Soovitused

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

Versioon 2.0

Vastu võetud 18. juunil 2021

Versiooniajalugu

Versioon 2.0.	18. juuni 2021	Soovituste vastuvõtmine pärast avalikku konsultatsiooni
Versioon 1.0	10. november 2020	Soovituste vastuvõtmine avalikuks konsulteerimiseks

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 standardsete andmekaitseklauslite kehtivust edastusvahendina, mis võib tagada kolmandatesse riikidesse edastatud andmetele lepingu alusel sisuliselt samaväärse kaitsetaseme.

Standardsed andmekaitseklauslid ega muud isikuandmete kaitse üldmääruse artiklis 46 nimetatud edastusvahendid ei toimi vaakumis. Kohus märgib, et eksportijatena tegutsevad vastutavad töötlejad ja volitatud töötlejad 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 töötlejad vastutaksid sama määruse isikuandmete töötlemisega seotud põhimõtete täitmise eest ja on võimelised seda tõendama.

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

Esimese sammuna soovitab Euroopa Andmekaitsenõukogu teil eksportijatena **tunda oma edastustoiminguid**. Kõigi isikuandmete kolmandatesse riikidesse edastamise juhtude uurimine võib olla keerukas ülesanne. Isikuandmete sihtkoha teadmist on siiski vaja selle tagamisel, 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 vaja nendeks eesmärkideks, milleks neid töödeldakse.

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 piisavuse otsus on jõus. Kui kaitse piisavuse otsus puudub, peate kasutama üht isikuandmete kaitse üldmääruse artiklis 46 loetletud edastusvahenditest. Ainult mõnel juhul võib olla võimalik kasutada üht isikuandmete kaitse üldmääruse artiklis 49 sätestatud eranditest, kui vastate selle tingimustele. Erandid ei saa praktikas muutuda reegliks, vaid neid tuleb piirata konkreetsete olukordadega.

Kolmanda sammuna tuleb **hinnata**, kas kolmanda riigi õiguses ja/või kehtivates tavades on midagi, mis võiks piirata teie kasutatavate edastusvahendite asjakohaste kaitsemeetmete tõhusust teie konkreetse edastustoimingu kontekstis. Teie hinnang peaks keskenduma eelkõige ja peamiselt kolmanda riigi õigusaktidele, mis on olulised teie andmeedastuse seisukohast, ja isikuandmete kaitse üldmääruse artikli 46 kohasele edastamisvahendile, millele te tuginete. Kolmanda riigi ametiasutuste

tavade uurimine võimaldab teil kontrollida, kas edastamisvahendis sisalduvad kaitsemeetmed suudavad tegelikkuses tagada edastatavate isikuandmete tõhusa kaitse. Nende tavade uurimine on teie hinnangu jaoks eriti oluline, kui:

(i.) kolmanda riigi õigusakte, mis vastavad ametlikult ELi standarditele, ilmselgelt ei kohaldata / ei täideta praktikas;

(ii.) esineb tavasid, mis on vastuolus edastusvahendi kohustustega, kui kolmandas riigis puuduvad asjakohased õigusaktid;

(iii.) teie edastatavad andmed ja/või importija kuuluvad või võivad kuuluda probleemsete õigusaktide kohaldamisalasse (st edastusvahendi lepingulise tagatise piiramine sisuliselt samaväärse kaitsetasemega ja mittevastamine põhiõigusi, vajalikkust ja proportsionaalsust käsitlevatele ELi standarditele).

Kahes esimeses olukorras peate edastamise peatama või võtma asjakohaseid täiendavaid meetmeid, kui soovite edastamist jätkata.

Kolmandas olukorras, arvestades ebakindlust seoses probleemsete õigusaktide võimaliku kohaldamisega teie andmeedastuse suhtes, võite otsustada: edastamise peatada, võtta täiendavaid meetmeid edastamise jätkamiseks või otsustada jätkata andmete edastamist ilma täiendavaid meetmeid võtmata, kui arvate ning suudate tõendada ja dokumenteerida, et teil ei ole põhjust uskuda, et asjakohaseid ja probleemseid õigusakte tõlgendatakse ja/või kohaldatakse praktikas nii, et need hõlmaksid teie edastatavaid andmeid ja importijat.

Et hinnata elemente, mida arvestada, kui hindate kolmanda riigi õigusakte, mis käsitlevad avaliku sektori asutuste juurdepääsu andmetele jälitustegevuse eesmärgil, tutvuge Euroopa Andmekaitsenõukogu Euroopa oluliste tagatiste soovitustega.

Peaksite hindamise teostama nõuetekohase hoolsusega ja seda põhjalikult dokumenteerima. Teie pädevad järelevalve- ja/või õigusasutused võivad seda nõuda ja võtta teid vastutusele kõigi selle alusel tehtud otsuste eest.

Neljas samm on **tuvastada ja võtta vastu 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 ja/või tavad piiravad isikuandmete kaitse üldmääruse artikli 46 kohase edastusvahendi tõhusust, mida kasutate või kavatsete kasutada oma edastustoimingu kontekstis. Siin soovitustes (2. lisas) 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. Olete kohustatud hindama nende tõhusust konkreetse edastamise kontekstis ning arvestades kolmanda riigi õigust ja tavasid ning kasutatavat edastusvahendit, sest teie vastutate iga selle alusel tehtud otsuse eest. 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 mõnda neist ametlikest nõuetest. Mõni võib vajada konsulteerimist pädevate järelevalveasutustega.

Kuuenda ja viimase sammuna tuleb sobivate ajavahemike järel **taashinnata** kolmandatesse riikidesse edastatavate isikuandmete kaitsetaset ning jälgida, kas on toimunud või tulemas arenguid, mis võivad seda mõjutada. Vastutuse põhimõte 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. Kohus tuletab meelde, et järelevalveasutused peatavad või keelavad 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 Andmekaitsenõukogus, et tagada ELi andmekaitseõigusaktide järjekindel kohaldamine.

SISUKORD

Euroopa Andmekaitsenõukogu,

võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta; edaspidi: „isikuandmete kaitse üldmäärus“) artikli 70 lõike 1 punkti e,

võttes arvesse Euroopa Majanduspiirkonna (EMP) lepingut, eriti selle XI lisa ja protokolli nr 37, mida on muudetud EMP ühiskomitee 6. juuli 2018. aasta otsusega nr 154/2018,[1]

võttes arvesse töökorra artiklit 12 ja artiklit 22,

ning arvestades järgmist:

(1) Euroopa Liidu Kohus järeldab 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 standardsete andmekaitseklauslite alusel, tagama õiguste kaitse, mille tase on sisuliselt samaväärne sellega, mis on Euroopa Liidus tagatud vastavalt kõnealusele määrusele, tõlgendatuna lähtuvalt Euroopa Liidu põhiõiguste hartast.[2]

(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.[3]

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

(4) Kohus selgitab, et komisjoni poolt vastu võetud standardsete andmekaitseklauslite eesmärk on üksnes teha liidus asuvatele vastutavatele töötlejatele või nende volitatud töötlejatele kättesaadavaks lepingulised kaitsemeetmed, mis on kõigis kolmandates riikides ühtviisi kohaldatavad. Lepingulise

[1] Kõiki käesoleva dokumendi viiteid liikmesriikidele tuleb mõista kui viiteid EMP liikmesriikidele.
[2] 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 järeldus.
[3] C-311/18 (Schrems II), punktid 92 ja 93.

olemuse tõttu ei saa standardsed andmekaitseklauslid olla siduvad kolmandate riikide avaliku sektori asutustele, sest nad ei ole lepingu pooled. Seetõttu võib andmeeksportijatel olla vaja lisada nendes standardsetes andmekaitseklauslites 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 julgustatakse vastutavaid töötlejaid ja volitatud töötlejaid seda kasutama.[4]

(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 standardsete andmekaitseklauslite alusel edastatud isikuandmete sisuliselt samaväärse kaitsetaseme, ja vajaduse korral näha lisaks standardsetes andmekaitseklauslites ettenähtule ette täiendavad kaitsemeetmed.[5]

(6) Kui Euroopa Liidus asuval vastutaval töötlejal või tema volitatud töötlejal 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.[6]

(7) Isikuandmete kaitse üldmäärus 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 töötlejad ja volitatud töötlejad võivad võtta, et tagada konkreetses kolmandas riigis kooskõla ELi õigusega nõutava kaitsetasemega.

(8) Euroopa Andmekaitsenõukogu on otsustanud küsimust omal algatusel uurida ning anda eksportijatena tegutsevatele vastutavatele töötlejatele ja volitatud töötlejatele soovitusi täiendavate meetmete tuvastamise ja vastuvõtmise võimaliku protsessi kohta. Soovituste eesmärk on koostada eksportijate jaoks metoodika, 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 EMPs tagatuga sisuliselt samaväärsel tasemel. Käesolevate soovituste andmisega on Euroopa Andmekaitsenõukogu eesmärk ergutada isikuandmete kaitse üldmääruse järjepidevat kohaldamist,[7]

ON VASTU VÕTNUD KÄESOLEVAD SOOVITUSED:

[4] C-311/18 (Schrems II), punktid 132 ja 133.
[5] C-311/18 (Schrems II), punkt 134.
[6] C-311/18 (Schrems II), punkt 135.
[7] Isikuandmete kaitse üldmääruse artikli 70 lõike 1 punkt e.

1 VASTUTUS ANDMEEDASTUSEL

1. ELi esmased õigusaktid käsitlevad õigust andmekaitsele põhiõigusena.[8] Vastavalt sellele on õigus andmekaitsele hästi kaitstud ning piiranguid võib 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 muude isikute õigusi ja vabadusi.[9] Õigus isikuandmete kaitsele ei ole absoluutne õigus, vaid seda tuleb kaalutleda vastavalt selle ülesandele ühiskonnas ning tasakaalustada muude põhiõigustega vastavalt proportsionaalsuse põhimõttele.[10]

2. Andmetega, mis liiguvad kolmandasse riiki väljapoole EMPd, peab kaasnema ELis tagatuga sisuliselt samaväärne kaitsetase, tagamaks, et nii edastamise ajal kui ka pärast seda ei kahjustuks isikuandmete kaitse üldmäärusega tagatud kaitsetase.

3. Õigus andmekaitsele on olemuselt aktiivne. Selleks on vaja, et eksportijad ja importijad (vastutavad ja/või volitatud töötlejad) teeksid enamat kui üksnes õiguse tunnustamine või passiivne järgimine.[11] Vastutavad töötlejad ja volitatud töötlejad peavad püüdma täita õigust andmekaitsele aktiivselt ja pidevalt, rakendades juriidilisi, tehnilisi ja korralduslikke meetmeid, mis tagavad selle tõhususe. Vastutavad töötlejad ja volitatud töötlejad peavad suutma ka tõendada seda tegevust andmesubjektidele ja andmekaitse järelevalveasutustele. Seda nimetatakse vastutuse põhimõtteks.[12]

4. Vastutuse põhimõtet on vaja isikuandmete kaitse üldmäärusega antava kaitse tõhusa kohaldamise tagamiseks ka andmete edastamisel kolmandatesse riikidesse[13], sest ka see on andmetöötluse vorm.[14] 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.[15]

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 standardseid andmekaitseklausleid.[16] Eksportijana tegutsev vastutav või volitatud töötleja peab tagama, et importijad teevad vajaduse korral eksportijaga nende ülesannete täitmisel koostööd,

---

[8] Põhiõiguste harta artikli 8 lõige 1 ja Euroopa Liidu toimimise lepingu artikli 16 lõige 1, isikuandmete kaitse üldmääruse põhjendus 1, artikli 1 lõige 2.
[9] Euroopa Liidu põhiõiguste harta artikli 52 lõige 1.
[10] 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.
[11] C-92/09 ja C-93/02, Volker und Markus Schecke GbR *vs.* Land Hessen, kohtujurist Sharpstoni ettepanek, 17. juuni 2010, punkt 71.
[12] Isikuandmete kaitse üldmääruse artikli 5 lõige 2 ja artikli 28 lõike 3 punkt h.
[13] Isikuandmete kaitse üldmääruse artikkel 44 ja põhjendus 101 ning isikuandmete kaitse üldmääruse artikli 47 lõike 2 punkt d.
[14] Euroopa Liidu Kohtu 6. oktoobri 2015. aasta otsus kohtuasjas Maximillian Schrems *vs.* Data Protection Commissioner, (edaspidi C-362/14 (Schrems I)), punkt 45.
[15] C-311/18 (Schrems II), punktid 92 ja 93.
[16] C-311/18 (Schrems II), punktid 134, 135, 139, 140, 141 ja 142.

hoides teda näiteks kursis importija asukohariigis vastu võetud isikuandmete kaitset mõjutavate arengutega.[17] Need ülesanded tähendavad isikuandmete kaitse üldmääruse vastutuse põhimõtte kohaldamist andmeedastusele.[18]

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[19] vastutavat või volitatud andmetöötlejat, kes töötleb isikuandmeid isikuandmete kaitse üldmääruse kohaldamisalas. See hõlmab ka eraõiguslike asutuste ja avaliku sektori asutuste tehtavat töötlemist, kui andmeid edastatakse eraõiguslikele asutustele.[20] 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.*[21]

7. See hindamine ning valitud ja rakendatavad täiendavad meetmed tuleb sobivalt dokumenteerida ning teha vastavad dokumendid nõudmise korral kättesaadavaks pädevale järelevalveasutusele.[22]

2.1 1. samm. Tundke oma edastustoiminguid

8. Et teada, mida võidakse nõuda teilt (andmeeksportijalt), et jätkata või alustada uut isikuandmete edastamist[23], 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 töötlejat ja alamtöötlejat. Oma edastustoimingute tundmine on hädavajalik esimene samm vastutuse põhimõttest tulenevate kohustuste täitmisel.

9. Oma edastustoimingutest täieliku ülevaate saamiseks võite lähtuda töötlemistoimingute kannetest, mille pidamise kohustus võib teil olla vastutava või volitatud töötlejana isikuandmete

[17] C-311/18 (Schrems II), punkt 134.
[18] Isikuandmete kaitse üldmääruse artikli 5 lõige 2 ja artikli 28 lõike 3 punkt h.
[19] Seega näiteks ei loeta teid andmeeksportijaks, kui olete andmesubjekt, kes esitab oma isikuandmed veebipõhise küsimustiku kaudu kolmandas riigis asuvale vastutavale töötlejale.
[20] Vt Euroopa Andmekaitsenõukogu suunised 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_en
[21] Euroopa Andmekaitsenõukogu suunised 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
[22] Isikuandmete kaitse üldmääruse artikli 5 lõige 2 ja artikli 24 lõige 1.
[23] NB! Edastamisena käsitatakse ka kolmandas riigis asuva isiku kaugjuurdepääsu EMPs asuvatele andmetele.

kaitse üldmääruse artikli 30 alusel.[24] Samuti võib teil abi olla varasematest tegevustest andmesubjektide 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.[25]

10. Ärge unustage edastustoimingute uurimisel arvestada ka edasi saatmist, näiteks seda, kas teie volitatud töötlejad väljaspool EMPd saadavad teilt neile usaldatud isikuandmeid edasi muus kolmandas riigis või samas kolmandas riigis asuvale alamtöötlejale.[26]

11. Kooskõlas isikuandmete kaitse üldmääruse võimalikult väheste andmete kogumise põhimõttega[27] peate kontrollima, et teie edastatavad andmed oleksid piisavad, asjakohased ja piirduksid sellega, mida on vaja nendeks eesmärkideks, milleks neid töödeldakse.

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 (kaardistama sihtkohad).

13. Pidage meeles, et edastamiseks loetakse ka kaugjuurdepääsu kolmandast riigist (näiteks tugitoimingute ajal) ja/või hoiustamist teenusepakkuja pakutavas väljaspool EMPd asuvas pilves.[28] Täpsemalt peate rahvusvahelise pilvetaristu kasutamise korral hindama, kas teie andmeid edastatakse kolmandatesse riikidesse ja kuhu, v.a kui teie pilveteenuse osutaja on asutatud EMPs ja lepingus on selgelt märgitud, et andmeid ei töödelda üldse kolmandates riikides.

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.

---

[24] 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 töötleja ja volitatud töötleja on registri pidamise kohustusest vabastatud (isikuandmete kaitse üldmääruse artikli 30 lõige 5). Selle erandi suunised: vt artikli 29 töörühma seisukohta erandite kohta isikuandmete kaitse üldmääruse artikli 30 lõike 5 kohase töötlemistoimingute registri pidamise kohustusest (Euroopa Andmekaitsenõukogus 25. mail 2018 heaks kiidetud).

[25] Isikuandmete kaitse üldmääruse läbipaistvuseeskirjade kohaselt peate teavitama andmesubjekte sellest, kui isikuandmeid edastatakse kolmandatasse 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.

[26] Kui vastutav töötleja on andnud eelnevalt konkreetse või üldise kirjaliku nõusoleku kooskõlas isikuandmete kaitse üldmääruse artikli 28 lõikega 2.

[27] Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkt c.

[28] Vt Euroopa Andmekaitsenõukogu 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“.

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.[29]

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.

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).[30]

18. Euroopa Komisjon avaldab oma kaitse piisavuse otsuste loetelu oma veebilehel.[31]

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**.[32] Peate siiski jälgima oma edastustoimingute seisukohast oluliste kaitse piisavuse otsuste võimalikku tühistamist või kehtetuks tunnistamist.[33]

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.[34]

Näide:

ELi kodanik Maximillian Schrems esitas 2013. aasta juunis Iirimaa 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

[29] 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.

[30] Isikuandmete kaitse üldmääruse artikli 45 lõige 1.

[31] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[32] Kui teie ja andmeimportija olete võtnud meetmeid isikuandmete kaitse üldmäärusest tulenevate muude kohustuste täitmiseks; vastasel juhul rakendage nimetatud meetmed.

[33] 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 Liidu Kohus kaitse piisavuse otsuseid kehtetuks tunnistada (vt otsused kohtuasjades C-362/14 (Schrems I) and C-311/18 (Schrems II).

[34] 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.

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 Iirimaa kõrge kohus pöördus küsimusega otsuse 2000/520 kehtivuse kohta Euroopa Liidu Kohtu poole. Seejärel otsustas Euroopa Liidu Kohus tunnistada kehtetuks komisjoni otsuse 2000/520 piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega.[35]

[35] 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. Isikuandmete kaitse üldmääruse artikli 46 kohaste andmeedastusvahendite peamised liigid on:

- standardsed andmekaitseklauslid ;
- siduvad kontsernisisesed eeskirjad;
- toimimisjuhendid;
- sertifitseerimismehhanismid;
- *ad hoc* 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. Olukorrast 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.[36]

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 tõlgendada viisil, mis ei ole vastuolus erandite olemusega, kuna need on erandid reeglist, et isikuandmeid ei tohi edastada kolmandasse riiki, v.a kui riik sätestab piisava andmekaitse taseme või kui on kehtestatud asjakohased kaitsemeetmed. Erandid ei saa praktikas muutuda reegliks, vaid neid tuleb piirata konkreetsete olukordadega. Euroopa Andmekaitsenõukogu on andnud välja suunised 2/2018 määruse 2016/679 artikli 49 erandite kohta. [37]

26. Enne isikuandmete kaitse üldmääruse artiklis 49 sätestatud erandi kasutamist peate kontrollima, kas teie edastustoiming vastab rangetele tingimustele, mille täitmist see säte iga toimingu korral nõuab.

***

27. Kui teie edastustoiming ei saa juriidiliselt põhineda kaitse piisavuse otsusel ega artikli 49 erandil, peate jätkama 3. sammuga.

[36] C-311/18 (Schrems II), punktid 130 ja 133. Vt ka alapunkt 2.3 allpool.
[37] Üksikasjalikumad suunised on aadressil https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.

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 kohane valitud andmeedastusvahend peab olema tõhus selle tagamisel, et andmete edastamine ei kahjusta isikuandmete kaitse üldmäärusega tagatud kaitse taset.[38]

29. Eelkõige peab kolmandas riigis edastatavate isikuandmete kaitse olema sisuliselt samaväärne kaitsega, mis on EMPs tagatud isikuandmete kaitse üldmäärusega koostoimes Euroopa Liidu põhiõiguste hartaga.[39] 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, sh andmete eksportijalt importija riiki edastamise ajal.[40]

30. Esmalt peate hindama, vajaduse korral koostöös importijaga, kas kolmanda riigi õiguses ja/või kasutatavas praktikas[41] on midagi, mis võiks kahjustada teie kasutatava isikuandmete kaitse üldmääruse artikli 46 kohase edastusvahendi asjakohaste kaitsemeetmete tõhusust teie konkreetse edastustoimingu kontekstis. See tähendab, et tuleb kindlaks teha, kas teie edastustoiming kuulub selliste õigusaktide ja/või tavade kohaldamisalasse, mis võivad piirata teie isikuandmete kaitse üldmääruse artikli 46 kohase andmeedastusvahendi tõhusust. Nõutud hindamine peab põhinema eelkõige avalikult kättesaadavatel õigusaktidel.

31. Hindamine peab sisaldama järgmisi elemente, mis käsitlevad teie importija kolmanda riigi ametiasutuste juurdepääsu andmetele:

    - teave, kas teie importija kolmanda riigi ametiasutused võivad taotleda andmetele juurdepääsu andmeimportija teadmisega või ilma, arvestades õigusakte, tavasid ja teatatud pretsedente;
    - elemendid seoses sellega, kas teie importija kolmanda riigi ametiasutustel võib olla andmetele juurdepääs andmeimportija või sideteenuse pakkujate või sidekanalite kaudu, arvestades nende käsutuses olevaid õigusakte, õiguslikke volitusi, tehnilisi, rahalisi ja inimressursse ning teatatud pretsedente.

Asjakohaste õigusaktide ja tavade tuvastamine, arvestades edastamise kõiki asjaolusid

32. Peate uurima iga edastustoimingu omadusi ja määrama, kas teie edastustoiminguid kahjustavad neile toimingutele kehtiv õiguskord ja/või tavad riigis, kuhu andmeid edastatakse (või hiljem edasi saadetakse). Teie hinnang piirdub seega teie edastatavate konkreetsete andmete kaitsega seotud õigusaktide ja tavadega erinevalt üldistest ja laiaulatuslikest kaitse piisavuse hindamistest, mida Euroopa Komisjon teeb kooskõlas isikuandmete kaitse üldmääruse artikliga 45.

---

[38] Isikuandmete kaitse üldmääruse artikkel 44 ja C-311/18 (Schrems II) punktid 126, 137 ja 148.
[39] C-311/18 (Schrems II), punkt 105 ja teine järeldus.
[40] Vt otsus kohtuasjas C-311/18 (Schrems II), punkt 183 koostoimes punktiga 184.
[41] Vt kohtuotsuse C-311/18 (Schrems II) punkt 126, milles kohus viitab sõnaselgelt „asjaomases kolmandas riigis kehtivatele õigusaktidele ja tavadele“ ning nõuab, et „tagataks praktikas asjaomasele kolmandale riigile edastatud isikuandmete tõhus kaitse.“ (rõhuasetus lisatud) ning punkt 158.

33. Kohalduv õiguslik kontekst ja/või tavad sõltuvad teie edastustoimingu konkreetsetest asjaoludest, eelkõige 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 (nt laste isikuandmed võivad kuuluda kolmandas riigis eriõigusaktide kohaldamisalasse);[42]
    - kas andmeid hoitakse kolmandas riigis või antakse kaugjuurdepääs ELis/EMPs hoitavatele andmetele;
    - edastatavate andmete vorm (lihttekstina / pseudonüümitud või krüptitud[43]);
    - võimalus, et andmeid võidakse kolmandast riigist muusse kolmandasse riiki edasi saata.[44]

34. Teie hinnang peaks arvestama kõiki edastustoimingute uurimisel tuvastatud edastamises osalejaid (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 andmete kavandatud hilisemat edasisaatmist.

35. Igal juhul tuleks erilist tähelepanu pöörata kõigile olulistele õigusaktidele, eelkõige neile, millega on kehtestatud nõudeid isikuandmete avaldamise kohta avaliku sektori ametiasutustele või antud sellistele asutustele volitusi isikuandmetega tutvumiseks (näiteks kriminaalõiguse jõustamise, regulatiivjärelevalve ja riikliku julgeoleku eesmärgil). Kui need nõuded või volitused piiravad andmesubjektide põhiõigusi, järgides samas nende olemust ning on demokraatlikus ühiskonnas vajalikud ja proportsionaalsed meetmed, et kaitsta ka liidu või ELi liikmesriikide õigusaktides[45] tunnustatud olulisi eesmärke, ei tohi need piirata kohustusi, mis sisalduvad isikuandmete kaitse üldmääruse artikli 46 kohases andmeedastusvahendis, millele te tuginete.

---

[42] Isikuandmete edastamine on töötlemistoiming (isikuandmete kaitse üldmääruse artikli 4 lõige 2). Kui soovite edastada isikuandmete kaitse üldmääruse artiklite 9 ja 10 alla kuuluvaid tundlikke andmeid, võite andmeid edastada ainult siis, kui see kuulub mõne isikuandmete kaitse üldmääruse artiklites 9 ja 10 ning ELi liikmesriikide õiguses sätestatud erandi ja tingimuse alla. Isikuandmete kaitse üldmääruse artikli 32 kohaselt peate rakendama koos vastutava töötleja või volitatud töötlejana tegutseva importijaga asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada asjakohane turvalisuse tase, mis vastab andmesubjektide õigusi ja vabadusi avalduvatele riskidele, mida võib põhjustada edastatavate andmetega seotud rikkumine (isikuandmete kaitse üldmääruse artikkel 4 punkt 12). Edastatavate andmete kategooriad ja nende tundlikkus on asjakohased riski ja meetmete asjakohasuse hindamisel.

[43] Mõni kolmas riik ei luba krüptitud andmete importimist.

[44] Kui vastutav töötleja on andnud eelnevalt konkreetse või üldise kirjaliku nõusoleku kooskõlas isikuandmete kaitse üldmääruse artikli 28 lõikega 2.

[45] Vt ELi põhiõiguste harta artiklid 47 ja 52, isikuandmete kaitse üldmääruse artikli 23 lõige 1 ja Euroopa Andmekaitsenõukogu 10. novembri 2020. aasta soovitused 02/2020 Euroopa oluliste tagatiste kohta seoses järelevalvemeetmetega, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

36. Peate hindama asjakohaseid üldist laadi eeskirju ja tavasid, kui need mõjutavad isikuandmete kaitse üldmääruse artikli 46 kohases andmeedastusvahendis sisalduvate kaitsemeetmete tõhusat kohaldamist.

37. Sellel hindamisel on olulised ka kolmanda riigi õigussüsteemi mitmesugused aspektid, nt isikuandmete kaitse üldmääruse artikli 45 lõikes 2 loetletud elemendid. 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 andmekaitseseaduse või sõltumatu andmekaitseasutuse olemasolu ning selliste rahvusvaheliste õigusaktide järgimine, milles on ette nähtud andmekaitsemeetmed.

38. Sellistest õigusaktidest ja tavadest tulenevaid kohustusi või volitusi käsitatakse isikuandmete kaitse üldmääruse artikli 46 kohase andmeedastusvahendi kohustuste suhtes või nendega vastuolus olevatena, kui need[46]:

    - ei austa ELi põhiõiguste hartas sätestatud põhiõiguste ja -vabaduste olemust või

    - lähevad kaugemale sellest, mis on demokraatlikus ühiskonnas vajalik ja proportsionaalne, et kaitsta üht olulistest eesmärkidest, mida on tunnustatud ka liidu või liikmesriigi õiguses, näiteks isikuandmete kaitse üldmääruse artikli 23 lõikes 1 loetletud eesmärgid.

39. Peaksite kontrollima, kas andmeimportija kohustusi, mis võimaldavad andmesubjektidel kasutada oma õigusi, mis on sätestatud isikuandmete kaitse üldmääruse artikli 46 kohases andmete edastamise vahendis (näiteks edastatud andmetele juurdepääsu, nende parandamise ja kustutamise taotlused ning (kohtulikud) õiguskaitsevahendid), saab tõhusalt kohaldada ning kas neid ei takista sihtriigiks oleva kolmanda riigi õigusaktid ja/või tavad.

40. Võrdluseks tuleb kasutada ELi standardeid, näiteks ELi põhiõiguste harta artikleid 47 ja 52, eelkõige selleks, et hinnata, kas selline avaliku sektori ametiasutuste juurdepääs piirdub demokraatlikus ühiskonnas vajaliku ja proportsionaalsega ning kas andmesubjektidel on tõhusad kaitsevõimalused.

41. Euroopa Andmekaitsenõukogu Euroopa oluliste tagatiste soovitustes[47] antakse selgitus elementide kohta, 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[48]. Eelkõige tuleb seda hoolikalt kaalutleda, kui avaliku sektori asutuste juurdepääsu andmetele reguleerivad õigusaktid on mitmeti mõistetavad või ei ole avalikult kättesaadavad. Euroopa oluliste tagatiste esimene nõue on, et selline juurdepääs peaks olema avalikult kättesaadav ja piisavalt selge, kui see on ette nähtud.

---

[46] Vt ELi põhiõiguste harta artiklid 47 ja 52, isikuandmete kaitse üldmääruse artikli 23 lõige 1, C-311/18 (Schrems II) punktid 174 ja 187 ja Euroopa Andmekaitsenõukogu 10. novembri 2020. aasta soovitused 02/2020 Euroopa oluliste tagatiste kohta seoses järelevalvemeetmetega.

[47] Euroopa Andmekaitsenõukogu 10. novembri 2020. aasta soovitused 02/2020 Euroopa oluliste tagatiste kohta seoses järelevalvemeetmetega.

[48] Seega ei ole see vastuolus isikuandmete kaitse üldmääruse artikli 46 kohase andmeedastusvahendiga võetud kohustustega.

42. Kui neid kohaldatakse artikli 46 kohastel edastusvahenditel põhinevate andmeedastustoimingutega seotud olukordadele, võivad Euroopa Andmekaitsenõukogu Euroopa oluliste tagatiste soovitused aidata andmeeksportijal hinnata, kas need volitused takistavad andmeeksportijal ja andmeimportijal vastavalt isikuandmete kaitse üldmäärusele või andmeedastusvahendiga kehtestatud kohustustele sisulise samaväärsuse tagamise kohustuste täitmist. Sisuliselt samaväärse kaitsetaseme puudumine on eriti ilmne, kui teie edastustoimingu suhtes asjakohase kolmanda riigi õigusaktid või praktika ei vasta Euroopa oluliste tagatiste nõuetele. Euroopa Andmekaitsenõukogu kordab, et Euroopa olulised tagatised on kolmanda riigi jälgimismeetmetega kaasneva riivamise hindamisel võrdlusalus rahvusvahelise andmeedastuse kontekstis. Need võrdlusalused tulenevad ELi õigusest ning Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu praktikast, mis on siduv ELi liikmesriikide suhtes.

43. Hindamine peab põhinema eelkõige avalikult kättesaadavatel õigusaktidel. Kolmanda riigi ametiasutuste tavade uurimine võimaldab teil kontrollida, kas isikuandmete kaitse üldmääruse artikli 46 kohases andmeedastusvahendis sisalduvad kaitsemeetmed võivad olla piisavad, et tagada edastatud isikuandmete tõhus kaitse.[49] Kolmandas riigis kehtivate tavade uurimine on hindamise jaoks eriti oluline allpool kirjeldatud olukordades.

43.1 **Kolmanda riigi asjakohased õigusaktid võivad ametlikult vastata ELi põhiõiguste ja -vabaduste standarditele ning nende piirangute vajalikkusele ja proportsionaalsusele.** Avaliku sektori asutuste tavad (nt juurdepääs erasektori valduses olevatele isikuandmetele või järelevalve- või kohtuasutustena õigusakte jõustades või mitte) võivad siiski selgelt viidata sellele, et need ei ole tavaliselt kohaldatavad ja/või järgivad õigusakte, millega põhimõtteliselt reguleeritakse nende tegevust. Sellisel juhul peate neid tavasid hindamisel arvesse võtma ning arvestama, et isikuandmete kaitse üldmääruse artikli 46 alusel ei ole iseenesest (st ilma täiendavate meetmeteta) võimalik tõhusalt tagada sisuliselt samaväärset kaitsetaset. Sellisel juhul, kui soovite edastamist jätkata, peate võtma asjakohaseid täiendavaid meetmeid.

43.2 **Kolmanda riigi asjakohased õigusaktid (nt juurdepääsu kohta erasektori valduses olevatele isikuandmetele) võivad puududa.** Sellisel juhul ei saa asjakohaste õigusaktide puudumisest automaatselt järeldada, et teie isikuandmete kaitse üldmääruse artikli 46 kohast andmeedastusvahendit on võimalik tõhusalt kohaldada. Peate kontrollima, kas riigis on märke tavadest, mis on vastuolus ELi õigusega ja isikuandmete kaitse üldmääruse artikli 46 kohase andmeedastusvahendi kohustustega. Vastuvõetamatute tavade korral ei ole isikuandmete kaitse üldmääruse artikli 46 kohase andmeedastusvahendiga võimalik iseenesest (st ilma piisavate täiendavate meetmeteta) tõhusalt tagada sisuliselt samaväärset kaitsetaset. Sellisel juhul, kui soovite edastamist jätkata, peate võtma asjakohaseid täiendavaid meetmeid.

[49] C-311/18 (Schrems II), punkt 126.

43.3 **Hindamisel võib selguda, et kolmanda riigi asjakohased õigusaktid võivad olla problemaatilised[50] ning et edastatavad andmed ja/või asjaomane importija kuuluvad või võivad kuuluda nende probleemsete õigusaktide kohaldamisalasse.[51]**

Arvestades ebakindlust seoses probleemsete õigusaktide võimaliku kohaldamisega teie edastustoimingu suhtes, võite seejärel otsustada:

- edastamine peatada;
- võtta täiendavaid meetmeid[52], et vältida riski, et teie importija ja/või teie edastatavate andmete suhtes võidakse kohaldada andmeimportija kolmanda riigi õigusakte ja/või tavasid, mis võivad takistada edastamisvahendi lepingulisi tagatisi sisuliselt samaväärsel tasemel kaitsetasemega, mis on tagatud EMPs; või
- teise võimalusena võite otsustada jätkata edastustoimingut, ilma et oleks vaja võtta täiendavaid meetmeid, kui leiate, et teil ei ole põhjust uskuda, et teie edastatavate andmete ja/või importija suhtes kohaldatakse praktikas asjakohaseid ja problemaatilisi õigusakte. Peate olema oma hindamisel (vajaduse korral koostöös importijaga) tõendanud ja dokumenteerinud, et õigust ei tõlgendata ja/või ei kohaldata praktikas nii, et see hõlmaks teie edastatavaid andmeid ja importijat, arvestades ka samas sektoris tegutsevate ja/või seotud sarnaste edastatavate isikuandmete ja allpool kirjeldatud täiendavate teabeallikatega seotud osalejate kogemusi.[53]

  Seepärast peate tõendama ja dokumenteerima üksikasjalikus aruandes[54], et teie edastatavate andmete ja/või importija suhtes ei kohaldata praktikas probleemseid õigusakte ning seega ei takista see importijat täitmast oma kohustusi, mis tulenevad isikuandmete kaitse üldmääruse artikli 46 kohasest andmeedastusvahendist.[55]

---

[50] Probleemsete õigusaktide all mõistetakse õigusnorme, mis 1) panevad Euroopa Liidust isikuandmete vastuvõtjale kohustusi ja/või mõjutavad edastatavaid andmeid viisil, mis võib mõjutada edastamisvahendite lepingulist tagatist, mis on sisuliselt samaväärne, ja 2) ei austa ELi põhiõiguste hartas tunnustatud põhiõiguste ja -vabaduste olemust või lähevad kaugemale sellest, mis on demokraatlikus ühiskonnas vajalik ja proportsionaalne, et kaitsta üht olulistest eesmärkidest, mida on tunnustatud ka liidu või ELi liikmesriikide õiguses, näiteks isikuandmete kaitse üldmääruse artikli 23 lõikes 1 loetletud eesmärgid.

[51] Võib olla ebaselge, kas importija ja/või edastatavad andmed kuuluvad sageli riikliku julgeoleku õigusaktide üldmõistete kohaldamisalasse, mida kasutatakse, et piirata nende kohaldamisala, näiteks „elektroonilise side teenuse osutaja“ ja „välisluureteave“.

[52] Vt isikuandmete kaitse üldmääruse põhjendus 109 ja C-311/18 (Schrems II) punkt 132.

[53] Vt punktid 45–47.

[54] Koostatavad aruanded peavad sisaldama põhjalikku teavet õigusaktide ja tavade õigusliku hindamise ning nende kohaldamise kohta konkreetsetele andmeedastustele, hindamise sisemenetluse kohta (sealhulgas teave hindamisel osalejate kohta, nt õigusbürood, konsultandid või asutusesisesed osakonnad) ja kontrollide kuupäevade kohta. Aruanded peab kinnitama eksportija seaduslik esindaja.

[55] Tõendamine, et teie edastatavate andmete ja importija suhtes ei kohaldata praktikas probleemseid õigusakte, arvestades ka muude samas sektoris tegutsevate ja/või sarnaste edastatavate isikuandmetega seotud osalejate kogemusi, ei vabasta teid vajalike täiendavate meetmete tagamisest, et kaitsta isikuandmeid nende edastamise ja töötlemise ajal kolmandas sihtriigis (nt andmete otspunktkrüptimine – vt tehniliste lisameetmete näited 2. lisas), kui teie analüüs kolmanda sihtriigi kohaldatavate õigusaktide kohta näitab, et juurdepääs andmetele võib toimuda ka siis, kui importija ei sekku, edastamise hetkel. Võite selliseid meetmeid juba ette näha, kui

Võimalikud teabeallikad

44. Teie andmeimportija peab esitama teile asjakohased allikad ja teabe kolmanda riigi kohta, kus ta asub, ning edastamisele kohaldatavate kehtivate õigusaktide ja tavade kohta.

45. Teie ja teie importija võivad hindamise lõpule viia, kasutades teavet, mis on saadud näiteks 3. lisas näidetena loetletud allikatest.

46. Lisaks edastamise suhtes kohaldatavale kolmanda riigi õigusraamistikule peaksid allikad ja teave olema asjakohased, objektiivsed, usaldusväärsed, kontrollitavad ja üldsusele kättesaadavad või muul viisil kättesaadavad, et teha kindlaks, kas teie artikli 46 kohast edastamisvahendit on võimalik tõhusalt kohaldada[56], ning peate hindama ja dokumenteerima, et need on seda.

importija tegutseb vastutava töötleja või volitatud töötlejana kooskõlas isikuandmete kaitse üldmääruse artikliga 32.

[56] Vt 3. lisa mitteammendav loetelu teabeallikatest, mida teie ja importija võite kasutada.

Asjakohane: teave peab olema asjakohane konkreetse edastamise ja/või importija suhtes ning selle vastavuse suhtes ELi õiguses ja isikuandmete kaitse üldmääruse artiklis 46 sätestatud nõuetele, mitte liiga üldine või abstraktne.

Objektiivne teave: teave, mida toetavad empiirilised tõendid, mis põhinevad varasematel teadmistel, mitte oletustel võimalike sündmuste ja riskide kohta.

Usaldusväärne: eksportija ja importija peavad objektiivselt hindama teabeallika ja teabe usaldusväärsust ning hindama neid eraldi.

Kontrollitav: teave ja järeldused peaksid olema kontrollitavad või vastandatavad muud liiki teabe või allikatega osana üldhinnangust, et võimaldada pädeval järelevalve- või kohtuasutusel vajaduse korral kontrollida selle teabe objektiivsust ja usaldusväärsust.

Avalikult kättesaadav või muul viisil kättesaadav teave: teave peaks eelistatult olema avalik või vähemalt kättesaadav, et hõlbustada eespool esitatud kriteeriumide kontrollimist ning tagada selle võimalik jagamine järelevalveasutuste, õigusasutuste ja lõppkokkuvõttes andmesubjektidega.

47. Samuti võite arvesse võtta importija dokumenteeritud praktilisi kogemusi seoses kolmandate riikide ametiasutustelt saadud juurdepääsutaotluste asjakohaste varasemate juhtumitega. Saate kasutada importija kogemusi täiendava teabeallikana üksnes juhul, kui kolmanda riigi õigusraamistik ei keela importijal esitada teavet riigiasutuste esitatud avalikustamistaotluste kohta või selliste taotluste puudumise kohta (ning peaksite sellise hinnangu dokumenteerima). Peate siiski arvestama, et importija varasemate taotluste puudumist ei saa kunagi pidada isikuandmete kaitse üldmääruse artikli 46 kohase andmeedastusvahendi tõhususe seisukohast otsustavaks teguriks, mis võimaldab andmete edastamist jätkata ilma täiendavate meetmeteta. Saate seda teavet koos muudest allikatest saadud muud liiki teabega arvestada teie edastustoimingu üldise hindamise osana seoses kolmanda riigi õigusaktide ja tavadega. Importija asjakohaseid ja dokumenteeritud kogemusi peaks kinnitama asjakohane, objektiivne, usaldusväärne, kontrollitav ja avalikult kättesaadav või muul viisil kättesaadav teave asjakohase õigusakti praktilise kohaldamise kohta (nt samas sektoris tegutsevatelt muudelt osalejatelt saadud ja/või sarnaste edastatavate isikuandmetega seotud juurdepääsutaotluste olemasolu või puudumine[57] ja/või õigusakti kohaldamine praktikas, näiteks kohtupraktika ja sõltumatute järelevalveasutuste aruanded).

Hindamise tulemused

48. Peaksite oma edastustoiminguga seotud importija kolmanda riigi õigusaktide ja tavade üldise hindamise teostama nõuetekohase hoolsusega ja seda põhjalikult dokumenteerima. Teie pädevad järelevalve- ja/või õigusasutused võivad seda nõuda ja võtta teid vastutusele kõigi selle alusel tehtud otsuste eest.[58]

[57] Kogemused võivad olla saadud teistelt üksustelt, keda otseselt teadsite oma varasemate samalaadsete andmeedastuste tõttu, või mida on kirjeldatud asjakohases kohtupraktikas, valitsusväliste organisatsioonide aruannetes jne (vt 3. lisa).
[58] Isikuandmete kaitse üldmääruse artikli 5 lõige 2.

49. Hindamisel võib lõpuks selguda, et teie kasutatav isikuandmete kaitse üldmääruse artikli 46 kohane edastusvahend on järgmiste omadustega.

    - Tagab tõhusalt, et edastatavad 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. Peaksite olukorda taas hindama asjakohaste ajavahemike järel või oluliste muudatuste ilmnemisel (vt 6. samm).

    - Ei taga tõhusalt sisuliselt samaväärset kaitsetaset. Andmeimportija ei saa oma kohustusi täita kolmanda riigi õigusaktide ja/või tavade tõttu, mida kohaldatakse andmete edastamise suhtes, mis ei vasta ELi põhiõiguste ja -vabaduste standarditele ning nende piirangute vajalikkusele ja proportsionaalsusele, et kaitsta avaliku huvi õiguspäraseid eesmärke. Euroopa Liidu Kohus on rõhutanud, et kui isikuandmete kaitse üldmääruse artikli 46 kohane edastusvahend osutub ebapiisavaks, on andmeeksportija ülesanne võtta tõhusaid täiendavaid meetmeid või isikuandmeid mitte edastada.[59]

Näide.

Taust
Näiteks otsustas Euroopa Liidu 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 paragrahviga 702 volitatud programmide kaitsetase ei ole ELi õigusega nõutavate kaitsemeetmetega sisuliselt samaväärne.

Hindamine
Kui teie hinnang asjakohastele USA õigusaktidele viib selleni, et teie edastustoiming võib kuuluda FISA paragrahvi 702 kohaldamisalasse, kuid te ei ole kindel, kas see kuulub selle praktilise kohaldamisala alla, võite otsustada, kas:

1. edastamine peatada;
2. võtta vastu asjakohased lisameetmed, mis tagavad edastatavate andmete tõhusa kaitse taseme, mis on sisuliselt samaväärne EMPs tagatuga; või
3. uurida muud objektiivset, usaldusväärset, asjakohast, kontrollitavat ja eelistatavalt avalikult kättesaadavat teavet (mis võib hõlmata teie andmeimportijalt saadud teavet), et selgitada FISA paragrahvi 702 praktilist kohaldamisala teie konkreetse edastamise suhtes. See teave peaks andma vastused mõnele asjakohasele küsimusele, näiteks järgmistele küsimustele.

- Kas avalikult kättesaadav teave näitab, et on olemas õiguslik keeld teavitada konkreetsest saadud andmetele juurdepääsu taotlusest ning ulatuslikud piirangud üldise teabe andmisel saadud andmetele juurdepääsu taotluste või saadud taotluste puudumise kohta?

- Kas teie andmeimportija on kinnitanud, et on varem saanud USA ametiasutustelt andmetele juurdepääsu taotlusi? Või on teie andmeimportija kinnitanud, et ta ei ole varem USA ametiasutustelt

[59] C-311/18 (Schrems II), punktid 134 ja 135.

andmetele juurdepääsu taotlusi saanud ning et tal ei ole keelatud esitada teavet selliste taotluste või nende puudumise kohta?

- Kas avalikult kättesaadav teave USA kohtupraktika kohta ning järelevalveasutustelt, kodanikuühiskonna organisatsioonidelt ja akadeemilistelt asutustelt saadud aruannetest[60] nähtub, et andmeimportijaid sama sektorist kui teie importija on varem saanud juurdepääsu taotlusi sarnastele edastatavatele andmetele?

Neile küsimustele antud vastuste põhjal võite järeldada järgmist.

- FISA paragrahvi 702 kohaldatakse praktikas teie konkreetse andmeedastuse suhtes ja seega piirab see teie kasutatava isikuandmete kaitse üldmääruse artikli 46 kohase andmeedastusvahendi tõhusust. Seega, kui soovite andmete edastamist jätkata, peate kaalutlema, vajaduse korral koostöös importijaga, kas saate võtta täiendavaid meetmeid, mis tagavad edastatavate andmete tõhusa kaitse taseme, mis on sisuliselt samaväärne EMPs tagatuga. Kui te ei leia tõhusaid täiendavaid meetmeid, ei tohi te isikuandmeid edastada.

või

- FISA paragrahv 702 ei ole teie konkreetse andmeedastuse suhtes praktikas kohaldatav ja seega ei piira see teie kasutatava isikuandmete kaitse üldmääruse artikli 46 kohase andmeedastusvahendi tõhusust. Seejärel võite edastamist jätkata ilma täiendavate meetmeteta.

2.4 4. samm. Võtke vastu täiendavad meetmed

50. 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.[61] „Täiendavad meetmed“ on määratluse kohaselt täienduseks isikuandmete kaitse üldmääruse artikli 46 kohase andmeedastusvahendiga juba ette nähtud kaitsemeetmetele ja muudele isikuandmete kaitse üldmääruses sätestatud kohaldatavatele turbenõuetele (nt tehnilised turbemeetmed).[62]

51. 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. Te ei pea hindamist kordama iga kord, kui

[60] nt FISA paragrahvi 702 sätted; välisluure järelevalvekohtu (FISC) kodukord, kustutatud salastatus FISCi arvamustest ja otsustest, USA kohtute kohtupraktika; eraelu puutumatuse kodanikuvabaduste järelevalve komisjoni aruanded ja kuulamiste transkriptsioonid; USA justiitsministeeriumi peainspektori büroo aruanded; riikliku julgeolekuameti kodanikuvabaduste ja eraelu puutumatuse büroo direktori aruanded; kongressi uurimistalituse koostatud aruanded; Ameerika kodanikuvabaduste liidu sihtasutuse (ACLU) aruanded.
[61] C-311/18 (Schrems II), punkt 96.
[62] Isikuandmete kaitse üldmääruse põhjendus 109 ja C-311/18 (Schrems II) punkt 133.

edastate sama liiki andmeid samasse kolmandasse riiki. Mõned edastamiseks kavandatud andmed võivad vajada täiendavaid meetmeid, samas kui muude andmete korral ei pruugi neid vaja olla (arvestades kolmanda riigi õiguse ametlikku ja/või praktilist kohaldamist). Saate kasutada oma varasemaid hindamisi (1., 2. ja 3. samm) ning kontrollida nende järelduste alusel täiendavate meetmete võimalikku tõhusust nõutava kaitsetaseme tagamisel.

52. 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.

53. Üksnes lepinguliste ja korralduslike meetmetega ei lahendata üldiselt kolmandate riikide ametiasutuste juurdepääsu isikuandmetele probleemsete õigusaktide ja/või tavade alusel[63]. On olukordi, kus üksnes asjakohaselt võetud tehnilised meetmed võivad takistada või muuta ebatulemuslikuks kolmandate riikide avaliku sektori ametiasutuste juurdepääsu isikuandmetele, eelkõige jälitustegevuseks.[64] Sellisel juhul võivad lepingulised või korralduslikud meetmed täiendada tehnilisi meetmeid ja tugevdada andmete üldist kaitset (nt võttes kasutusele kontrollid ja kõrvaldades automatismi avaliku sektori ametiasutuste katsetest saada andmetele juurdepääsu viisil, mis ei vasta ELi standarditele).

54. Võite vajaduse korral koostöös andmeimportijaga tutvuda järgmiste tegurite (mitteammendava) loeteluga, et tuvastada, mis täiendavad meetmed oleksid kõige tõhusamad, et kaitsta edastatavaid andmeid avaliku sektori ametiasutuste taotluste eest andmetele juurdepääsuks, mis põhinevad praktikas kohaldatavatel probleemsetel õigusaktidel:

    - edastatavate andmete vorm (lihttekstina / pseudonüümitud või krüptitud);
    - andmete olemus (nt EMPs tagatakse isikuandmete kaitse üldmääruse artiklitega 9 ja 10 hõlmatud andmekategooriatele kõrgem kaitsetase);[65]
    - andmetöötluse töövoo pikkus ja keerukus, töötluses osalevate tegutsejate arv ning nende suhe (nt kas edastamine hõlmab mitut vastutavat töötlejat või nii vastutavaid kui ka volitatud töötlejaid või selliste volitatud töötlejate kaasamine, kes edastavad andmed teie andmeimportijale (arvestades nende suhtes kohaldatavaid asjakohaseid sätteid vastavalt kolmanda sihtriigi õigusaktidele));[66]

---

[63] Probleemsete õigusaktide all mõistetakse õigusnorme, mis 1) panevad Euroopa Liidust isikuandmete vastuvõtjale kohustusi ja/või mõjutavad edastatavaid andmeid viisil, mis võib mõjutada edastamisvahendite lepingulist tagatist, mis on sisuliselt samaväärne, ja 2) ei austa ELi põhiõiguste hartas tunnustatud põhiõiguste ja -vabaduste olemust või lähevad kaugemale sellest, mis on demokraatlikus ühiskonnas vajalik ja proportsionaalne, et kaitsta üht olulistest eesmärkidest, mida on tunnustatud ka liidu või ELi liikmesriikide õiguses, näiteks isikuandmete kaitse üldmääruse artikli 23 lõikes 1 loetletud eesmärgid.

[64] 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 Andmekaitsenõukogu 10. novembri 2020. aasta soovitused 02/2020 Euroopa oluliste tagatiste kohta seoses järelevalvemeetmetega https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[65] Vt allmärkus 42.

[66] Isikuandmete kaitse üldmäärusega määratakse vastutavatele töötlejatele ja volitatud töötlejatele selgepiirilised kohustused. Edastamine võib toimuda ühelt vastutavalt töötlejalt teisele, kaasvastutavate töötlejate vahel, vastutavalt töötlejalt volitatud töötlejale ning vastutava töötleja volituse korral volitatud töötlejalt vastutavale töötlejale või volitatud töötlejalt volitatud töötlejale.

- kolmanda riigi õiguse praktilise kohaldamise tehnika või parameetrid, mis on kokku lepitud 3. sammu ajal;
- võimalus, et andmeid saadetakse veel edasi samas kolmandas riigis või isegi kolmandate riikide vahel (nt andmeimportija alamtöötleja osalusel[67]).

[67] Vt allmärkus 26.

Täiendavate meetmete näited

55. Mõne näite tehnilistest, lepingulistest ja korralduslikest meetmetest, mida võiks kaalutleda, kui neid ei ole juba kasutatud isikuandmete kaitse üldmääruse artikli 46 kohases andmeedastusvahendis, võib leida 2. lisas kirjeldatud mitteammendavatest loeteludest.

***

56. 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 edastustoiminguid jätkata.

57. Kui te ei suuda leida või võtta tõhusaid täiendavaid meetmeid, mis tagaksid edastatavatele andmetele sisuliselt samaväärse kaitse, [68] 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.[69] Vastavalt teie kasutatavas isikuandmete kaitse üldmääruse artikli 46 kohases edastusvahendis sisalduvatele kaitsemeetmetele peab importija täielikult tagastama teile või hävitama andmed, mida olete sellesse kolmandasse riiki juba edastanud, ning nende koopiad.[70]

Näide.

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

58. 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

59. 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.

[68] 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 Andmekaitsenõukogu 10. novembri 2020. aasta soovitused 02/2020 Euroopa oluliste tagatiste kohta seoses järelevalvemeetmetega https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[69] C-311/18 (Schrems II), punkt 135.

[70] Vt lepingu tüüptingimuste otsuse 87/2010 lisa 12. tingimus; vt (valikuline) täiendav lõpetamistingimus lepingu tüüptingimuste otsuse 2004/915/EÜ lisas B.

2.5.1 Standardsed andmekaitseklauslid (isikuandmete kaitse üldmääruse artikli 46 lõike 2 punktid c ja d)

60. Kui kavatsete kehtestada täiendavaid meetmeid lisaks standardsetele andmekaitseklauslitele, ei ole teil vaja küsida pädeva järelevalveasutuse luba nende tingimuste või täiendavate kaitsemeetmete lisamiseks, kui tuvastatud täiendavad meetmed ei ole otseselt või kaudselt vastuolus standardsete andmekaitseklauslitega ja on piisavad tagamaks, et isikuandmete kaitse üldmäärusega tagatud kaitset ei kahjustata.[71] Andmeeksportija ja importija peavad tagama, et täiendavaid tingimusi ei saaks mõista viisil, mis piirab standardsetes andmekaitseklauslites 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 järelevalveasutustel on õigus neid täiendavaid tingimusi läbi vaadata, kui asjakohane (näiteks kaebuse või omal algatusel esitatud päringu korral).

61. Kui kavatsete muuta standardseid andmekaitseklausleid endid või kui lisatud täiendavad meetmed lähevad standardsete andmekaitseklauslitega otseselt või kaudselt vastuollu, ei käsitleta teid enam standardseid andmekaitseklausleid kasutavana[72] 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)

62. 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.[73]

63. Schrems II kohtuotsus on siduvate kontsernisiseste eeskirjade alusel tehtaval isikuandmete edastusel oluline, sest kolmandate riikide õigusaktid võivad mõjutada selliste vahenditega pakutavat kaitset.

---

[71] Isikuandmete kaitse üldmääruse põhjenduses 109 märgitakse: „Vastutavale töötlejale või volitatud töötlejale antud võimalus kasutada komisjoni või järelevalveasutuse vastu võetud standardseid andmekaitsetingimusi ei tohiks takistada vastutavat töötlejat või volitatud töötlejat lisamast standardsed andmekaitseklauslid laiemasse lepingusse, nagu näiteks kahe volitatud töötleja 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.

[72] Vt analoogia alusel: Euroopa Andmekaitsenõukogu vastu võetud arvamus 17/2020 Sloveenia järelevalveasutuse esitatud artikli 28 kohaste lepingu tüüptingimuste eelnõu kohta (isikuandmete kaitse üldmääruse artikli 28 lõige 8), mis sisaldab sarnast sätet („Lisaks tuletab andmekaitsenõukogu 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_en.pdf.

[73] C-311/18 (Schrems II), punkt 132.

64. Kõigile kohustustele, mis tuleb lisada, viidatakse ajakohastatud dokumendis WP256/257[74], millele kõik siduvatele kontsernidele kui edastusvahenditele tuginevad grupid peavad ühtlustama oma olemasolevad ja tulevased siduvad kontsernisisesed eeskirjad.

65. Kohus rõhutas, et andmeeksportija ja andmeimportija ülesanne on hinnata, kas asjaomases kolmandas riigis järgitakse ELi õigusega nõutavat kaitsetaset, et määrata, kas standardsete andmekaitseklauslite või siduvate kontsernisiseste 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 Ad hoc lepingutingimused (isikuandmete kaitse üldmääruse artikli 46 lõike 3 punkt a)

66. 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.[75] Seetõttu on Schrems II kohtuotsus ad hoc lepingutingimuste alusel tehtaval isikuandmete edastusel oluline, sest kolmandate riikide õigusaktid võivad mõjutada selliste vahenditega pakutavat kaitset.

2.6 6. samm. Taashinnake olukorda asjakohaste ajavahemike järel

67. 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).

68. 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

69. 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 Liidu Kohtu otsuses kohtuasjas C-311/18 (Schrems II)

[74] Artikli 29 töörühma töödokument, milles kehtestatakse siduvates kontsernisisestes eeskirjades sisalduvate elementide ja põhimõtete tabel (viimati muudetud ja vastu võetud 6. veebruaril 2018, WP 256 rev.01); artikli 29 töörühma töödokument, milles kehtestatakse siduvates kontsernisisestes eeskirjades sisalduvate elementide ja põhimõtete tabel (viimati muudetud ja vastu võetud 6. veebruaril 2018, WP 257 rev.01).
[75] C-311/18 (Schrems II), punkt 132.

rõhutatakse vajadust tagada isikuandmete edastamisel kolmandatesse riikidesse isikuandmete kaitse üldmäärusega loodud kaitsetaseme järjepidevus.[76]

70. Oma andmetele sisuliselt samaväärse kaitse tagamiseks peate eelkõige olema põhjalikult kursis oma edastustoimingutega. Peate ka kontrollima, et teie edastatavad andmed oleksid piisavad, asjakohased ja piirduksid sellega, mida on vaja nendeks eesmärkideks, milleks neid töödeldakse.

71. 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.

72. 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.

73. 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 Andmekaitsenõukogu nimel

Eesistuja

(Andrea Jelinek)

[76] 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 – Euroopa Liidu Kohus. See asutus esindab Euroopa Liidu kohtuvõimu ning jälgib koostöös liikmesriikide kohtutega, et Euroopa Liidu õigust kohaldataks ja tõlgendataks ühetaoliselt.
- Andmeeksportija – EMPs asuv vastutav või volitatud töötleja, kes edastab isikuandmeid kolmandas riigis asuvale vastutavale või volitatud töötlejale.
- Andmeimportija – kolmandas riigis asuv vastutav või volitatud töötleja, 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 andmeeksportijad 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.
- Standardsed andmekaitseklauslid – Euroopa Komisjoni vastu võetud andmekaitseklauslid seoses isikuandmete edastamisega EMPs ja sellest väljaspool asuvate vastutavate töötlejate ja volitatud töötlejate vahel. Euroopa Komisjoni vastu võetud standardsed andmekaitseklauslid on isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkti c ja lõike 5 alusel isikuandmete kaitse üldmääruse kohane edastusvahend.

2. LISA. TÄIENDAVATE MEETMETE NÄITED

74. Siin on näited täiendavatest meetmetest, mida saate kaalutleda, kui olete jõudnud 4. sammuni, mil tuleb võtta täiendavaid meetmeid. See loetelu ei ole ammendav. Võite uurida muid täiendavaid meetmeid. Tulevased tehnoloogilised, õiguslikud või organisatsioonilised arengud võivad viia uute täiendavate meetmete tekkeni, mida võite kaaluda. 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.

75. Mis tahes täiendavat meedet võib pidada tõhusaks Euroopa Liidu Kohtu otsuse Schrems II tähenduses ainult siis ja sellises ulatuses, milles see üksi või koos teistega kõrvaldab konkreetsed puudused, mis on tuvastatud teie hinnangus olukorra kohta kolmandas riigis seoses teie edastustoimingu suhtes kohaldatavate õigusaktide ja tavadega. Kui te ei suuda kokkuvõttes tagada sisuliselt samaväärsel tasemel kaitset, ei tohi te isikuandmeid edastada.

76. Vastutava töötleja või volitatud töötlejana võidakse teilt juba nõuda mõne käesolevas lisas kirjeldatud meetme rakendamist, et olla kooskõlas isikuandmete kaitse üldmäärusega. See tähendab, et EMPs töödeldavate isikuandmete suhtes, mis edastatakse kaitse piisavuse otsusega hõlmatud andmeimportijale või muudele kolmandatele riikidele, võib olla vaja kehtestada sarnased meetmed.[77]

2.1 Tehnilised meetmed

77. 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.[78]

78. Täiendava selguse huvides kirjeldatakse käesolevas jaos esimesi näiteid stsenaariumidest, mille korral mõned tehnilised meetmed võiksid olla tõhusad, et tagada sisuliselt samaväärne kaitsetase. See osa jätkub mõne stsenaariumiga, mille korral ei ole tuvastatud tehnilisi meetmeid sellise kaitsetaseme tagamiseks.

[77] Isikuandmete kaitse üldmääruse artikli 5 lõige 2 ja artikkel 32.
[78] C-311/18 (Schrems II), punkt 135.

Näited stsenaariumidest, mis viitavad juhtumitele, mille korral on tuvastatud *tõhusad* meetmed

79. 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. Need meetmed oleksid vajalikud, et tagada EMPs tagatavaga sisuliselt samaväärne kaitsetase, isegi kui riigiasutuste juurdepääs on kooskõlas importija riigi õigusega, kui praktikas läheb selline juurdepääs kaugemale sellest, mis on demokraatlikus ühiskonnas vajalik ja proportsionaalne[79]. Nende meetmete eesmärk on vältida juurdepääsu võimalikku rikkumist, 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 andmete seas andmesubjektide poolt teistes kontekstides kasutatavate seadmete, rakenduste, vahendite ja protokollide antud võrguidentifikaatoreid.

80. 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.

81. 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.

82. Stsenaariumides kirjeldatakse konkreetseid asjaolusid ja näitena võetud meetmeid. Stsenaariumide mis tahes muutmisega võib viia teistsuguste järeldusteni. Stsenaariumid viitavad

[79] Vt ELi põhiõiguste harta artiklid 47 ja 52, isikuandmete kaitse üldmääruse artikli 23 lõige 1 ja Euroopa Andmekaitsenõukogu 10. novembri 2020. aasta soovitused 02/2020 Euroopa oluliste tagatiste kohta seoses järelevalvemeetmetega.

olukordadele, kus on järeldatud, et kõigepealt on vaja võtta täiendavaid meetmeid, st kus kõnealuse edastustoimingu suhtes kohaldatakse praktikas kolmanda riigi probleemseid õigusakte.

83. Võib juhtuda, et vastutavad töötlejad 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 töötlejatel ja volitatud töötlejatel võib olla kohustus rakendada neid andmete töötlemisel EMP piires.

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

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

Kui

1. isikuandmeid töödeldakse enne edastamist, kasutades tugevat krüptimist, ja kontrollitakse importija isikusamasust;
2. krüptimisalgoritm ja selle parameetrid (nt võtme pikkus ja töörežiim, kui asjakohane) vastavad tehnika tipptasemele ja eeldatavasti on vastupidavad vastuvõtva riigi avaliku sektori asutuste tehtava krüptoanalüüsi suhtes, arvestades neile kättesaadavaid ressursse ja tehnilisi võimalusi (nt arvutusvõimsus jõuründe jaoks),[80]
3. krüptimise tugevuse ja võtmepikkuse puhul arvestatakse konkreetset ajavahemikku, mille vältel peab krüptitud isikuandmete konfidentsiaalsus olema kaitstud,[81]
4. krüptimisalgoritmi rakendab õigesti ja nõuetekohaselt hooldatud tarkvara, millel ei ole teadaolevaid puudusi ja mille vastavus valitud algoritmi nõuetele on verifitseeritud näiteks sertifitseerimisega,

---

[80] Et hinnata krüptimisalgoritmide tugevust, nende vastavust tehnika tasemele ja nende vastupidavust krüptoanalüüsile aja jooksul, võivad andmeeksportijad tugineda ELi ja selle liikmesriikide ametlike küberturvalisuse asutuste avaldatud tehnilistele suunistele. Vt nt ENISA aruanne „Milline on tehnika tase IT-turbe valdkonnas?“, 2019, https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security; Saksamaa föderaalse infoturbeameti suunised TR-02102 seeria tehnilistes suunistes ja aruanne „Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018“ aadressil https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

[81] Krüptograafiliste algoritmide kaitsevõime väheneb aja jooksul uute krüptoanalüüsi meetodite avastamise, uute andmetöötlusparadigmade, näiteks kvantandmetöötluse, ja olemasoleva andmetöötlusvõimsuse üldise suurenemise tõttu, v.a kui rakendatavad algoritmid on tõendatult teoreetiliselt turvalised. See probleem puudutab eelkõige avaliku võtme algoritme, mis kirjutamise ajal on tavakasutuses. Seega peab andmeeksportija arvestama, et ametiasutused võivad lubada juurdepääsu krüptitud andmetele punktis 80 kirjeldatud asjaoludel ja säilitada neid seni, kuni nende ressursid on dekrüptimiseks piisavad. Täiendavat meedet saab pidada tõhusaks üksnes siis, kui selline dekrüptimine ja sellele järgnev edasine töötlemine ei oleks sel ajal enam andmesubjektide õiguste rikkumine, näiteks seetõttu, et andmeid ei saa enam kasutada nende otseseks või kaudseks tuvastamiseks.

5. usaldusväärne võtmehaldus (loomine, kasutamine, talletamine, kui asjakohane, sidumine kavandatud vastuvõtja identiteediga, tühistamine),[82] ning
6. võtmed on säilitatud üksnes andmeeksportija kontrolli all või üksuse poolt, keda eksportija usaldab EMPs või jurisdiktsioonis, mis pakub sisuliselt samaväärset kaitsetaset, kui on tagatud EMPs,

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

2. näide. Pseudonüümitud andmete edastamine

85. Kõigepealt pseudonüümib 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,[83]
2. et täiendavat teavet säilitab üksnes andmeeksportija ja seda hoitakse eraldi liikmesriigis või kolmandas riigis, EMPs asuva eksportija poolt usaldatavas üksuses või jurisdiktsioonis, mis pakub sisuliselt samaväärset kaitsetaset, kui on tagatud EMPs,
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 tõendanud asjaomaste andmete põhjaliku analüüsiga ning arvestades kogu teavet, mida vastuvõtva riigi avaliku sektori ametiasutused võivad eeldatavalt omada ja kasutada, et pseudonüümitud isikuandmeid ei saa seostada tuvastatud või tuvastatava füüsilise isikuga isegi sellise teabega ristviitamise kaudu,

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

86. NB! Sageli võivad füüsilise isiku füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse identiteediga seotud tegurid, isiku asukoht või suhtlus internetipõhise

---

[82] NISTi eriväljaanne 800-57, võtmehalduse soovitused https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

[83] Kooskõlas isikuandmete kaitse üldmääruse artikli 4 lõikega 5: „pseudonüümimine – isikuandmete töötlemine sellisel viisil, et isikuandmeid ei saa enam seostada konkreetse andmesubjektiga ilma täiendavat teavet kasutamata, tingimusel et sellist lisateavet hoitakse eraldi ning selle suhtes kohaldatakse tehnilisi ja korralduslikke meetmeid tagamaks, et isikuandmeid ei omistata tuvastatud või tuvastatavale füüsilisele isikule“; lisaandmed võivad koosneda pseudonüümide ja nende asendatavate identifitseerimisatribuutidega samastatavatest tabelitest, krüptograafilistest võtmetest või muudest atribuutide teisendamise parameetritest või muudest andmetest, mis võimaldavad pseudonüümitud andmeid omistada tuvastatud või tuvastatavatele füüsilistele isikutele.

teenusega teatud hetkedel[84] võimaldada isiku tuvastamist isegi nime, aadressi või muude lihtsate tuvastustunnuste puudumisel.

87. Eriti on see nii siis, kui andmed käsitlevad teabeteenuste kasutamist (pöördumise kellaaeg, 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.

88. Arvestades ka seda, et teatud teabeteenuste kasutamine on olemuselt avalik või suurte ressurssidega pooled võivad neid ära kasutada, peavad vastutavad töötlejad olema eriti hoolikad, sest nende jurisdiktsiooni avaliku sektori asutused valdavad tõenäoliselt andmeid, kas ja kuidas nende uuritav isik on neid teabeteenuseid kasutanud.

89. Kui pseudonüümimisel teisendatakse isikuandmetes sisalduvad atribuudid krüptograafilise algoritmi abil, kohaldatakse allmärkustes 80 ja 81 esitatud juhiseid. Seega on soovitatav loobuda üksnes krüptograafia kasutamisest ja rakendada modifikatsioone, mis põhinevad tabelipõhistel mehhanismidel.

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

90. Andmeeksportija soovib edastada andmeid sihtkohta, kus õigusaktid ja/või tavad võimaldavad riigiasutustele juurdepääsu andmetele eksportija riigi ja sihtriigi vahelise transiidi ajal.

Kui

1. andmeeksportija edastab isikuandmed andmeimportijale sellises jurisdiktsioonis, kus seaduse ja/või tava kohaselt on avaliku sektori asutustel juurdepääs andmetele ajal, mil neid transporditakse interneti kaudu kõnealusesse kolmandasse riiki ilma sellise juurdepääsuga seotud oluliste Euroopa tagatisteta, kasutatakse transpordi krüptimist, mille korral on tagatud, et kasutatavad krüptimisprotokollid on tipptasemel ning pakuvad tõhusat kaitset aktiivsete ja passiivsete rünnakute eest ressurssidega, mis on selle kolmanda riigi ametiasutustele teadaolevalt kättesaadavad;
2. side pooled lepivad kokku usaldusväärse avaliku võtme sertifitseerimisasutuse või -taristu kasutamise,
3. transpordi krüptimist võimaldavate saatja- ja vastuvõtusüsteemide aktiivsete ja passiivsete rünnete vastu kasutatakse spetsiaalseid kaitse- ja tehnikataseme meetmeid, sealhulgas tarkvara puuduste ja võimalike nn tagauste testimist;
4. kui krüptitud edastus ise ei taga piisavat turvet, arvestades kogemusi kasutatava taristu või tarkvara haavatavustega, otspunktkrüptitakse isikuandmed ka rakenduskihil, kasutades tipptasemel krüptimismeetodeid,

[84] 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, 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;“.

5. krüptimisalgoritm ja selle parameetrid (nt võtme pikkus ja töörežiim, kui asjakohane) vastavad tehnika tipptasemele ning eeldatavasti taluvad andmete vastavasse kolmandasse riiki edastamisel avaliku sektori asutuste tehtavat krüptoanalüüsi, arvestades neile kättesaadavaid ressursse ja tehnilisi võimalusi (näiteks arvutusvõimsus jõuründe jaoks) (vt eespool allmärkus 80),[85]
6. krüptimise tugevus arvestab konkreetset ajavahemikku, mille vältel peab krüptitud isikuandmete konfidentsiaalsus olema kaitstud,
7. krüptimisalgoritmi rakendab õigesti ja nõuetekohaselt hooldatud tarkvaraga, millel puuduvad teadaolevalt nõrgad kohad ja mille vastavus valitud algoritmi nõuetele on verifitseeritud näiteks sertifitseerimisega,
8. eksportija või tema volitatud üksuse võtmehaldus (loomine, kasutamine, talletamine, kui asjakohane, sidumine kavandatud vastuvõtja identiteediga, tühistamine) sisuliselt samaväärset kaitset tagavas jurisdiktsioonis on usaldusväärne,

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

4. näide. Kaitstud vastuvõtja

91. Andmeeksportija edastab isikuandmeid kolmandas riigis asuvale 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 töötleja teenuseid viisil, mis võimaldaks avaliku sektori asutustel saada andmetele juurdepääsu nende volitatud töötleja 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 dekrüptimisvõtmega võimalik (otspunktkrüptimine) kogu aja vältel, mil andmed peavad olema kaitstud,
5. dekrüptimisvõti on üksnes kaitstud andmeimportija ja võimaluse korral eksportija enda või eksportija poolt usaldatava muu üksuse, mis asub EMPs või jurisdiktsioonis, mis pakub sisuliselt samaväärset kaitset kui EMPs tagatud kaitsetase, ning mis on nõuetekohaselt kaitstud loata kasutamise või avalikustamise eest tehnika tasemele vastavate tehniliste ja korralduslike meetmetega, ning
6. andmeeksportija on usaldusväärselt tõestanud, et dekrüptimisvõti, mida ta kavatseb kasutada, vastab vastuvõtja valduses olevale dekrüptimisvõtmele,

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

---

[85] Vt allmärkus 80, kus on mõned viited ELi ja selle liikmesriikide ametlike küberturvalisuse asutuste avaldatud tehnilistele suunistele.

5. näide. Jagatud või ühine andmetöötlus

92. Andmeeksportija soovib, et isikuandmeid töötleksid vähemalt kaks eri jurisdiktsioonides asuvat sõltumatut volitatud töötlejat ühiselt ilma neile andmete sisu avaldamata. Enne edastamist jagab ta andmed nii, et mitte ükski ühe volitatud töötleja kätte jõudev osa ei ole isikuandmete täielikuks või osaliseks taastamiseks piisav. Andmeeksportija võtab töötlemise tulemuse vastu igalt volitatud töötlejalt 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 asuvale erinevale volitatud töötlejale,
3. volitatud töötlejad 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. vastutav töötleja on tõendanud asjaomaste andmete põhjaliku analüüsi alusel ja arvestades puuduvat teavet, mida vastuvõtvate riikide avaliku sektori ametiasutused võivad omada ja kasutada, et isikuandmete osi, mille ta edastab volitatud töötlejatele, ei saa seostada tuvastatud või tuvastatava füüsilise isikuga isegi sellise teabega ristviitamise kaudu,
6. puuduvad tõendid koostöö kohta vastavates iga volitatud töötleja asukoha jurisdiktsioonides asuvate avaliku sektori asutuste vahel, mis võimaldaks neil saada juurdepääsu volitatud töötlejate valduses olevatele kõigile isikuandmete kogumitele ja võimaldaks neil isikuandmete sisu taasluua 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 töötlejate valduses olevatele isikuandmetele,

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

Näited stsenaariumidest, mis viitavad juhtumitele, kus *tõhusaid* meetmeid ei tuvastata

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

6. näide. Edastamine pilveteenuste osutajatele või teistele töötlejatele, kellel on vaja krüptimata juurdepääsu andmetele

94. Andmeeksportija edastab isikuandmeid kas elektroonilise edastamise teel või pilveteenuse osutajale või muule volitatud töötlejale, et lasta isikuandmeid töödelda kolmandas riigis (nt tehnilise toe pakkumiseks või mis tahes liiki pilvetöötluseks), ning neid andmeid ei pseudonüümita või neid ei saa pseudonüümida, nagu on kirjeldatud näites 2, või krüptida, nagu on kirjeldatud näites 1, sest töötlemiseks on vaja juurdepääsu krüptimata andmetele.

Kui

1. vastutav töötleja edastab andmeid pilveteenuse osutajale või muule volitatud töötlejale,
2. pilveteenuse osutajal või muul volitatud töötlejal on vaja määratud ülesande täitmiseks krüptimata juurdepääsu andmetele ning
3. vastuvõtjariigi ametiasutustele antud õigus juurdepääsuks kõnealustele edastatud andmetele läheb kaugemale sellest, mis on vajalik ja proportsionaalne demokraatlikus ühiskonnas, kus kõnealuse edastamise suhtes kohaldatakse praktikas kolmanda riigi probleemseid õigusakte (vt 3. etapp),[86]

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

95. 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.

7. näide. Isikuandmete edastamine ärilistel eesmärkidel, sealhulgas kaugjuurdepääsu teel

96. Andmeeksportija edastab isikuandmed kolmandas riigis asuvatele üksustele, et neid saaks kasutada ühistel ärilistel eesmärkidel, kas elektroonilise edastamise teel või tehes need kättesaadavaks andmeimportija kaugjuurdepääsule, ning neid andmeid ei pseudonüümita või ei saa pseudonüümida, nagu on kirjeldatud näites 2, või krüptida, nagu on kirjeldatud näites 1, sest töötlemine nõuab juurdepääsu krüptimata andmetele. 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[87] töötleb krüptimata andmeid kolmandas riigis (sealhulgas enda tarbeks, kui importija on vastutav töötleja);
3. vastuvõtjariigi ametiasutustele antud õigus juurdepääsuks edastatavatele andmetele läheb kaugemale sellest, mis on vajalik ja proportsionaalne demokraatlikus ühiskonnas, kus

[86] Vt ELi põhiõiguste harta artiklid 47 ja 52, isikuandmete kaitse üldmääruse artikli 23 lõige 1 ja Euroopa Andmekaitsenõukogu 10. novembri 2020. aasta soovitused 02/2020 Euroopa oluliste tagatiste kohta seoses järelevalvemeetmetega.

[87] Kolmandas riigis asuv vastutav või volitatud töötleja, kes võtab vastu EMPst edastatud isikuandmeid või saab neile juurdepääsu.

kõnealuse edastamise suhtes kohaldatakse praktikas kolmanda riigi probleemseid õigusakte (vt 3. samm);

siis ei suuda Euroopa Andmekaitsenõukogu näha ette tõhusat tehnilist meedet, mis takistaks sellise juurdepääsu korral andmesubjekti põhiõiguste rikkumist.

97. 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.

2.2 Täiendavad lepingulised meetmed

98. Tavaliselt koosnevad sellised meetmed ühepoolsetest, kahepoolsetest või mitmepoolsetest[88] lepingulistest kohustustest.[89] 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.[90]

99. 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 EMPs tagatuga sisuliselt samaväärne kaitsetase. Arvestades lepinguliste meetmete olemust, mis üldiselt ei saa olla siduvad vastava kolmanda riigi ametiasutustele, kui nad ei ole lepingu pooled,[91] võib need meetmed tihti osutuda vajalikuks kombineerida muude tehniliste ja korralduslike meetmetega, et tagada nõutav andmekaitse tase. Neist ühe või mitme meetme valimine ja rakendamine ei pruugi tingimata ja süstemaatiliselt tagada, et teie edastustoimingud vastavad ELi õigusega nõutavale sisulise samaväärsuse standardile.

100. 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.

101. Nagu öeldud, ei suuda lepingulised meetmed välistada sellise Euroopa Andmekaitsenõukogu Euroopa oluliste tagatiste standardile mittevastava kolmanda riigi õigusaktide kohaldamist juhtudel, kui õigusaktid kohustavad importijaid täitma avaliku sektori asutustelt saadud andmete avaldamise korraldusi.[92]

102. Mõni selliste potentsiaalsete lepinguliste meetmete näide on allpool ning liigitatud olemuse järgi.

Lepingukohustuses konkreetsete tehniliste meetmete kasutamise sätestamine

103. Olenevalt edastamise konkreetsetest asjaoludest (sealhulgas kolmanda riigi õigusaktide praktilisest kohaldamisest) võib olla vaja sätestada lepingus, et edastamise toimumiseks tuleb rakendada konkreetseid tehnilisi meetmeid (vt soovitatavad tehnilised meetmed eespool).

104. Tõhususe eeldused:

---

[88] Näiteks siduvate kontsernisiseste eeskirjade raames, mis peaksid alati reguleerima mõningaid allpool loetletud meetmeid.

[89] 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.

[90] Vt otsuse C-311/18 (Schrems II) punkt 137, milles kohus tunnustas, et standardsed andmekaitseklauslid sisaldasid „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.

[91] C-311/18 (Schrems II), punkt 125.

[92] Euroopa Liidu Kohtu otsus C-311/18 (Schrems II), punkt 132.

- 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

105. Eksportija võib lisada lepingule lisad teabega, mida importija oleks pidanud esitama oma parimate võimaluste alusel seoses avaliku sektori ametiasutuste juurdepääsuga andmetele enne lepingu sõlmimist, sealhulgas luure valdkonnas, kui sihtriigi õigusaktid on kooskõlas Euroopa Andmekaitsenõukogu Euroopa oluliste tagatistega. See võib aidata andmeeksportijal täita kohustust dokumenteerida oma hindamine kolmanda riigi kaitsetaseme kohta. Samuti võib ta rõhutada importija kohustust abistada eksportijat hindamisel ja võtta endale kohustus esitada talle objektiivset, usaldusväärset, asjakohast, kontrollitavat ja avalikult kättesaadavat või muul viisil kättesaadavat teavet.

106. 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 konkreetses järelevalvevaldkonnas; seoses asutuse tüübiga, mille hulka andmeimportija kuulub jne);

(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[93], 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;[94]

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

107. 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.

---

[93] Perioodi pikkus peab sõltuma asjaomase edastamisega hõlmatud andmesubjektide õigustele ja vabadustele tekkivast riskist – näiteks viimane aasta enne andmete eksportimise vahendi sulgemist andmeeksportijaga.

[94] Selle kohustuse täitmine ei tähenda iseenesest piisaval tasemel kaitse tagamist. Samas tekitab mis tahes tegelikult toimunud sobimatu andmete avaldamisega vajadus rakendada täiendavaid meetmeid.

108. Tõhususe eeldused:

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

***

109. 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.[95]

110. 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.
- 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.
- Olukorras, kus andmeimportija avalikustas isikuandmed, mis on edastatud valitud edastusvahendis sisalduvaid kohustusi rikkudes, võib leping hõlmata ka andmeimportijalt andmesubjektile tekitatud materiaalse ja mittevaralise kahju hüvitamist.

***

111. Eksportija võib tugevdada oma volitusi importija andmetöötluskohtade auditeerimiseks[96] 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

[95] See tingimus on oluline, et tagada edastatavatele isikuandmetele piisav kaitse, ning tavaliselt tuleb seda nõuda.
[96] Vt näiteks otsuses 2010/87/EL vastutavate töötlejate ja volitatud töötlejate vaheliste lepingu tüüptingimuste 5. tingimuse punkt f; auditeid saab sätestada ka toimimisjuhendis või sertifitseerimise kaudu.

kontrolliorganite kiire sekkumise ja tugevdavad eksportija autonoomsust kontrolliorganite valimisel.

112. 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.
- Juurdepääsu logid ja muud sarnased jäljed peaksid olema võltsimiskindlad (nt need tuleks teha mittemuudetavateks, kasutades tipptasemel krüptimistehnikaid, näiteks räsimist, ning edastada korrapäraselt eksportijale), et audiitorid saaksid leida avalikustamise tõendeid. Pääsulogid ja muud sarnased jäljed peavad eristama ka korralistest töötoimingutest tulenevat juurdepääsu ning juurdepääsu, mis tulenevad korraldustest või juurdepääsunõuetest.

***

113. 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 olukorra muutumise korral viivitamata oma suutmatusest täita lepingulisi kohustusi ning seega ka nõutavat „sisuliselt samaväärsel tasemel andmekaitse“ standardit.[97]..

114. Selline suutmatus kohustusi täita võib tuleneda kolmanda riigi õigusaktide või praktika muutumisest.[98] 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.

115. Tõhususe eeldused:

- Teatamine peab toimuma enne andmetele 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 poliitikate 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.

---

[97] Lepingu tüüptingimuste otsuse 2010/87/EÜ 5. tingimuse punkt a ja punkti d alapunkt i.

[98] 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.“

- Tingimustes tuleb sätestada kiirmehhanism, mille alusel andmeeksportija volitab andmeimportijat andmeid kohe turvama või tagastama need andmeeksportijale või (kui see ei ole teostatav) ilma eksportija juhiseid tingimata ootamata andmed kustutama või turvaliselt krüptima[99], kui on jõutud andmeeksportija ja andmeimportija vahel kokku lepitud konkreetse 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.

***

116. 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.

117. 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 privaatvõtit 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

118. 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.

119. Tõhususe eeldused:

[99] See künnis peaks tagama, et andmesubjektidele tagatakse jätkuvalt kaitsetase, mis on samaväärne EMPs tagatuga.

- 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.

***

120. Eespool kirjeldatuga samas olukorras võib importija kohustuda teavitada taotlevat avaliku sektori asutust korralduse sobimatusest isikuandmete kaitse üldmääruse artikli 46 kohases edastusvahendis sisalduvate kaitsemeetmetega[100] 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.

121. 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.

Andmesubjektide jõustamine oma õiguste kasutamiseks

122. Lepinguga võib sätestada, et tavapärase tööprotsessi (sealhulgas tugitegevuse) käigus lihttekstina edastatavatele isikuandmetele on juurdepääs võimalik ainult eksportija ja/või andmesubjekti otsesel või kaudsel kokkuleppel konkreetse juurdepääsu saamiseks andmetele.

123. Tõhususe eeldused:

---

[100] Standardsetes andmekaitseklauslitega 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 puutumatuse õigust seoses isikuandmete töötlemisega ning mis on kohaldatav vastutava andmetöötleja suhtes liikmesriigis, kus andmeeksportija asub“.* Euroopa Liidu 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.

- 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) (nt töötajate korral).[101]
- 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.

***

124. 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), sealhulgas nõuda andmeimportijalt mis tahes materiaalse ja mittevaralise kahju hüvitamist, mis on tekkinud tema valitud edastusvahendi alusel sellega sätestatud kohustusi rikkudes edastatud isikuandmete avalikustamise tõttu.

125. Tõhususe eeldused:

- Sellise teate abil võib hoiatada andmesubjekti kolmanda riigi avaliku sektori asutuste potentsiaalsest juurdepääsust tema andmetele. Seega võib see anda andmesubjektile võimaluse taotleda eksportijatelt 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 ametiasutuste 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.

***

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

127. Tõhususe eeldused:

[101] Isikuandmete kaitse üldmääruse artikli 4 lõige 11.

- Mõned riiklikud eeskirjad ei pruugi võimaldada andmeimportijal pakkuda sellist abi otse andmesubjektidele, kuigi need võivad võimaldada andmeimportijal hankida sellist abi andmesubjektidele.
- 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, muu hulgas järelevalvemeetmete vastu.

2.3 Korralduslikud meetmed

128. 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 korralduslikke meetmeid olla vaja lepinguliste ja/või tehniliste meetmete täiendamiseks, et tagada isikuandmetele ELis tagatuga sisuliselt samaväärne kaitsetase.

129. Sobivaimad meetmed tuleb leida juhtumipõhisel hindamisel, arvestades vastutavate töötlejate ja volitatud töötlejate vajadust järgida vastutuse põhimõtet. Allpool esitab Euroopa Andmekaitsenõukogu korralduslike meetmete mõne näite, mida eksportijad võivad kasutada, kuigi loetelu ei ole ammendav ja sobida võivad ka muud meetmed.

Edastamise haldamise sise-eeskirjad, eelkõige ettevõtete kontsernide korral

130. Piisavate sisepoliitikate vastuvõtmine, milles selgelt nimetatakse andmete edastamisega seotud vastutusalad, 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 infotehnoloogia, andmekaitse- ja privaatsusõiguse ekspertidest koosneva rühma nimetamist, kes käsitleb EMPst 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.

131. 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.

132. Tõhususe eeldused

- Neid poliitikaid võib näha ette ainult juhtudeks, kui kolmanda riigi avaliku sektori asutuste taotlus on kooskõlas ELi õigusega.[102] Kui taotlus ei ole kooskõlas, ei piisa neist poliitikatest, et

[102] Vt kohtuasi C-362/14 (Schrems I), punkt 94; kohtuasi C-311/18 (Schrems II), punktid 168, 174, 175 ja 176.

tagada isikuandmete samaväärne kaitse, ning edastamine tuleb, nagu märgitud eespool, peatada või rakendada asjakohaseid täiendavaid meetmeid juurdepääsu takistamiseks.

Läbipaistvuse ja vastutuse tagamise meetmed

133. 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 asjaomastele andmesubjektidele.

134. 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 edastamine peatada, kui see suutmatus tekitaks võimetuse tagada piisav kaitsetase.

***

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

136. 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.

Korralduslikud meetodid ja võimalikult väheste andmete kogumise meetmed

137. Edastamise kontekstis võivad olla kasulikud ka juba vastutuse põhimõtte alusel kasutusele võetud organisatsioonilised nõuded, näiteks range ja granulaarse andmetele juurdepääsu ning konfidentsiaalsuse poliitikad ja parimad tavad, mille aluseks on range vajaduspõhisuse põhimõte ning mille üle tehakse regulaarsete auditite vormis järelevalvet ja mida jõustatakse distsiplinaarmeetmete 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).

138. Tõhususe eeldused

- Võimalikult väheste andmete kogumise meetmete järelevalveks ja jõustamiseks ka edastamise kontekstis peavad kasutusel olema regulaarsed auditid ja mõjuvad distsiplinaarmeetmed.
- Andmeeksportija 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.

***

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

140. Tõhususe eeldused

- Andmekaitseametnikule (kui olemas) ning õigus- ja siseauditi talitusele 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

141. Rangete andmeturbe- ja andmeprivaatsuspoliitikate vastuvõtmine ELi sertifikaadi või toimimisjuhendite või rahvusvaheliste standardite (nt ISO normide) ja parimate tavade (nt ENISA) alusel, arvestades tehnika taset, kooskõlas töödeldavate andmekategooriate riskiga.

Muu

142. 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.

***

143. 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.[103]

[103] C-311/18 (Schrems II), punktid 135 ja 137.

3. LISA. VÕIMALIKUD TEABEALLIKAD KOLMANDA RIIGI HINDAMISEKS

144. Teie andmeimportijal võib olla võimalus esitada teile asjakohaseid allikaid ja teavet enda asukohaks oleva kolmanda riigi ja edastatud andmete importija suhtes kohaldatavate õigusaktide ja tavade kohta. Te võite ja importija viidata mitmele teabeallikale, näiteks allpool mitteammendavalt loetletud ja eelistusjärjekorras esitatud teabeallikatele:

- Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu praktika[104], millele viidatakse Euroopa oluliste tagatiste soovitustes;[105]
- sihtriigi kaitse piisavuse otsused, kui edastamine tugineb muule õiguslikule alusele;[106]
- valitsusvaheliste organisatsioonide, näiteks Euroopa Nõukogu,[107] muude piirkondlike organite[108] ning ÜRO organite ja asutuste (nt ÜRO Inimõiguste Nõukogu,[109] inimõiguste komitee[110]) resolutsioonid ja aruanded;
- pädevate regulatiivvõrgustike, näiteks ülemaailmse privaatsusassamblee (GPA) aruanded ja analüüsid;[111]
- riikide kohtupraktika või kolmandate riikide andmeprivaatsuse ja andmekaitse suhtes pädevate sõltumatute kohtu- või haldusasutuste otsused;
- sõltumatute järelevalve- või parlamentaarsete organite aruanded;
- aruanded, mis põhinevad praktilistel kogemustel, mis on saadud varasematel avaliku sektori asutuste esitatud avalikustamistaotlustel või selliste taotluste puudumisel importijatega samas sektoris tegutsevatelt üksustelt;
- teiste importijatega samas valdkonnas andmeid töötlevate üksuste kanaarid;
- aruanded, mille on koostanud või tellinud eksportija kaubanduskojad, äri-, kutse- ja kaubandusliidud, valitsusasutused, diplomaatilised, kaubandus- ja investeerimisasutused või muud kolmandad riigid, kes ekspordivad kolmandasse riiki, kuhu andmeid edastatakse;
- akadeemiliste asutuste ning kodanikuühiskonna organisatsoonide (nt vabaühenduste) aruanded.
- erasektori äriteabe pakkujate aruanded ettevõtete finants-, regulatiiv- ja mainega seotud riskide kohta;

---

[104] Vt Euroopa Inimõiguste Kohtu teabedokument kohtupädevuse kohta seoses massilise jälitustegevusega: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[105] Vt Euroopa Andmekaitsenõukogu 10. novembri 2020. aasta soovitused 02/2020 Euroopa oluliste tagatiste kohta jälgimismeetmete kontekstis, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en

[106] 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_en

[107] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[108] Vt näiteks Ameerika Inimõiguste Komisjoni (IACHR) riigiaruanded, https://www.oas.org/en/iachr/reports/country.asp.

[109] Vt https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx

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

[111] Vt https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

- importija enda kanaarid;[112]
- läbipaistvusaruanded, tingimusel et neis mainitakse sõnaselgelt asjaolu, et juurdepääsutaotlusi ei saadud. Läbipaistvusaruandeid, kus seda ei mainita, ei saaks pidada piisavaks tõendusmaterjaliks, sest nendes aruannetes keskendutakse kõige sagedamini õiguskaitseasutustelt saadud juurdepääsutaotlustele ja esitatakse arvandmed ainult selle aspekti kohta, jättes märkimata riikliku julgeoleku eesmärgil saadud juurdepääsutaotlused. See ei tähenda, et juurdepääsutaotlusi ei saadud, vaid et seda teavet ei saa jagada; [113]
- Importija ettevõttesisesed avaldused või dokumendid, milles on selgelt märgitud, et juurdepääsutaotlusi ei ole esitatud piisavalt pika aja jooksul; ning eelistades avaldusi ja dokumente, mis hõlmavad importija vastutust ja/või mille annavad välja asutusesisesed ametikohad, kellel on teatav autonoomia, näiteks siseaudiitorid, andmekaitseametnikud jne.[114]

[112] Vt tingimused importija dokumenteeritud praktiliste kogemuste arvessevõtmiseks seoses kolmandate riikide ametiasutustelt saadud juurdepääsutaotluste asjakohaste varasemate juhtumitega punktis 47.
[113] *Ibid.*
[114] *Ibid.*