edastada.<sup>48</sup>

---

<sup>45</sup> Vt punkt 43 allpool ning 3. lisa.

<sup>46</sup> Isikuandmete kaitse üldmääruse artikli 5 lõige 2.

<sup>47</sup> Vt ka 3. lisa.

<sup>48</sup> C-311/18 (Schrems II), punktid 134–135.

Näiteks otsustas Euroopa Kohus, et Ameerika Ühendriikide välisluure jälitustegevuse seaduse (FISA) paragrahv 702 ei vasta ELi õiguse kohasest proportsionaalsuse põhimõttest tulenevatele minimaalsetele kaitsemeetmetele ning seda ei saa käsitleda rangelt vajalikuga piirduvana. See tähendab, et nimetatud seaduse paragrahvi 702 volitatud programmide kaitsetase ei ole ELi õigusega nõutavate kaitsemeetmetega sisuliselt samaväärne. Seetõttu võib siis, kui andmeimportija või kes tahes edasine vastuvõtja, kellele andmeimportija võib andmeid avaldada, kuulub FISA paragrahvi 702 kohaldamisalasse<sup>49</sup>, tugineda sellisel edastamisel andmekaitse tüüptingimustele või teistele isikuandmete kaitse üldmääruse artikli 46 kohastele edastusvahenditele ainult siis, kui täiendavad tehnilised meetmed välistavad juurdepääsu edastatavatele andmetele.

## 2.4 4. samm. Võtke vastu täiendavad meetmed

45. Kui 3. sammu hinnang on näidanud, et teie kasutatav isikuandmete kaitse üldmääruse artikli 46 kohane edastusvahend ei ole tõhus, peate kaalutlema (koos importijaga, kui asjakohane), kas on olemas täiendavaid meetmeid, mille lisamine edastusvahendi kaitsemeetmetele võiks tagada, et edastatud andmed oleksid kolmandas riigis kaitstud ELis tagatuga sisuliselt samaväärsel tasemel.<sup>50</sup> „Täiendavad meetmed“ on meetmed, mis täiendavad kaitsemeetmeid, mida isikuandmete kaitse üldmääruse artikli 46 kohane edastusvahend juba pakub.<sup>51</sup>
46. Peate igal üksikjuhul eraldi tuvastama, mis täiendavad meetmed võiksid olla tõhusad, kui andmeid edastatakse korduvalt konkreetsesse kolmandasse riiki, kasutades konkreetset isikuandmete kaitse üldmääruse artikli 46 kohast edastusvahendit. Saate kasutada oma varasemaid hindamisi (1., 2. ja 3. sammus) ning kontrollida nende järelduste alusel täiendavate meetmete võimalikku tõhusust nõutava kaitsetaseme tagamisel.
47. Põhimõtteliselt võivad täiendavad meetmed olla olemuslikult lepingulised, tehnilised või korralduslikud. Eri meetmete üksteist toetav ja täiendav kombineerimine võib parandada kaitsetaset ning aidata seega saavutada ELi standardeid.
48. Üldiselt ei lahenda avaliku sektori asutuste juurdepääsu isikuandmetele kolmandas riigis ainult lepinguliste ja korralduslike meetmetega (kui juurdepääs takistab põhjendamatult andmeimportija kohustuste täitmist sisulise samaväärsuse tagamisel). Tekib tõepoolest olukordi, kus kolmandate riikide avaliku sektori asutuste juurdepääsu isikuandmetele, eriti jälitustegevuseks, võiksid takistada

---

<sup>49</sup> FISA paragrahvi 702 kohaldatakse siis, kui andmed on saadud „elektroonilise sideteenuse osutajalt või tema abiga“ (FISA paragrahv 702 = Ameerika Ühendriikide seadustiku 50. jaotise paragrahvi 1881a lõike h punkti 2 alapunkti A alapunkt vi), mis omakorda on määratletud Ameerika Ühendriikide seadustiku 50. jaotise paragrahvi 1881 lõike b punktis 4 järgmiselt:

„A) sideettevõtja, nagu on määratletud 47. jaotise paragrahvis 153;

B) elektroonilise sideteenuse osutaja, nagu on määratletud 18. jaotise paragrahvis 2510;

C) kaugandmetöötlusteenuse osutaja, nagu on määratletud 18. jaotise paragrahvis 2711;

D) mis tahes muu sideteenuse osutaja, kellel on juurdepääs kaabel- või elektroonilisele sidele kas side edastamisel või salvestamisel, või

E) punktides A, B, C või D kirjeldatud üksuse ametnik, töötaja või agent.“

<sup>50</sup> C-311/18 (Schrems II), punkt 96.

<sup>51</sup> Isikuandmete kaitse üldmääruse põhjendus 109 ja C-311/18 (Schrems II) punkt 133.

või muuta mõjutuks ainult tehnilised meetmed.<sup>52</sup> Sellisel juhul võivad lepingulised või korralduslikud meetmed täiendada tehnilisi meetmeid ja tugevdada andmete üldist kaitset, näiteks takistades avaliku sektori asutuste püüdeid saada andmetele juurdepääsu ELi standarditega kokkusobimatul viisil.

49. Võite uurida (koostöös importijaga, kui asjakohane) järgmist (mitteammendavat) tegurite loetelu, et tuvastada, mis täiendavad meetmed on edastatavate andmete kaitset kõige tõhusamad:
- edastatavate andmete vorm (lihttekstina / pseudonüümitud või krüptitud);
  - andmete olemus;
  - andmetöötluse töövoos pikkus ja keerukus, töötlemises osalevate tegutsejate arv ning nende suhe (näiteks kas edastamine hõlmab mitut vastutavat töötajat või nii vastutavaid kui ka volitatud töötajaid või selliste volitatud töötajate kaasamine, kes edastavad andmed teie andmeimportijale (arvestades nende suhtes kohaldatavaid asjakohaseid sätteid vastavalt kolmanda sihtriigi õigusaktidele));<sup>53</sup>
  - võimalus, et andmeid saadetakse veel edasi samas kolmandas riigis või isegi kolmandate riikide vahel (näiteks andmeimportija alamtöötaja osalusel<sup>54</sup>).

#### Täiendavate meetmete näited

50. Mõni tehniliste, lepinguliste ja organisatsiooniliste meetmete näide, mida kaalutleda, on 2. lisa kirjeldatud mitteammendavates loeteludes.

\*\*\*

51. Kui olete võtnud tõhusad täiendavad meetmed, mis koos teie valitud isikuandmete kaitse üldmääruse artikli 46 kohase edastusvahendiga ulatuvad kaitsetasemele, mis on nüüd EMPs tagatuga sisuliselt samaväärne, tohib edastamine toimuda.
52. Kui te ei suuda leida või rakendada tõhusaid täiendavaid meetmeid, mis tagaksid edastatavatele andmetele sisuliselt samaväärse kaitse<sup>55</sup>, ei tohi te isikuandmeid enda kasutatava isikuandmete kaitse üldmääruse artikli 46 kohase edastusvahendi abil asjaomasesse kolmandasse riiki edastada. Kui te andmeid juba edastate, peate isikuandmete edastamise peatama või lõpetama.<sup>56</sup> Vastavalt teie kasutatavas isikuandmete kaitse üldmääruse artikli 46 kohases edastusvahendis sisalduvatele

---

<sup>52</sup> Kui selline juurdepääs ületab demokraatlikus ühiskonnas vajaliku ja proportsionaalse; vt ELi põhiõiguste harta artiklid 47 ja 52, isikuandmete kaitse üldmääruse artikli 23 lõige 1 ja Euroopa Andmekaitse nõukogu 10. novembri 2020. aasta soovitus 02/2020 Euroopa oluliste tagatiste kohta seoses järelevalvemeetmetega, [https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential\\_et](https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_et).

<sup>53</sup> Isikuandmete kaitse üldmäärusega määratakse vastutavatele töötajatele ja volitatud töötajatele selgepiirilised kohustused. Edastamine võib toimuda ühelt vastutavalt töötajalt teisele, ka vastutavate töötajate vahel, vastutavalt töötajalt volitatud töötajale ning vastutava töötaja volituse korral volitatud töötajalt vastutavale töötajale või volitatud töötajalt volitatud töötajale.

<sup>54</sup> Vt 25. allmärkus.

<sup>55</sup> Kui selline juurdepääs ületab demokraatlikus ühiskonnas vajaliku ja proportsionaalse; vt ELi põhiõiguste harta artiklid 47 ja 52, isikuandmete kaitse üldmääruse artikli 23 lõige 1 ja Euroopa Andmekaitse nõukogu 10. novembri 2020. aasta soovitus 02/2020 Euroopa oluliste tagatiste kohta seoses järelevalvemeetmetega, [https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential\\_et](https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_et).

<sup>56</sup> C-311/18 (Schrems II), punkt 135.



kaitsemeetmetele peab importija täielikult tagastama teile või hävitama andmed, mida olete sellesse kolmandasse riiki juba edastanud, ning nende koopiad.<sup>57</sup>

Näide: kolmanda riigi õigus keelab teie tuvastatud täiendavad meetmed (näiteks keelab krüptimise) või takistab teisiti nende tõhusust. Te ei tohi alustada isikuandmete edastamist sellesse riiki või peate lõpetama toimuvad edastustoimingud sellesse riiki.

53. Kui otsustate jätkata edastamist, kuigi importija ei suuda täita isikuandmete kaitse üldmääruse artikli 46 kohase edastusvahendiga võetud kohustusi, peate sellest teatama pädevale järelevalveasutusele vastavalt asjakohase edastusvahendiga seotud erisätetele.<sup>58</sup> Pädev järelevalveasutus peab peatama või keelama andmete edastamise sellistel juhtudel, kui ta leiab, et sisuliselt samaväärset kaitsetaset ei ole võimalik tagada.<sup>59</sup>
54. Pädev järelevalveasutus võib määrata mis tahes muu parandusmeetme (näiteks trahvi), kui alustate või jätkate andmete edastamist, kuigi te ei suuda tõendada sisuliselt samaväärset kaitset kolmandas riigis.

## 2.5 5. samm. Menetluslikud sammud, kui olete tuvastanud tõhusad täiendavad meetmed

55. Menetluslikud sammud, mida võite vajada pärast rakendatavate tõhusate täiendavate meetmete tuvastamist, võivad oleneda isikuandmete kaitse üldmääruse artikli 46 kohasest edastusvahendist, mida kasutate või kavatsete kasutada.

### 2.5.1 Andmekaitse tüüptingimused (isikuandmete kaitse üldmääruse artikli 46 lõike 2 punktid c ja d)

56. Kui kavatsete kehtestada täiendavaid meetmeid lisaks lepingu tüüptingimustele, ei ole teil vaja küsida pädeva järelevalveasutuse luba nende tingimuste või täiendavate kaitsemeetmete lisamiseks, kui tuvastatud täiendavad meetmed ei ole otseselt või kaudselt vastuolus lepingu tüüptingimustega ja on piisavad tagamaks, et isikuandmete kaitse üldmäärusega tagatud kaitset ei kahjustata.<sup>60</sup> Andmeekspordija ja -importija peavad tagama, et täiendavaid tingimusi ei saaks mõista viisil, mis piirab lepingu tüüptingimustes sisalduvaid õigusi ja kohustusi või vähendab mis tahes muul viisil andmekaitse taset. Peate suutma seda tõendada, sealhulgas kõigi tingimuste üheselt mõistetavust, lähtudes vastutuse põhimõttest ja teie kohustusest tagada piisav andmekaitse tase. Pädevatel

<sup>57</sup> Vt lepingu tüüptingimuste otsuse 87/2010 lisa 12. tingimus; vt (valikuline) täiendav lõpetamistingimus lepingu tüüptingimuste otsuse 2004/915/EÜ lisa B.

<sup>58</sup> Vt Euroopa Andmekaitsekoja korduvad küsimused Euroopa Liidu Kohtu otsuse kohta kohtuasjas Data Protection Commissioner vs. Facebook Ireland Ltd ja Maximillian Schrems (C-311/18), vastu võetud 23. juulil 2020, ning eriti küsimused 5, 6 ja 9. Vt komisjoni otsuse 2010/87/EL 4. tingimuse punkt g, komisjoni otsuse 2001/497/EÜ 5. klausli punkt a ja komisjoni otsuse 2004/915/EÜ lisa „II kogum“ punkt c.

<sup>59</sup> C-311/18 (Schrems II), punktid 113 ja 121.

<sup>60</sup> Isikuandmete kaitse üldmääruse põhjenduses 109 märgitakse: „Vastutavale töötajale või volitatud töötajale antud võimalus kasutada komisjoni või järelevalveasutuse vastu võetud standardseid andmekaitsetingimusi ei tohiks takistada vastutavat töötajat või volitatud töötajat lisamast standardsed andmekaitseklauslid laiemasse lepingusse, nagu näiteks kahe volitatud töötaja vahelisse lepingusse, ega lisamast muid klausleid või täiendavaid kaitsemeetmeid, tingimusel et need ei lähe otseselt ega kaudselt vastuollu komisjoni või järelevalveasutuse vastu võetud lepingu tüüptingimustega ega piira andmesubjektide põhiõigusi ja -vabadusi.“ Sarnased sätted on sätestanud Euroopa Komisjon direktiivi 95/45/EÜ alusel vastu võetud lepingu tüüptingimuste kogumites.

järelevalveasutustel on õigus neid täiendavaid tingimusi läbi vaadata, kui asjakohane (näiteks kaebuse või omal algatusel esitatud päringu korral).

57. Kui kavatsete muuta andmekaitse tüüptingimusi endid või kui lisatud täiendavad meetmed lähevad lepingu tüüptingimustega otseselt või kaudselt vastuollu, ei käsitleta teid enam lepingu tüüptingimusi kasutavana<sup>61</sup> ning peate küsima pädeva järelevalveasutuse loa kooskõlas isikuandmete kaitse üldmääruse artikli 46 lõike 3 punktiga a.

### 2.5.2 Siduvad kontsernisisesed eeskirjad (isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkt b)

58. Schrems II kohtuotsuses esitatud põhjendused kehtivad ka teiste isikuandmete kaitse üldmääruse artikli 46 lõike 2 kohaste edastusvahendite korral, sest kõik need vahendid on olemuselt lepingulised, nii et nende alusel ette nähtud tagatised ja osaliste võetud kohustused ei saa siduda kolmanda riigi avaliku sektori asutusi.<sup>62</sup>
59. Schrems II kohtuotsus on siduvate kontsernisisesete eeskirjade alusel tehtaval isikuandmete edastusel oluline, sest kolmandate riikide õigusaktid võivad mõjutada selliste vahenditega pakutavat kaitset. Schrems II otsuse täpset mõju siduvatele kontsernisisesetele eeskirjadele arutatakse endiselt. Euroopa Andmekaitsekoostöögrupp annab esimesel võimalusel üksikasjalikumalt teavet, kas viitedokumendis WP256/257 esitatud siduvatesse kontsernisisesesse eeskirjadesse on vaja lisada täiendavaid kohustusi.<sup>63</sup>
60. Kohus rõhutas, et andmeeksportija ja andmeimportija ülesanne on hinnata, kas asjaomases kolmandas riigis järgitakse ELi õigusega nõutavat kaitsetaset, et määrata, kas lepingu tüüptingimuste või siduvate kontsernisisesete eeskirjadega ette nähtud kaitsemeetmeid on võimalik järgida praktikas. Vastasel juhul peate hindama, kas saate sätestada täiendavaid meetmeid, et tagada sisuliselt samaväärne kaitsetase, nagu tagatakse EMPs, ning kas kolmanda riigi õigus ega praktika ei piira neid täiendavaid meetmeid, vähendades nende tõhusust.

### 2.5.3 Spetsiaalsed lepingutingimused (isikuandmete kaitse üldmääruse artikli 46 lõike 3 punkt a)

61. Schrems II kohtuotsuses esitatud põhjendused kehtivad ka teiste isikuandmete kaitse üldmääruse artikli 46 lõike 2 kohaste edastusvahendite korral, sest kõik need vahendid on olemuselt lepingulised, nii et nende alusel ette nähtud tagatised ja osaliste võetud kohustused ei saa siduda kolmanda riigi avaliku sektori asutusi.<sup>64</sup> Seetõttu on Schrems II kohtuotsus spetsiaalsete lepingutingimuste alusel

---

<sup>61</sup> Vt analoogia alusel: juba vastu võetud Euroopa Andmekaitsekoostöögrupp arvamused 17/2020 Sloveenia järelevalveasutuse esitatud artikli 28 kohaste lepingu tüüptingimuste eelnõu kohta (isikuandmete kaitse üldmääruse artikli 28 lõige 8), mis sisaldab sarnast sätet („Lisaks tuleb andmekaitsekoostöögrupp meelde, et järelevalveasutuse vastuvõetud lepingu tüüptingimuste kasutamise võimalus ei takista pooli lisamast muid tingimusi või täiendavaid kaitsemeetmeid, tingimusel et need ei lähe otseselt ega kaudselt vastuollu vastuvõetud lepingu tüüptingimustega ega piira andmesubjektide põhiõigusi ega -vabadusi. Peale selle, kui andmekaitse tüüptingimusi muudetakse, ei loeta seda enam olukorraks, kus pooled rakendavad vastuvõetud lepingu tüüptingimusi.“)

([https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_opinion\\_202017\\_art28sccs\\_si\\_et.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_et.pdf)).

<sup>62</sup> C-311/18 (Schrems II), punkt 132.

<sup>63</sup> Artikli 29 tööühma töödokument, milles kehtestatakse siduvates kontsernisisesetes eeskirjades sisalduvate elementide ja põhimõtete tabel (viimati muudetud ja vastu võetud 6. veebruaril 2018, WP 256 rev.01); artikli 29 tööühma töödokument, milles kehtestatakse siduvates kontsernisisesetes eeskirjades sisalduvate elementide ja põhimõtete tabel (viimati muudetud ja vastu võetud 6. veebruaril 2018, WP 257 rev.01).

<sup>64</sup> C-311/18 (Schrems II), punkt 132.

tehtaval isikuandmete edastusel oluline, sest kolmandate riikide õigusaktid võivad mõjutada selliste vahenditega pakutavat kaitset. Schrems II otsuse täpset mõju spetsiaalsetele tingimustele arutatakse endiselt. Andmekaitsekoostöö annab esimesel võimalusel üksikasjalikumad teavet.

## 2.6 6. samm. Taashinnake olukorda asjakohaste ajavahemike järel

62. Peate jälgima pidevalt ja (kui asjakohane) koostöös andmeimportijatega muutusi kolmandas riigis, kuhu olete isikuandmeid edastanud, mis võiksid mõjutada teie algset kaitsetaseme hinnangut ja otsuseid, mida olete teinud selle põhjal oma edastustoimingute kohta. Vastutus on jätkuv kohustus (isikuandmete kaitse üldmääruse artikli 5 lõige 2).
63. Peate võtma kasutusele piisavalt usaldusväärsed mehhanismid tagamaks, et peatate või lõpetate andmete edastamise kohe, kui
  - importija on rikkunud või ei suuda täita kohustusi, mida ta on isikuandmete kaitse üldmääruse artikli 46 kohase edastusvahendi alusel võtnud, või
  - täiendavad meetmed ei ole selles kolmandas riigis enam tõhusad.

### 3 KOKKUVÕTE

64. Isikuandmete kaitse üldmäärusega on kehtestatud eeskirjad isikuandmete töötlemise kohta EMPs ning sellega lubatakse isikuandmete vaba liikumist EMP piires. Isikuandmete kaitse üldmääruse V peatükk reguleerib isikuandmete edastamist kolmandatesse riikidesse ja seab kõrge eesmärgi: edastamine ei tohi kahjustada isikuandmete kaitse üldmäärusega tagatud füüsiliste isikute kaitsetaset (artikkel 44). Euroopa Kohtu otsuses kohtuasjas C-311/18 (Schrems II) rõhutatakse vajadust tagada isikuandmete edastamisel kolmandatesse riikidesse isikuandmete kaitse üldmäärusega loodud kaitsetaseme järjepidevus.<sup>65</sup>
65. Oma andmetele sisuliselt samaväärse kaitse tagamiseks peate eelkõige olema põhjalikult kursis oma andmeedastustegevusega. Peate ka kontrollima, et teie edastatavad andmed oleksid piisavad, asjakohased ja piirduksid sellega, mis on nende kolmandasse riiki edastamiseks ja seal töötlemiseks vajalik.
66. Samuti peate tuvastama, mis edastusvahendit oma edastustoimingutel kasutate. Kui edastusvahendiks ei ole kaitse piisavuse otsus, peate kontrollima igal üksikjuhul eraldi, kas kolmanda sihtriigi õigus või praktika ohustab (või mitte) teie edastustoimingute korral isikuandmete kaitse üldmääruse artikli 46 kohases edastusvahendis sisalduvaid kaitsemeetmeid. Kui isikuandmete kaitse üldmääruse artikli 46 kohane edastusvahend üksi ei suuda saavutada edastatavatele isikuandmetele sisuliselt samaväärset kaitset, võivad lünga täita täiendavad meetmed.
67. Kui te ei suuda leida või rakendada tõhusaid täiendavaid meetmeid, mis tagaksid edastatavatele andmetele sisuliselt samaväärse kaitse, ei tohi te isikuandmeid enda valitud edastusvahendi abil asjaomasesse kolmandasse riiki edastada. Kui te andmeid juba edastate, peate isikuandmete edastamise kohe peatama või lõpetama.
68. Pädeval järelevalveasutusel on volitused peatada või lõpetada isikuandmete edastamine kolmandasse riiki, kui ELi õigusega, eelkõige isikuandmete kaitse üldmääruse artiklitega 45 ja 46 nõutav edastatavate andmete kaitse ei ole tagatud.

Euroopa Andmekaitsekojale nimel

eesistuja

(Andrea Jelinek)

---

<sup>65</sup> C-311/18 (Schrems II), punkt 93.

## 1. LISA. MÕISTED

- Kolmas riik – iga riik, mis ei ole EMP liikmesriik.
- EMP – Euroopa Majanduspiirkond, kuhu kuuluvad Euroopa Liidu liikmesriigid ning Island, Norra ja Liechtenstein. Isikuandmete kaitse üldmäärust kohaldatakse viimaste suhtes EMP lepingu, täpsemalt selle XI lisa ja protokolli nr 37 alusel.
- Isikuandmete kaitse üldmäärus – Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus).
- Harta – Euroopa Liidu põhiõiguste harta (ELT C 326, 26.10.2012, lk 391–407).
- Kohus või Euroopa Kohus – Euroopa Liidu Kohus. See asutus esindab Euroopa Liidu kohtuvõimu ning jälgib koostöös liikmesriikide kohtutega, et Euroopa Liidu õigust kohaldataks ja tõlgendataks ühetaoliselt.
- Andmeksportija – EMPs asuv vastutav või volitatud töötaja, kes edastab isikuandmeid kolmandas riigis asuvale vastutavale või volitatud töötajale.
- Andmeimportija – kolmandas riigis asuv vastutav või volitatud töötaja, kes võtab vastu EMPst edastatud isikuandmeid või saab neile juurdepääsu.
- Isikuandmete kaitse üldmääruse artikli 46 kohane edastusvahend – asjakohased isikuandmete kaitse üldmääruse artikli 46 kohased kaitsemeetmed, mida andmeksportijad rakendavad isikuandmete edastamisel kolmandasse riiki, kui isikuandmete kaitse üldmääruse artikli 45 lõike 3 kohast kaitse piisavuse otsust ei ole vastu võetud. Isikuandmete kaitse üldmääruse artikli 46 lõiked 2 ja 3 sisaldavad loetelu selle artikli kohastest edastusvahenditest, mida vastutavad töötlejad ja volitatud töötlejad võivad kasutada.
- Lepingu tüüptingimus – Euroopa Komisjoni vastu võetud andmekaitse tüüptingimus seoses isikuandmete edastamisega EMPs ja sellest väljaspool asuvate vastutavate töötajate ja volitatud töötajate vahel. Euroopa Komisjoni vastu võetud lepingu tüüptingimused on isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkti c ja lõike 5 alusel isikuandmete kaitse üldmääruse kohane edastusvahend.

## 2. LISA. TÄIENDAVATE MEETMETE NÄITED

69. Siin on näited täiendavatest meetmetest, mida saate kaalutleda, kui olete jõudnud 4. sammuni, mil tuleb võtta täiendavaid meetmeid. See loetelu ei ole ammendav. Neist ühe või mitme meetme valimine ja rakendamine ei pruugi tingimata ja süstemaatiliselt tagada, et teie edastustoimingud vastavad ELi õigusega nõutavale sisulise samaväärsuse standardile. Valige need täiendavad meetmed, mis suudavad selle kaitsetaseme teie edastustoimingutele tõhusalt tagada.
70. Mis tahes täiendavat meetet võib pidada Euroopa Kohtu otsuse „Schrems II“ tähenduses tõhusaks ainult siis ja ulatuses, kui see kõrvaldab teie kolmanda riigi õigusolukorra hinnangus tuvastatud konkreetsed puudused. Kui te ei suuda kokkuvõttes tagada sisuliselt samaväärsel tasemel kaitset, ei tohi te isikuandmeid edastada.
71. Vastutava või volitatud töötlejana võib teil juba olla kohustus rakendada mõnd käesolevas lisas kirjeldatud meetet, isegi kui teie andmeimportija on hõlmatud kaitse piisavuse otsusega, samamoodi nagu teil võib olla kohustus rakendada neid andmete töötlemisel EMP piires.<sup>66</sup>

### Tehnilised meetmed

72. Siin punktis on mitteammendav loetelu tehnilistest meetmetest, mis võivad täiendada isikuandmete kaitse üldmääruse artikli 46 kohastes edastusvahendites sisalduvaid kaitsemeetmeid, et tagada isikuandmete kolmandasse riiki edastamise kontekstis kooskõla kaitsetasemega, mida nõutakse ELi õigusega. Need meetmed on eriti vajalikud juhul, kui asjaomase kolmanda riigi õigusaktid kehtestavad andmeimportijale kohustusi, mis on vastuolus isikuandmete kaitse üldmääruse artikli 46 kohaste edastusvahendite kaitsemeetmetega ning mis võivad eelkõige kahjustada lepingulist tagatist, et pakutakse sisuliselt samaväärset kaitset asjaomase kolmanda riigi avaliku sektori asutuste neile andmetele juurdepääsu vastu.<sup>67</sup>
73. Täiendava selguse huvides kirjeldatakse siin kõigepealt tehnilisi meetmeid, mis võivad olla tõhusad teatud stsenaariumides/kasutusjuhtudel sisuliselt samaväärse kaitse tagamisel. Seejärel kirjeldatakse stsenaariume/kasutusjuhte, mille korral ei suudetud leida tehnilisi meetmeid, mis tagaksid selle kaitsetaseme.

---

### Stsenaariumid, mille korral suudeti leida *tõhusad* meetmed

---

74. Allpool loetletud meetmete eesmärk on tagada, et kolmandate riikide avaliku sektori asutuste juurdepääs edastatavatele andmetele ei kahjusta isikuandmete kaitse üldmääruse artikli 46 kohases edastusvahendis sisalduvate asjakohaste kaitsemeetmete tõhusust. Neid meetmeid rakendatakse ka siis, kui avaliku sektori asutuste juurdepääs on kooskõlas importija riigi õigusega, kui see juurdepääs ulatub demokraatlikus ühiskonnas vajalikust ja proportsionaalsest kaugemale.<sup>68</sup> Nende meetmete eesmärk on ennetada potentsiaalselt nõuetevastast juurdepääsu, takistades ametiasutuste võimalust tuvastada andmesubjekte, tuletada nende kohta teavet, eristada neid muus kontekstis või seostada edastatud andmeid teiste nende käsutuses olevate andmekogumitega, mis võivad sisaldada muude

---

<sup>66</sup> Isikuandmete kaitse üldmääruse artikli 5 lõige 2 ja artikkel 32.

<sup>67</sup> C-311/18 (Schrems II), punkt 135.

<sup>68</sup> Vt ELi põhiõiguste harta artiklid 47 ja 52, isikuandmete kaitse üldmääruse artikli 23 lõige 1 ja Euroopa Andmekaitseõukogu soovitused Euroopa oluliste tagatiste kohta seoses järelevalvemeetmetega.

andmete seas andmesubjektide poolt teistes kontekstides kasutatavate seadmete, rakenduste, vahendite ja protokollide antud võrguidentifikaatoreid.

75. Kolmandate riikide avaliku sektori asutused võivad üritada saada edastatud andmetele juurdepääsu järgmisega.
- a) Edastamise ajal, kasutades juurdepääsu andmete vastuvõtvasse riiki ülekandmise sideliinidele. See juurdepääs võib olla passiivne, mis juhul side sisu lihtsalt kopeeritakse, võib-olla pärast valikuprotsessi. See võib siiski olla ka aktiivne selles mõttes, et avaliku sektori asutused sekkuvad sideprotsessi peale sisu lugemise seda ka muutes või sellest osa varjates.
  - b) Kui andmed on ettenähtud vastuvõtja valduses, saades juurdepääsu kas töötluskohta endasse või nõudes andmete vastuvõtjalt huvipakkuvate andmete asukoha määramist ja eraldamist ning ametiasutustele üleandmist.
76. Siin punktis käsitletakse stsenaariume, milles rakendatakse mõlemal juhul tõhusaid meetmeid. Konkreetse edastamise korral võivad piisavad olla mitmesugused täiendavad meetmed, kui vastuvõtva riigi õigus näeb ette ainult üht liiki juurdepääsu. Seega peab andmeeksportija koostöös andmeimportijaga hoolega analüüsima viimase suhtes kehtivaid kohustusi.

Näide: Ameerika Ühendriikide andmeimportijad, kes kuuluvad Ameerika Ühendriikide seadustiku 50. jaotise paragrahvi 1881a (FISA paragrahv 702) kohaldamisalasse, on otseselt kohustatud andma juurdepääsu enda valduses või kontrolli all olevatele imporditud isikuandmetele või andma need andmed üle. See võib laieneda mis tahes krüptovõtmetele, mida on vaja andmete loetavaks muutmiseks.

77. Stsenaariumides kirjeldatakse konkreetseid asjaolusid ja võetud meetmeid. Stsenaariumide mis tahes muutmisega võib viia teistsuguste järeldusteni.
78. Võib juhtuda, et vastutavad töötledjad peavad rakendama osa või kõiki selles dokumendis kirjeldatud meetmeid, olenemata andmeimportija suhtes kohaldatavates õigusaktides sätestatud kaitsetasemest, sest neid on vaja isikuandmete kaitse üldmääruse artiklite 25 ja 32 järgimiseks konkreetsete edastamise asjaolude korral. Teisisõnu võib andmeeksportijatel olla kohustus rakendada käesolevas lisas kirjeldatud meetmeid isegi siis, kui andmeimportija on hõlmatud kaitse piisavuse otsusega, samamoodi nagu vastutavatel töötledajatel ja volitatud töötledajatel võib olla kohustus rakendada neid andmete töötlemisel EMP piires.

1. kasutusjuhtum: andmete talletamine varundamiseks ja muudel eesmärkidel, milleks ei ole vaja juurdepääsu krüptimata andmetele

79. Andmeeksportija kasutab hostimisteenuse pakkujat kolmandas riigis, et talletada isikuandmeid näiteks varundamiseks.

Kui

- 1. isikuandmeid töödeldakse enne edastamist tugevat krüptimist kasutades,
- 2. krüptimisalgoritm ja selle parameetrid (nt võtme pikkus ja töörežiim, kui asjakohane) vastavad tehnika tipptasemele ja eeldatavasti taluvad vastuvõtva riigi avaliku sektori asutuste tehtavat krüptoanalüüsi, arvestades neile kättesaadavaid ressursse ja tehnilisi võimalusi (näiteks arvutusvõimsus jõuründe jaoks),

3. krüptimise tugevus arvestab konkreetset ajavahemikku, mille vältel peab krüptitud isikuandmete konfidentsiaalsus olema kaitstud,
4. krüptimisalgoritmi rakendab täiuslikul viisil nõuetekohaselt hooldatud tarkvara, mille vastavus valitud algoritmi nõuetele on verifitseeritud näiteks sertifitseerimisega,
5. võtmehaldus (loomine, kasutamine, talletamine, kui asjakohane, sidumine kavandatud vastuvõtja identiteediga, tühistamine) on usaldusväärne ning
6. võtmeid säilitatakse ainult andmeeksportija või teiste selleks volitatud üksuse kontrolli all EMPs või kolmandas riigis, territooriumil või ühes või mitmes kolmanda riigi kindlaks määratud sektoris või rahvusvahelises organisatsioonis, mille kohta on komisjon kooskõlas isikuandmete kaitse üldmääruse artikliga 45 kindlaks teinud, et piisav kaitsetase on tagatud,

siis on Euroopa Andmekaitse nõukogu seisukohal, et tehtav krüptimine on tõhus täiendav meede.

## 2. kasutusjuhtum: pseudonüümitud andmete edastamine

80. Kõigepealt anonüümib andmeeksportija enda hoitavad andmed ning edastab need seejärel kolmandasse riiki analüüsimiseks, näiteks teadusuuringuteks.

Kui

1. andmeeksportija edastab sellisel viisil töödeldud isikuandmeid, et isikuandmeid ei saa enam täiendavat teavet kasutamata seostada konkreetse andmesubjektiga ega eristada andmesubjekti suuremast rühmast,<sup>69</sup>
2. seda täiendavat teavet säilitab ainult andmeeksportija liikmesriigis või kolmandas riigis, territooriumil või ühes või mitmes kolmanda riigi kindlaks määratud sektoris või rahvusvahelises organisatsioonis, mille kohta komisjon on kooskõlas isikuandmete kaitse üldmääruse artikliga 45 kindlaks teinud, et piisav kaitsetase on tagatud,
3. selle täiendava teabe avaldamine või volitamata kasutamine on välistatud asjakohaste tehniliste ja korralduslike kaitsemeetmetega ning on tagatud, et andmeeksportijale jääb ainukontroll selle täiendava teabe abil taastuvastamist võimaldava algoritmi või hoidla üle, ning
4. vastutav töötleja on tõestanud asjaomaste andmete põhjaliku analüüsiga ja arvestades kogu teavet, mida vastuvõtva riigi avaliku sektori asutused võivad omada, et pseudonüümitud isikuandmeid ei saa seostada tuvastatud või tuvastatava füüsilise isikuga isegi sellise teabega ristviitamise kaudu,

siis on Euroopa Andmekaitse nõukogu seisukohal, et tehtav pseudonüümimine on tõhus täiendav meede.

81. NB! Sageli võivad füüsilise isiku füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse identiteediga seotud tegurid, isiku asukoht või suhtlus internetipõhise teenusega teatud hetkedel<sup>70</sup> võimaldada isiku tuvastamist isegi nime, aadressi või muude lihtsate tuvastustunnuste puudumisel.

<sup>69</sup> Kooskõlas isikuandmete kaitse üldmääruse artikli 4 lõikega 5: pseudonüümimine on „isikuandmete töötlemine sellisel viisil, et isikuandmeid ei saa enam täiendavat teavet kasutamata seostada konkreetse andmesubjektiga, tingimusel et sellist täiendavat teavet hoitakse eraldi ja andmete tuvastatud või tuvastatava füüsilise isikuga seostamise vältimise tagamiseks võetakse tehnilisi ja korralduslikke meetmeid“.

<sup>70</sup> Isikuandmete kaitse üldmääruse artikli 4 lõige 1: „isikuandmed“ – igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti“) kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada,



82. Eriti on see nii siis, kui andmed käsitlevad teabeteenuste kasutamist (pöördumise kellaeg, kasutatud funktsioonide järjekord, kasutatud seadme omadused jt). Selliste teenuste korral võib ka isikuandmete importijal olla kohustus tagada juurdepääs samadele enda jurisdiktsiooni avaliku sektori asutustele, kes pärast seda tõenäoliselt valdavad andmeid, kas ja kuidas nende uuritav(ad) isik(ud) on neid teabeteenuseid kasutanud.
83. Arvestades ka seda, et teatud teabeteenuste kasutamine on olemuselt avalik või suurte ressurssidega pooled võivad neid ära kasutada, peavad vastutavad töötajad olema eriti hoolikad, sest nende jurisdiktsiooni avaliku sektori asutused valdavad tõenäoliselt andmeid, kas ja kuidas nende uuritav isik on neid teabeteenuseid kasutanud.

### 3. kasutusjuhtum: krüptitud andmed, mis kolmandat riiki ainult läbivad

84. Andmeeksportija soovib edastada andmeid isikuandmete kaitse üldmääruse artikli 45 kohaselt piisavat kaitset pakkuvana tunnustatud sihtkohta. Andmed suunatakse läbi kolmanda riigi.

Kui

1. andmeeksportija edastab isikuandmeid andmete piisavat kaitset tagavas jurisdiktsioonis asuvale andmeimportijale, andmeid teisaldatakse interneti kaudu ning andmeid võidakse suunata geograafiliselt läbi kolmanda riigi, mis ei taga sisuliselt samaväärsel tasemel kaitset,
2. kasutatakse krüptitud edastust, mille suhtes on tagatud, et kasutatavad krüptimisprotokollid on tiptasemel ja tagavad tõhusa kaitse teadaolevalt kolmanda riigi avaliku sektori asutuste käsutuses olevate ressurssidega võimalike aktiiv- ja passiivrünnete vastu,
3. dekrüptimine on võimalik ainult väljaspool asjaomast kolmandat riiki,
4. side pooled lepivad kokku usaldusväärse avaliku võtme sertifitseerimisasutuse või -taristu kasutamise,
5. krüptitud edastuse vastaste aktiiv- ja passiivrünnete vastu kasutatakse konkreetseid tiptasemel kaitsemeetmeid,
6. kui krüptitud edastus ise ei taga piisavat turvet, arvestades kogemusi kasutatava taristu või tarkvara haavatavustega, otspunktkrüptitakse isikuandmed ka rakenduskihil, kasutades tiptasemel krüptimismeetodeid,
7. krüptimisalgoritm ja selle parameetrid (nt võtme pikkus ja töörežiim, kui asjakohane) vastavad tehnika tiptasemele ja eeldatavasti taluvad vastuvõtva riigi avaliku sektori asutuste tehtavat krüptoanalüüsi, arvestades neile kättesaadavaid ressursse ja tehnilisi võimalusi (näiteks arvutusvõimsus jõuründe jaoks),
8. krüptimise tugevus arvestab konkreetset ajavahemikku, mille vältel peab krüptitud isikuandmete konfidentsiaalsus olema kaitstud,
9. krüptimisalgoritmi rakendab täiuslikul viisil nõuetekohaselt hooldatud tarkvara, mille vastavus valitud algoritmi nõuetele on verifitseeritud näiteks sertifitseerimisega,
10. tagauste olemasolu (riist- või tarkvaras) on välistatud,
11. eksportija või tema volitatud üksuse võtmehaldus (loomine, kasutamine, talletamine, kui asjakohane, sidumine kavandatud vastuvõtja identiteediga, tühistamine) sisuliselt samaväärset kaitset tagavas jurisdiktsioonis on usaldusväärne,

---

eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal;“.

siis on Euroopa Andmekaitsekoostöö rühma seisukohal, et krüptitud edastus (vajaduse korral koos sisu otspunktkrüptimisega) on tõhus täiendav meede.

#### 4. kasutusjuhtum: kaitstud vastuvõtja

85. Andmeeksportija edastab isikuandmeid kolmandas riigis asuvalle andmeimportijale, kes on selle riigi õigusega konkreetselt kaitstud, näiteks patsiendile ühiselt pakutava ravi jaoks või kliendile õigusteenuste pakkumiseks.

Kui

1. kolmanda riigi õigus vabastab residendist andmeimportija potentsiaalselt õigusvastasest juurdepääsust andmetele, mida see vastuvõtja hoiab nimetatud eesmärgil, näiteks andmeimportijale kohalduva ametisaladuse kohustuse alusel,
2. see vabastus laieneb andmeimportija valduses olevale kogu teabele, millega võidakse eirata privilegeeritud teabe (krüptovõtmed, salasõnad, muud pääsumandaadid jt) kaitset,
3. andmeimportija ei kasuta volitatud töötaja teenuseid viisil, mis võimaldaks avaliku sektori asutustel saada andmetele juurdepääsu nende volitatud töötaja valduses olemuse ajal, ega edasta isikuandmete kaitse üldmääruse artikli 46 alusel andmeid teisele kaitsmata üksusele,
4. isikuandmed krüptitakse enne edastamist tehnika tipptasemel oleva meetodiga, tagades, et dekrüptimine ei ole ilma dekrüptimisvõtmeaga võimalik (otspunktkrüptimine) kogu aja vältel, mil andmed peavad olema kaitstud,
5. dekrüptimisvõti on kaitstud andmete importija ainuvalduses ning tipptasemel tehniliste või korralduslike meetmetega asjakohaselt turvatud volitamata kasutuse või avaldamise eest,
6. andmeeksportija on usaldusväärselt tõestanud, et dekrüptimisvõti, mida ta kavatses kasutada, vastab vastuvõtja valduses olevale dekrüptimisvõtmele,

siis on Euroopa Andmekaitsekoostöö rühma seisukohal, et tehtav krüptitud edastus on tõhus täiendav meede.

#### 5. kasutusjuhtum: jagatud või ühistöötlus

86. Andmeeksportija soovib, et isikuandmeid töötleksid vähemalt kaks eri jurisdiktsioonides asuvat sõltumatut volitatud töötajat ühiselt ilma neile andmete sisu avaldamata. Enne edastamist jagab ta andmed nii, et mitte ükski ühe volitatud töötaja kätte jõudev osa ei ole isikuandmete täielikuks või osaliseks taastamiseks piisav. Andmeeksportija võtab töötlemise tulemuse vastu igalt volitatud töötajalt eraldi ning ühendab saadud osad, et saada lõpptulemus, mis võib sisaldada isiku- või koondandmeid.

Kui

1. andmeeksportija töötleb isikuandmeid nii, et see jagatakse vähemalt kahte ossa, millest ühtki ei saa täiendavate andmeteta enam tõlgendada ega seostada konkreetse andmesubjektiga,
2. iga osa edastatakse eri jurisdiktsioonis asuvalle erinevale volitatud töötajale,
3. volitatud töötajad töötlevad andmeid valikuliselt ühiselt, näiteks kasutades turvalist ühistöötlust nii, et ükski neist ei näe teavet, mida neil enne töötlust ei olnud,
4. ühistöötluse algoritm on aktiivsete rünnete suhtes turvaline,
5. puuduvad tõendid koostöö kohta vastavates iga volitatud töötaja asukoha jurisdiktsioonides asuvate avaliku sektori asutuste vahel, mis võimaldaks neil saada juurdepääsu volitatud töötajate

valduses olevatele kõigile isikuandmete kogumitele ja võimaldaks neil isikuandmete sisu taastada ja kasutada selges vormis, kui see kasutamine ei oleks kooskõlas andmesubjektide põhiõiguste ja -vabaduste olemusega; samamoodi ei tohiks ühegi riigi avaliku sektori asutustel olla volitusi juurdepääsuks kõigi asjaomaste jurisdiktsioonide volitatud töötajate valduses olevatele isikuandmetele,

6. vastutav töötaja on tõestanud asjaomaste andmete põhjaliku analüüsi alusel ja arvestades kogu teavet, mida vastuvõtivate riikide avaliku sektori asutused võivad omada, et isikuandmete osi, mida ta edastab volitatud töötajatele, ei saa seostada tuvastatud või tuvastatava füüsilise isikuga isegi sellise teabega ristviitamise kaudu,

siis on Euroopa Andmekaitsekoostöögrupi seisukohal, et tehtav jagatud töötlus on tõhus täiendav meedet.

---

### Stsenaariumid, mille korral *ei leitud* tõhusaid meetmeid

---

87. Allpool seose mõne stsenaariumiga kirjeldatud meetmed ei ole tõhusad kolmandatesse riikidesse edastatavatele andmetele sisuliselt samaväärse kaitse tagamisel. Seega ei kvalifitseeruks need täiendavate meetmetena.

6. kasutusjuhtum: edastamine pilveteenuste osutajatele või teistele töötajatele, kellel on vaja krüptimata juurdepääsu andmetele

88. Andmeksportija kasutab isikuandmete töötlemiseks kolmandas riigis vastavalt oma juhiste pilveteenuse osutajat või muud volitatud töötajat.

Kui

1. vastutav töötaja edastab andmeid pilveteenuse osutajale või muule volitatud töötajale,
2. pilveteenuse osutajal või muul volitatud töötajal on vaja määratud ülesande täitmiseks krüptimata juurdepääsu andmetele ning
3. vastuvõtva riigi avaliku sektori asutustele edastatud andmetele juurdepääsuks antud volitused ületavad seda, mis on demokraatlikus ühiskonnas vajalik ja proportsionaalne,<sup>71</sup>

siis ei suuda Euroopa Andmekaitsekoostöögrupi praegust tehnika tippaset arvestades näha ette tõhusat tehnilist meedet, mis takistaks sellise juurdepääsu korral andmesubjekti õiguste rikkumist. Euroopa Andmekaitsekoostöögrupi ei välista, et tulevikus võib tehnika arenedes ilmuda meetmeid, mis saavutavad kavandatud ärilised eesmärgid, vajamata krüptimata juurdepääsu.

89. Nendes stsenaariumides, milles on tehniliselt vaja krüptimata isikuandmeid, et volitatud töötaja saaks osutada teenust, ei ole isegi krüptitud edastus ja jõudeandmete krüptimine koos täiendav meede, mis tagaks sisuliselt samaväärse kaitse, kui krüptovõtmed on andmeimportija valduses.

---

<sup>71</sup> Vt ELi põhiõiguste harta artiklid 47 ja 52, isikuandmete kaitse üldmääruse artikli 23 lõige 1 ja Euroopa Andmekaitsekoostöögrupi soovitus Euroopa oluliste tagatiste kohta seoses järelevalvemeetmetega.

## 7. kasutusjuhtum: kaugjuurdepääs andmetele ärieesmärgil

90. Andmeeksportija teeb isikuandmed kolmandas riigis asuvatele üksustele kättesaadavaks kasutamiseks ühistel ärieesmärkidel. Tüüpiline kombinatsioon võib koosneda liikmesriigi territooriumil asuvast vastutavast ja volitatud töötlejast, kes edastavad isikuandmeid samasse ettevõtete kontserni või ühises majandustegevuses osalevate ettevõtete rühma kuuluvale kolmanda riigi vastutavale või volitatud töötlejale. Andmeimportija võib näiteks kasutada vastu võetud andmeid personaliteenuste osutamiseks andmeeksportijale, milleks tal on vaja personalihalduse andmeid, või suhelda telefoni või e-posti kaudu andmeeksportija klientidega, kes elavad Euroopa Liidus.

Kui

1. andmeeksportija edastab isikuandmeid kolmandas riigis asuvale andmeimportijale, tehes selle kättesaadavaks ühiskasutatavas teabesüsteemis viisil, mis võimaldab importijal saada otsejuurdepääsu enda valitud andmetele, või edastades neid sideteenust kasutades otse, individuaalselt või hulgi,
2. importija kasutab krüptimata andmeid enda eesmärkidel,
3. vastuvõtva riigi avaliku sektori asutustele edastatud andmetele juurdepääsuks antud volitused ületavad seda, mis on demokraatlikus ühiskonnas vajalik ja proportsionaalne,

siis ei suuda Euroopa Andmekaitsekoostööühendus näha ette tõhusat tehnilist meetet, mis takistaks sellise juurdepääsu korral andmesubjekti õiguste rikkumist.

91. Nendes stsenaariumides, milles on tehniliselt vaja krüptimata isikuandmeid, et volitatud töötleja saaks osutada teenust, ei ole isegi krüptitud edastus ja jõudeandmete krüptimine koos täiendav meede, mis tagaks sisuliselt samaväärse kaitse, kui krüptovõtmed on andmeimportija valduses.

## Täiendavad lepingulised meetmed

92. Tavaliselt koosnevad sellised meetmed ühepoolsetest, kahepoolsetest või mitmepoolsetest<sup>72</sup> lepingulistest kohustustest.<sup>73</sup> Kui kasutatakse isikuandmete kaitse üldmääruse artikli 46 kohast edastusvahendit, sisaldab see enamasti juba mitut andmeeksportija ja andmeimportija (peamiselt lepingulist) kohustust, mille eesmärk on toimida isikuandmete kaitsemeetmena.<sup>74</sup>
93. Mõnes olukorras võivad need meetmed täiendada ja tugevdada kaitsemeetmeid, mida võivad tagada edastusvahend ja kolmanda riigi asjakohased õigusaktid, kui need ei vasta edastamise asjaolusid arvestades kõigile tingimustele, mida on vaja, et tagada ELis tagatuga sisuliselt samaväärne kaitsetase. Arvestades lepinguliste meetmete olemust, mis üldiselt ei saa olla siduvad vastava kolmanda riigi ametiasutustele, kui nad ei ole lepingu pooled<sup>75</sup>, tuleb kombineerida need meetmed teiste tehniliste ja korralduslike meetmetega, et tagada nõutav andmekaitse tase. Neist ühe või mitme meetme

<sup>72</sup> Näiteks siduvate kontsernisisesete eeskirjade raames, mis peaksid alati reguleerima mõningaid allpool loetletud meetmeid.

<sup>73</sup> Need on olemuslikult eraõiguslikud ja neid ei käsitleta rahvusvahelises avalikus õiguses rahvusvaheliste lepingutena. Seega ei ole need tavaliselt siduvad kolmanda riigi avaliku sektori asutuste suhtes, kes ei ole kolmandate riikide eraõiguslike isikutega sõlmitud lepingute pooled, nagu kohus rõhutas otsuse C-311/18 (Schrems II) punktis 125.

<sup>74</sup> Vt otsuse C-311/18 (Schrems II) punkt 137, milles kohus tunnustas, et lepingu tüüpitingimus sisaldas „tõhusaid mehhanisme, mis praktikas võimaldavad tagada, et järgitakse liidu õigusega nõutava kaitse taset ja et selliste tingimuste alusel toimuv isikuandmete edastamine peatatakse või keelatakse juhul, kui neid tingimusi rikutakse või kui neid ei ole võimalik täita“; vt ka punkt 148.

<sup>75</sup> C-311/18 (Schrems II), punkt 125.

valimine ja rakendamine ei pruugi tingimata ja süstemaatiliselt tagada, et teie edastustoimingud vastavad ELi õigusega nõutavale sisulise samaväärsuse standardile.

94. Olenevalt sellest, mis lepingulised meetmed sisalduvad kasutatavas isikuandmete kaitse üldmääruse artikli 46 kohases edastusvahendis, võivad ka täiendavad lepingulised meetmed aidata EMPs asuvatel andmeeksportijatel olla kursis kolmandatesse riikidesse edastatavate andmete kaitset mõjutavate uute suundumustega.
95. Nagu öeldud, ei suuda lepingulised meetmed välistada sellise Euroopa Andmekaitseõukogu Euroopa oluliste tagatiste standardile mittevastava kolmanda riigi õigusaktide kohaldamist juhtudel, kui õigusaktid kohustavad importijaid täitma avaliku sektori asutustelt saadud andmete avaldamise korraldusi.<sup>76</sup>
96. Mõni selliste potentsiaalsete lepinguliste meetmete näide on allpool ja jaotatud olemuse järgi.

#### Lepingukohustuses konkreetsete tehniliste meetmete kasutamise sätestamine

97. ***Olenevalt edastamise konkreetsetest asjaoludest võib olla vaja sätestada lepingus, et edastamise toimumiseks tuleb kasutada konkreetseid tehnilisi meetmeid (vt soovitatavad tehnilised meetmed eespool).***

98. ***Tõhususe eeldused***

- See tingimus võib olla tõhus olukordades, kus eksportija on tuvastanud tehniliste meetmete vajaduse. See tuleb sätestada juriidiliselt, tagamaks, et ka importija kohustub võtma vajaduse korral asjakohaseid tehnilisi meetmeid.

#### Läbipaistvuskohustused

99. ***Eksportija võib lisada lepingule lisad teabega, mida importija peab oma parimate võimaluste järgi esitama seoses juurdepääsuga andmetele avaliku sektori asutuste poolt, sealhulgas luure valdkonnas, kui sihtriigi õigusaktid on kooskõlas Euroopa Andmekaitseõukogu Euroopa oluliste tagatistega. See võib aidata andmeeksportijal täita kohustust dokumenteerida oma hindamine kolmanda riigi kaitsetaseme kohta.***
100. Näiteks võib nõuda importijalt järgmist:

(1) sihtriigis importija või tema volitatud (alam)töötleja suhtes kohaldatavate eeskirjade loetlemine, mis võimaldavad avaliku sektori asutuste juurdepääsu edastatavatele isikuandmetele, eelkõige luure, õiguskaitse ning edastatavate andmete suhtes kohaldatava haldus- ja regulatiivjärelevalve valdkonnas;

(2) kui ei ole õigusakte, millega reguleeritakse avaliku sektori asutuste juurdepääsu andmetele, siis teabe ja statistika esitamine importija kogemuste või eri allikate alusel (näiteks partnerid, avalikud allikad, riiklik kohtupraktika ja järelevalveorganite otsused, käsitledes avaliku sektori asutuste juurdepääsu isikuandmetele olukordades, mis vastavad edastatavate andmete olemusele (st konkreetsetes järelevalvevaldkonnas; seoses asutuse tüübiga, mille hulka andmeimportija kuulub jne);

---

<sup>76</sup> Euroopa Kohtu otsus C-311/18 (Schrems II), punkt 132.

(3) märkimine, mis meetmetega takistatakse juurdepääsu edastatavatele andmetele (kui olemas);

(4) piisavalt üksikasjaliku teabe esitamine kõigi avaliku sektori asutuste tehtud juurdepääsutaotluste kohta isikuandmetele, mille importija on saanud teatud ajavahemikus<sup>77</sup>, eriti eespool punktis 1 nimetatud valdkondades ning koos teabega saadud taotluste kohta, taotletud andmete, taotleva organi ning avaldamise õigusliku aluse ja selle kohta, mis ulatuses on importija avaldanud küsitud andmeid;<sup>78</sup>

(5) täpsustamine, kas ja mis ulatuses on importijal seaduslikult keelatud esitada punktides 1–5 nimetatud teavet.

101. Seda teavet võib esitada liigendatud küsimustikes, mida importija täidab ja allkirjastab, ning tugevdada importija lepingulise kohustusega teatada ettenähtud aja jooksul igast selle teabe võimalikust muutusest, nagu on praegune tava seoses hoolsuskohustuse protsessidega.

#### 102. *Tõhususe eeldused*

- Importija peab suutma esitada seda tüüpi teavet eksportijale oma parimate teadmiste alusel ning olles teinud võimalikult palju selle saamiseks.<sup>79</sup>

- See importijale määratud kohustus on vahend, mis tagab, et eksportija saab teada kolmandasse riiki andmete edastamise riskid ja püsib nendega kursis. Seega võimaldab see eksportijal hoiduda lepingu sõlmimisest või juhul, kui teave pärast lepingu sõlmimist muutub, täita oma kohustus peatada edastamine ja/või lõpetada leping, kui kolmanda riigi õigus, kasutatava isikuandmete kaitse üldmääruse artikli 46 kohases edastusvahendis sisalduvad kaitsemeetmed ning võimalikud lisakaitsemeetmed, mida eksportija võib olla kasutusele võtnud, ei saa enam tagada ELiga sisuliselt samaväärset kaitset. Selle kohustusega ei saa importija samas põhjendada isikuandmete avaldamist ja selle alusel ei saa eeldada, et uusi juurdepääsutaotlusi ei tule.

\*\*\*

103. ***Samuti võib eksportija lisada tingimusi, mille alusel importija kinnitab, et 1) ta ei ole loonud tahtlikult tagauksi ega sarnast programmiosa, mida saaks kasutada süsteemile ja/või isikuandmetele juurdepääsuks; 2) ta ei ole tahtlikult loonud ega muutnud tööprotsesse nii, et see võimaldaks juurdepääsu isikuandmetele või süsteemidele; ning 3) riiklik õigus ega valitsuse poliitika ei nõua importijalt tagauste loomist või hoidmist ega juurdepääsu võimaldamist isikuandmetele või süsteemidele ega seda, et importija valdaks krüptovõtit või annaks selle edasi.***<sup>80</sup>

#### 104. *Tõhususe eeldused*

- Selliste õigusaktide või valitsuse poliitikate olemasolu, mis ei võimalda importijatel sellist teavet avaldada, võib muuta selle tingimuse ebatõhusaks. Sel juhul ei saa importija lepingut sõlmida või peab teatama eksportijale, et ta ei suuda täita oma lepingulisi kohustusi.<sup>81</sup>

<sup>77</sup> Perioodi pikkus peab sõltuma asjaomase edastamisega hõlmatud andmesubjektide õigustele ja vabadustele tekkivast riskist – näiteks viimane aasta enne andmete eksportimise vahendi sulgemist andmeeksportijaga.

<sup>78</sup> Selle kohustuse täitmine ei tähenda iseenesest piisaval tasemel kaitse tagamist. Samas tekitab mis tahes tegelikult toimunud sobimatu andmete avaldamisega vajadus rakendada täiendavaid meetmeid.

<sup>79</sup> Vt punkt 32.5 eespool.

<sup>80</sup> See tingimus on oluline, et tagada edastatavatele isikuandmetele piisav kaitse, ning tavaliselt tuleb seda nõuda.

<sup>81</sup> Vt punkt 32.5 eespool.

- Leping peab sisaldama karistusi ja/või eksportija võimalust lõpetada leping lühiajalise etteteatamisega juhtudel, kui importija ei avalda tagaukse või muu sarnase programmiosa või manipuleeritud tööprotsesside või neist mõne rakendamise kohustuse olemasolu või ei teata eksportijale kohe selliste võtete olemasolust teadasaamisest.

\*\*\*

105. ***Eksportija võib tugevdada oma volitusi importija andmetöötluskohtade auditeerimiseks<sup>82</sup> või kontrollimiseks kohapeal ja/või eemalt, et kontrollida, kas avaliku sektori asutustele on andmeid avaldatud ja mis tingimustel (juurdepääs, mis ei ületa demokraatlikus ühiskonnas vajalikku ja proportsionaalset), sätestades näiteks lühikese teatamisaja ning mehhanismid, mis tagavad kontrolliorganite kiire sekkumise ja tugevdavad eksportija autonoomsust kontrolliorganite valimisel.***

106. ***Tõhususe eeldused***

- Täieliku tõhususe saavutamiseks peab auditi ulatus juriidiliselt ja tehniliselt hõlmama kogu kolmandatesse riikidesse edastatavate isikuandmete töötlemist, mida teevad importija volitatud töötlejad ja alamtöötlejad.

- Pääsulogid ja muud sarnased jäljed peavad olema rikkumiskindlad, et audiitorid saaksid leida avaldamise kohta tõendeid. Pääsulogid ja muud sarnased jäljed peavad eristama ka korraldest töötoimingutest tulenevat juurdepääsu ning juurdepääsu, mis tulenevad korraldustest või juurdepääsunõuetest.

\*\*\*

107. ***Kui eksportija on algselt hinnanud importija kolmanda riigi õigusakte ja praktikat ning pidanud need ELis edastatavatele andmetele sätestatud kaitsega sisuliselt samaväärset kaitset tagavaks, võib eksportija sellegipoolest tugevdada andmeimportija kohustust teatada andmeeksportijale viivitamata oma suutmatusest täita lepingulisi kohustusi ning sellest tulenevalt ka nõutavat „sisuliselt samaväärset tasemel andmekaitse“ standardit.<sup>83</sup>***

108. Selline suutmatus kohustusi täita võib tuleneda kolmanda riigi õigusaktide või praktika muutumisest.<sup>84</sup> Tingimustega võib määrata konkreetsed ja ranged tähtajad ja menetlused andmeedastuse kiire peatamise ja/või lepingu lõpetamise ning selle kohta, millal importija peab saadud andmed tagastama või kustutama. Saadud taotluste, nende ulatuse ja neile suhtes võetud vastumeetmete tõhususe jälgimine annab eksportijale piisavalt viiteid andmeedastus peatada või lõpetada ja/või leping lõpetada.

---

<sup>82</sup> Vt näiteks otsuses 2010/87/EL vastutavate töötlejate ja volitatud töötlejate vaheliste lepingu tüüptingimuste 5. tingimuse punkt f; auditeid saab sätestada ka toimumisjuhendis või sertifitseerimise kaudu.

<sup>83</sup> Lepingu tüüptingimuste otsuse 2010/87/EÜ 5. tingimuse punkt a ja punkti d alapunkt i.

<sup>84</sup> Vt C-311/18 (Schrems II), punkt 139, milles kohus rõhutab, et „Kuigi 5. tingimuse punkti d alapunkt i võimaldab vastuvõtjal, kellele isikuandmed edastatakse, selliste õigusaktide alusel, millest tuleneb näiteks uurimissaladuse hoidmiseks kehtiv kriminaalmenetluslik keeld, jätta teatamata liidus asuvale vastutavale töötlejale õiguskaitseorganite õiguslikult siduvatest taotlustest isikuandmete avaldamiseks, on ta 5. tingimuse punkti a alusel siiski kohustatud teavitama vastutavat töötlejat asjaolust, et tal on võimatu andmekaitse tüüptingimusi täita.“

#### 109. **Tõhususe eeldused**

- Teatamine peab toimuma enne andmete juurdepääsu lubamist. Vastasel juhul võivad ajaks, kui eksportija saab teate, olla üksikisiku õigused juba rikutud, kui taotluse aluseks on selle kolmanda riigi õigusaktid, mis ületavad ELi õigusega tagatud andmekaitse taset. Teade võib sellegipoolest aidata ennetada rikkumisi tulevikus ning võimaldada eksportijal täita oma kohustust peatada isikuandmete edastamine kolmandasse riiki ja/või lõpetada leping.
- Andmeimportija peab jälgima kõiki juriidilisi ja poliitilisi suundumusi, mis võiksid tekitada tema suutmatuse täita kohustusi, ning kõigist sellistest muudatustest ja suundumustest kohe teatama andmeeksportijale, võimaluse korral enne nende rakendamist, et andmeeksportija saaks andmed andmeimportijalt tagasi.
- Tingimustes tuleb sätestada kiirmehhanism, mille alusel andmeeksportija volitab andmeimportijat andmeid kohe turvama või tagastama need andmeeksportijale või (kui see ei ole otstarbekas) ilma eksportija juhiseid tingimata ootamata andmed kustutama või turvaliselt krüptima, kui on jõutud andmeeksportija ja andmeimportija vahel kokku lepitud spetsiaalse künniseni. Importija peab rakendama seda mehhanismi andmete alates edastamise algusest ja testima seda regulaarselt, et tagada, et seda saab rakendada lühikese etteteatamisega.
- Teised tingimused võivad anda eksportijale võimaluse jälgida auditite, kontrollide ja teiste kontrollimeetmete abil, kuidas importija neid kohustusi täidab, ning jõustada kohustusi importijale määratavate karistuste ja/või eksportija võimaluse abil peatada andmete edastamine ja/või lõpetada kohe leping.

\*\*\*

110. ***Kui see on kolmandas riigis riikliku õigusega lubatud, võib leping tugevdada importija läbipaistvuskohustusi sellega, et sätestab regulaarse nõudekontrolli meetodi, mille kohaselt importija kohustub avaldama regulaarselt (näiteks iga 24 tunni järel) krüptograafiliselt allkirjastatud sõnumi, millega teavitab eksportijat, et konkreetse kuupäeva ja kellaaja seisuga ei ole ta saanud isikuandmete avaldamise korraldust ega muud taolist. Selle teate ajakohastamata jätmine näitab eksportijale, et importija võib olla saanud sellise korralduse.***

#### 111. **Tõhususe eeldused**

- Kolmanda riigi eeskirjad peavad võimaldama andmeimportijal saata sellises vormis passiivset teadet eksportijale.
- Andmeeksportija peab nõudekontrolli teateid automaatselt jälgima.
- Andmeimportija peab tagama, et tema nõudekontrolli teadete allkirjastamise privaatsust hoitakse turvaliselt ja teda ei saa kolmanda riigi eeskirjade alusel sundida väljastama ebaõigeid nõudekontrolli teateid. Selleks võib olla kasulik, kui on vaja mitme isiku allkirju ja/või nõudekontrolli teateid edastab väljaspool kolmanda riigi jurisdiktsiooni asuv isik.

#### Erimeetmete võtmise kohustused

112. ***Importija võib kohustuda vaadata sihtriigi õiguse kohaselt läbi mis tahes andmete avaldamise korralduse õiguspärasus, eelkõige seoses sellega, kas see jääb taotleva avaliku sektori asutuse volituste piiresse, ning vaidlustama korralduse juhul, kui ta järeldab hoolika hindamise järel, et sihtriigi õiguse kohaselt on selleks alused olemas. Korralduse vaidlustamise korral peab***



***andmeimportija taotlema ajutisi meetmeid korralduse mõju peatamiseks, kuni kohus on teinud selle põhjuste kohta otsuse. Importijal on kohustus mitte avaldada nõutavaid isikuandmeid, enne kui selleks tekib kohustus kohaldatavate menetluseeskirjade alusel. Samuti kohustub andmeimportija esitama korraldusele vastates minimaalne lubatav hulk teavet vastavalt korralduse mõistlikule tõlgendamisele.***

**113. Tõhususe eeldused**

- Kolmanda riigi õiguskord peab võimaldama tõhusaid juriidilisi võimalusi vaidlustada andmete avaldamise korraldusi.
- See tingimus pakub alati väga piiratud lisakaitset, sest andmete avaldamise korraldus võib olla kolmanda riigi õiguskorras seaduslik, kuid see õiguskord ei pruugi vastata ELi standarditele. See lepinguline meede peab kindlasti olema teisi lisameetmeid täiendav.
- Korralduste vaidlustamisel peab olema kolmanda riigi õiguse kohaselt peatav mõju. Vastasel korral on avaliku sektori asutustel jätkuvalt juurdepääs isikuandmetele ning igal järgmisel toimingul isiku kasuks oleks piiratud mõju, mis võimaldab tal nõuda hüvitist andmete avaldamisest tuleneva kahju eest.
- Importijal peab olema võimalus dokumenteerida ja tõendada eksportijale enda võimalikult ulatuslikku tegevust selle kohustuse täitmisel.

\*\*\*

**114. *Eespool kirjeldatuga samas olukorras võib importija kohustuda teavitada taotlevat avaliku sektori asutust korralduse sobimatusest isikuandmete kaitse üldmääruse artikli 46 kohases edastusvahendis sisalduvate kaitsemeetmetega<sup>85</sup> ning sellest tulenevast konfliktist importija kohustustega. Importija teavitab samal ajal ja niipea kui võimalik sellest eksportijat ja/või EMP pädevat järelevalveasutust, kui see on kolmanda riigi õiguskorras võimalik.***

**115. Tõhususe eeldused**

- Selline teade ELi õigusega loodava kaitse ja kohustuste konflikti kohta peaks olema kolmanda riigi õiguskorras teatud õigusliku tagajärjega, näiteks juurdepääsukorralduse või -taotluse kohtulik või halduskorras läbivaatamine, kohtumääruse nõue ja/või korralduse ajutine peatamine, et lisada andmetele mõningast kaitset.
- Kolmanda riigi õigussüsteem ei tohi keelata importijal teavitada eksportijat või vähemalt pädevat EMP järelevalveasutust saadud korraldusest või taotlusest.
- Importijal peab olema võimalus dokumenteerida ja tõendada eksportijale enda võimalikult ulatuslikku tegevust selle kohustuse täitmisel.

---

<sup>85</sup> Lepingu tüüptingimustes saab näiteks sätestada, et andmete töötlemine, sealhulgas andmete edastamine on toimunud ja toimub kooskõlas „kohaldatava andmekaitseõigusega“. See õigus on määratletud kui „õigusakt, mis kaitseb üksikisikute põhiõigusi ja -vabadusi ning eriti nende eraelu puutumatus õigust seoses isikuandmete töötlemisega ning mis on kohaldatav vastutava andmetöötaja suhtes liikmesriigis, kus andmeeksportija asub“. Euroopa Kohus kinnitab, et isikuandmete kaitse üldmääruse sätted tõlgendatuna ELi põhiõiguste hartast lähtuvalt moodustavad nende õigusaktide osa – vt kohtuotsus C-311/18 (Schrems II), punkt 138.

116. **Lepinguga võib sätestada, et tavapärase tööprotsessi (sealhulgas tugitegevuse) käigus lihttekstina edastatavatele isikuandmetele on juurdepääs võimalik ainult eksportija ja/või andmesubjekti selgesõnalisel või kaudsel nõusolekul.**

117. **Tõhususe eeldused**

- See tingimus võib olla tõhus olukordades, kus importija saab avaliku sektori asutuselt taotluse teha vabatahtlikku koostööd, erinevalt näiteks avaliku sektori asutuse juurdepääsust andmetele, mis toimub ilma andmeimportija teadmata või tema soovi vastaselt.
- Mõnes olukorras ei pruugi andmesubjektil olla võimalust vaidlustada juurdepääsu või anda nõusolek, mis vastab kõigile ELi õigusega sätestatud tingimustele (vabatahtlik, konkreetne, teadlik ja ühemõtteline) (näiteks töötajate korral).<sup>86</sup>
- Riiklikud eeskirjad või poliitikad, mis sunnivad importijat juurdepääsukorraldust mitte avaldama, võivad muuta selle tingimuse ebatõhusaks, kui seda ei saa tagada tehniliste meetoditega, mis nõuavad lihttekstiandmetele juurdepääsuks eksportija või andmesubjekti sekkumist. Sellised tehnilised meetmed juurdepääsu piiramiseks võib näha ette eelkõige siis, kui juurdepääs antakse konkreetsetel tugitegevuse või teenuse osutamise juhtudel, kuid andmeid endid talletatakse EMPs.

\*\*\*

118. **Leping võib kohustada importijat ja/või eksportijat teatama kolmanda riigi avaliku sektori asutuselt saadud taotlusest või korraldusest või importija suutmatusest täita lepingulisi kohustusi kohe andmesubjektile, et ta saaks taotleda teavet ja tõhusat õiguskaitset (esitades näiteks kaebuse enda pädevale järelevalveasutusele ja/või kohtuasutusele ja tõendades oma õigustatud huvi kolmanda riigi kohtutes).**

119. **Tõhususe eeldused**

- Sellise teate abil võib hoiatada andmesubjekti kolmanda riigi avaliku sektori asutuste potentsiaalsest juurdepääsust tema andmetele. Seega võib see anda andmesubjektile võimaluse taotleda eksportijalt lisateavet ning esitada kaebus enda pädevale järelevalveasutusele. Samuti võib see tingimus lahendada mõne raskuse, mis võivad üksikisikul tekkida enda õigustatud huvi (*locus standi*) tõendamisel kolmanda riigi kohtutes, vaidlustamaks avaliku sektori asutuste juurdepääsu tema andmetele.
- Riiklikud eeskirjad ja poliitikad võivad välistada sellise teate saatmise andmesubjektile. Sellegipoolest võivad eksportija ja importija kohustuda teavitama andmesubjekti kohe, kui andmete avaldamise piirangud tühistatakse, ning teha kõik, et saada vabastus avaldamise keelust. Minimaalse sammuna võib eksportija või pädev järelevalveasutus teatada andmesubjektile tema isikuandmete edastamise peatamisest või lõpetamisest tulenevalt importija suutmatusest täita juurdepääsu taotluse saamise tõttu oma lepingulisi kohustusi.

\*\*\*

---

<sup>86</sup> Isikuandmete kaitse üldmääruse artikli 4 lõige 11.

120. ***Leping võib kohustada eksportijat ja importijat abistama spetsiaalsete õiguskaitse mehhanismide ja õigusnõustamise abil andmesubjekti tema õiguste kasutamisel kolmanda riigi jurisdiktsioonis.***

121. ***Tõhususe eeldused***

- Riiklikud eeskirjad ja poliitikad võivad kehtestada tingimusi, mis võivad kahjustada sätestatud spetsiaalsete õiguskaitse mehhanismide tõhusust.
- Andmesubjektile võib abi olla õigusnõustamisest, eriti kui arvestada, kui keerukas ja kulukas võib tema jaoks olla kolmanda riigi õigussüsteemi mõistmine ja kohtumenetluses osalemine välismaalt ja tõenäoliselt võõrkeeles. See tingimus pakub siiski alati piiratud lisakaitset, sest abi ja õigusnõustamise pakkumine andmesubjektidele ei saa iseenesest heastada kolmanda riigi õigussüsteemi suutmatust tagada ELis tagatuga sisuliselt samaväärset kaitsetaset. See lepinguline meede peab kindlasti olema teisi lisameetmeid täiendav.

See täiendav meede oleks tõhus ainult siis, kui kolmanda riigi õigus näeb ette õiguskaitse oma riiklikes kohtutes või kui on olemas spetsiaalne õiguskaitse mehhanism. Igal juhul ei oleks see piisav täiendav meede jälitusmeetmete vastu ilma õiguskaitse mehhanismideta.

### Korralduslikud meetmed

122. Täiendavad korralduslikud meetmed võivad koosneda sisepoliitikatest, korralduslikest meetoditest ja standarditest, mida võivad vastutavad töötlejad ja volitatud töötlejad kohaldada enda suhtes ja kehtestada kolmandates riikides asuvatele andmeimportijatele. Need võivad toetada isikuandmete kaitse järjepidevuse tagamist kogu töötlemistsükli vältel. Samuti võivad korralduslikud meetmed parandada eksportijate teadlikkust riskist ja kolmandates riikides tehtavatest üritustest saada andmetele juurdepääs ning nende võimekusest nendele reageerida. Neist ühe või mitme meetme valimine ja rakendamine ei pruugi tingimata ja süstemaatiliselt tagada, et teie edastustoimingud vastavad ELi õigusega nõutavale sisulise samaväärsuse standardile. Olenevalt konkreetsetest edastamise asjaoludest ja kolmanda riigi õigusaktide hinnangust võib korralduslike meetmeid olla vaja lepinguliste ja/või tehniliste meetmete täiendamiseks, et tagada isikuandmetele ELis tagatuga sisuliselt samaväärne kaitsetase.
123. Sobivaimad meetmed tuleb leida juhtumipõhisel hindamisel, arvestades vastutavate töötlejate ja volitatud töötlejate vajadust järgida vastutuse põhimõtet. Allpool esitab Euroopa Andmekaitsekoogu korralduslike meetmete mõne näite, mida eksportijad võivad kasutada, kuigi loetelu ei ole ammendav ja sobida võivad ka muud meetmed.

### Edastamise haldamise sisepoliitika, eelkõige ettevõtete kontsernide korral

124. ***Piisavate sisepoliitika vastuvõtmine, milles selgelt nimetatakse andmete edastamisega seotud vastutusosalad, teavituskanalid ja standardmenetlused juhtudeks, kui avaliku sektori asutused taotlevad varjatult või ametlikult andmetele juurdepääsu. Eriti ettevõtete kontsernide vaheliste edastustoimingute korral võivad need poliitikad sisaldada muu hulgas konkreetse EMPs asuva ning infotehnoloogia, andmekaitse- ja privaatsusõiguse ekspertidest koosneva rühma nimetamist, kes käsitleb ELis edastatud isikuandmetega seotud taotlusi; selliste taotluste saamise korral kontserni tippjuristidele ja juhtkonnale ning andmeeksportijale teatamist; menetlussamme ebaproportsionaalsete ja ebaseaduslike taotluste vaidlustamiseks ning läbipaistva teabe andmist andmesubjektidele.***

125. Konkreetsete koolitustegevuste väljatöötamine avaliku sektori asutustest saadavate isikuandmetele juurdepääsu taotlusi käsitlevatele töötajatele, mida tuleb regulaarselt ajakohastada, et arvestada kolmanda riigi ja EMP õigusloome ja kohtupädevuse uusi suundumusi. Koolitustegevused peavad hõlmama ELi õiguse nõudeid seoses avaliku sektori asutuste juurdepääsuga isikuandmetele, eriti vastavalt põhiõiguste harta artikli 52 lõikele 1. Töötajate teadlikkust tuleb suurendada, kasutades eelkõige praktilisi näiteid avaliku sektori asutuste taotluste kohta andmetele juurdepääsuks ning kohaldades nende näidete suhtes põhiõiguste harta artikli 52 lõikest 1 tulenevat standardit. See koolitus peaks arvestama eelkõige andmeimportija olukorda, näiteks kolmanda riigi õigusakte ja eeskirju, mis tema suhtes kohalduvad, ning see tuleb koostada võimaluse korral koostöös andmeeksportijaga.

126. **Tõhususe eeldused**

- Neid poliitikaid võib näha ette ainult juhtudeks, kui kolmanda riigi avaliku sektori asutuste taotlus on kooskõlas ELi õigusega.<sup>87</sup> Kui taotlus ei ole kooskõlas, ei piisa neist poliitikatest, et tagada isikuandmete samaväärne kaitse, ning edastamine tuleb, nagu märgitud eespool, peatada või rakendada asjakohaseid täiendavaid meetmeid juurdepääsu takistamiseks.

Läbipaistvuse ja vastutuse tagamise meetmed

127. ***Avaliku sektori asutustelt saadud juurdepääsutaotluste ja antud vastuste dokumenteerimine ja registreerimine koos õigusliku põhjenduse ja seotud pooltega (näiteks kas eksportijat on teavitatud ja tema vastus, selliseid taotlusi käsitleva talituse hinnang jne). Need dokumendid tuleb teha kättesaadavaks andmeeksportijale, kes esitab selle vajaduse korral asjaomastele andmesubjektidele.***

128. **Tõhususe eeldused**

- Kolmanda riigi riiklikud õigusaktid võivad keelata taotluste või selle olulise teabe avaldamise ning muuta selle tava seega ebatõhusaks. Andmeimportija peab teavitama eksportijat oma suutmatusest esitada selliseid dokumente, andes seega eksportijale võimaluse peatada edastamine, kui see suutmatuse tekitab kaitsetaseme nõrgenemise.

\*\*\*

129. ***Läbipaistvusaruannete või kokkuvõtete regulaarne avaldamine valitsuse andmetele juurdepääsu taotluste ning antud vastuste kohta, kui see avaldamine on lubatud kohaliku õigusega.***

130. **Tõhususe eeldused**

- Esitatav teave peab olema asjakohane, selge ja võimalikult üksikasjalik. Kolmanda riigi riiklikud õigusaktid võivad keelata üksikasjaliku teabe avaldamise. Sellistel juhtudel peab andmeimportija tegema kõik, et avaldada statistilist või muud sarnast koondteavet.

---

<sup>87</sup> Vt kohtuasi C-362/14 (Schrems I), punkt 94; kohtuasi C-311/18 (Schrems II), punktid 168, 174, 175 ja 176.

## Korralduslikud meetodid ja võimalikult väheste andmete kogumise meetmed

131. **Edastamise kontekstis võivad olla kasulikud ka juba vastutuse põhimõtte alusel kasutusele võetud organisatsioonilised nõuded, näiteks range ja granulaarse andmetele juurdepääsu ning konfidentsiaalsuse poliitika ja parimad tavad, mille aluseks on range vajaduspõhisuse põhimõte ning mille üle tehakse regulaarsete auditite vormis järelevalvet ja mida jõustatakse distsiplinaarmedetega abil. Sellega seoses tuleb kaalutleda võimalikult väheste andmete kogumist, et piirata volitamata juurdepääsu isikuandmetele. Näiteks mõnikord ei pruugi olla vaja teatud andmeid edastada (näiteks kaugjuurdepääsul EMP andmetele tugitegevuste korral, kui täieliku juurdepääsu asemel antakse piiratud juurdepääs, või kui teenuse osutamiseks on vaja ainult piiratud andmekogumit, kuid mitte kogu andmebaasi).**

### 132. Tõhususe eeldused

- Võimalikult väheste andmete kogumise meetmete järelevalveks ja jõustamiseks ka edastamise kontekstis peavad kasutusel olema regulaarsed auditid ja mõjuvad distsiplinaarmedetmed.
- Andmeksportija peab enne edastamist hindama enda valduses olevaid isikuandmeid, et tuvastada andmekogumid, mida ei ole edastamise eesmärkide jaoks vaja ja mida seetõttu andmeimportijaga ei jagata.
- Võimalikult väheste andmete kogumise meetmetega peavad kaasnema tehnilised meetmed, mis tagavad, et volitamata juurdepääs andmetele puudub. Näiteks võib turvaliste ühistöötlusmehhanismide rakendamine ja krüptitud andmekogumite jagamine volitatud üksuste vahel olemuslikult ennetada, et ühepoolse juurdepääsuga kaasneks tuvastamist võimaldavate andmete avaldamine.

\*\*\*

133. **Parimate tavade väljatöötamine, et asjakohaselt ja õigel ajal kaasata ja anda juurdepääs teabele andmekaitseametnikule (kui olemas) ning õigus- ja siseaudititalitusele seoses isikuandmete rahvusvahelise edastamisega.**

### 134. Tõhususe eeldused

- Andmekaitseametnikule (kui olemas) ning õigus- ja siseaudititalitusele antakse kogu vajalik teave enne edastamist ning nendega konsulteeritakse edastamise vajalikkuse ja võimalike lisakaitsemeetmete teemal.
- Asjakohane teave peab sisaldama näiteks konkreetsete isikuandmete edastamise vajalikkuse hinnangut, kohaldatavate kolmanda riigi õigusaktide ülevaadet ning kaitsemeetmeid, mida importija kohustub rakendama.

## Standardite ja parimate tavade vastuvõtmine

135. **Rangete andmeturbe- ja andmeprivaatsuspoliitikate vastuvõtmine ELi sertifikaadi või toimimisjuhendite või rahvusvaheliste standardite (näiteks ISO normide) ja parimate tavade (näiteks ENISA) alusel, arvestades tehnika taset, kooskõlas töödeldavate andmekategooriate riski ja tõenäosusega, et avaliku sektori asutused püüavad saada sellele juurdepääsu.**

Muu

136. *Sisepoliitikate vastuvõtmine rakendatud täiendavate meetmete sobivuse hindamiseks ning vajaduse korral uute või alternatiivsete lahenduste tuvastamiseks ja rakendamiseks, samuti nende poliitikate regulaarne ajakohastamine, et tagada edastatavate isikuandmete ELis tagatuga samaväärse kaitsetaseme säilimine.*

\*\*\*

137. *Andmeimportija kohustused mitte saata isikuandmeid edasi samas kolmandas riigis või teistesse kolmandatesse riikidesse või peatada edastamine, kui kolmandas riigis ei ole võimalik tagada ELis tagatuga samaväärset isikuandmete kaitset.<sup>88</sup>*

---

<sup>88</sup> C-311/18 (Schrems II), punktid 135 ja 137.

### 3. LISA. VÕIMALIKUD TEABEALLIKAD KOLMANDA RIIGI HINDAMISEKS

138. Teie andmeimportijal võib olla võimalus esitada teile asjakohaseid allikaid ja teavet enda asukohaks oleva kolmanda riigi ja tema suhtes kohaldatavate õigusaktide kohta. Samuti võite kasutada muid teabeallikaid, näiteks muu hulgas allpool loetletud allikaid:

- Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu praktika<sup>89</sup>, millele viidatakse Euroopa oluliste tagatiste soovitus<sup>90</sup>;
- sihtriigi kaitse piisavuse otsused, kui edastamine tugineb muule õiguslikule alusele;<sup>91</sup>
- valitsusvaheliste organisatsioonide, näiteks Euroopa Nõukogu<sup>92</sup>, teiste piirkondlike organite<sup>93</sup> ning ÜRO organite ja asutuste (näiteks ÜRO Inimõiguste Nõukogu<sup>94</sup>, inimõiguste komitee<sup>95</sup>) resolutsioonid ja aruanded;
- riikide kohtupraktika või kolmandate riikide andmeprivaatsuse ja andmekaitse suhtes pädevate sõltumatute kohtu- või haldusasutuste otsused;
- akadeemiliste asutuste ning kodanikuühiskonna organisatsioonide (näiteks vabaühenduste ja kutseühingute) aruanded.

---

<sup>89</sup> Vt Euroopa Inimõiguste Kohtu teabedokument kohtupädevuse kohta seoses massilise jälitustegevusega: [https://www.echr.coe.int/Documents/FS\\_Mass\\_surveillance\\_ENG.pdf](https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf)

<sup>90</sup> <https://www.coe.int/en/web/data-protection/reports-studies-and-opinions>

<sup>91</sup> C-311/18 (Schrems II), punkt 141; vt kaitse piisavuse otsuseid aadressil [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_et](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_et)

<sup>92</sup> <https://www.coe.int/en/web/data-protection/reports-studies-and-opinions>

<sup>93</sup> Vt näiteks Ameerika Inimõiguste Komisjoni riigiaruanded, <https://www.oas.org/en/iachr/reports/country.asp>.

<sup>94</sup> Vt <https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx>.

<sup>95</sup> Vt

[https://tbinternet.ohchr.org/\\_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5)