

Euroopa Andmekaitseenõukogu dokumendid



Olulised andmekaitsemeetmed EMP andmekaitseasutuste ja kolmandate riikide pädevate andmekaitseasutuste vahelises täitmise tagamise alases koostöös

Vastu võetud 14. märtsil 2022

Euroopa Andmekaitsekoogu,

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 u ja artikli 50 punkti a,

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

võttes arvesse töökorra artikleid 12 ja 22,

ON VASTU VÕTNUD JÄRGMISE DOKUMENDI.

Seoses isikuandmete kaitse üldmääruse artikliga 50, mis käsitleb rahvusvahelist koostööd kolmandate riikide pädevate andmekaitseasutustega, on välja töötatud järgmised olulised andmekaitsemeetmed, mis tuleb võtta lisaks täitmise tagamise koostöölepingule või lisada sellesse.

Need kaitsemeetmed võib sätestada kas halduskokkuleppes või rahvusvahelises lepingus. Nende sõnastust tuleb vastavalt kohandada sõltuvalt sellest, kas väljatöötatav vahend on halduskokkulepe või rahvusvaheline leping, ning käsitletava andmeedastuse konkreetsetest asjaoludest. Nagu on märgitud Euroopa Andmekaitsekoogu suunistes 2/2020 isikuandmete kaitse üldmääruse artikli 46 lõike 2 punkti a ja lõike 3 punkti b kohta,² tuleb halduskokkulepete puhul võtta konkreetseid meetmeid, et tagada tõhusad individuaalsed õigused, õiguskaitse ja järelevalve, eelistatavalt vastu võtva poole kinnituse kaudu, et tema siseriiklikus õiguses on juba ette nähtud olulised kaitsemeetmed. Rahvusvaheliste lepingutega võib kehtestada kaitsemeetmeid otse rahvusvahelise lepingu raames või tugineda kolmanda riigi õiguses juba olemasolevatele elementidele.

Konkreetselt halduskokkuleppeid käsitlevad osad on esile tõstetud hallil taustal, konkreetselt rahvusvahelisi lepinguid käsitlevad osad on esile tõstetud sinisel taustal.

¹ Viiteid liikmesriikidele tuleks mõista viidetena „EMP liikmesriikidele“.

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

I. Mõisted³

Käesolevas dokumendis:

a) „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, või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal;

b) „isikuandmete töötlemine“ („töötlemine“) – isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamine, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, töötlemise piiramine, kustutamine või hävitamine;

c) „[lepingu]poolte⁴ pädev asutus“ – andmekaitsealaste õigusaktide täitmise tagamise pädevusega asutus, [X] EMPs ja [Y] kolmandas riigis. Käesoleva dokumendi kohastel pädevatel asutustel on regulatiivsed volitused ja kohustused, mis hõlmavad andmekaitsestandardite kohaldamise järelevalvet ja jõustamist, kaebuste käsitlemist, andmekaitsestandardite võimalike rikkumiste uurimist ja vajaduse korral sanktsioonide kehtestamist;

d) „vastu võtva pädev asutus“ – pädev asutus, kes saab teiselt pädevalt asutuselt edastatud isikuandmeid;

e) „isikuandmete jagamine“ – isikuandmete edasijagamine EMP pädevalt andmekaitseasutuselt andmeid vastu võtva pädeva asutuse poolt oma riigis asuva kolmanda isikuga kooskõlas [täitmise tagamise koostöölepinguga];

f) „edasisaatmine“ – isikuandmete edastamine vastuvõtva pädeva asutuse poolt teises riigis asuvalle kolmandale isikule;

g) „isikuandmete / tundlike andmete erikategooriad“ – andmed, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, samuti andmetöötlus, mis hõlmab geneetilisi andmeid, füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid, samuti terviseandmed või andmeid füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta ning süüdimõistvate kohtuotsuste ja süütegudega seotud andmed;

h) „kohaldatavad siseriiklikud andmekaitsealased õigusaktid“ – [kohaldatavad õigusaktid];

[i) „täitmise tagamise alane koostööleping“⁵ – täitmise tagamise alane koostööleping [kolmanda riigi pädeva asutuse] ja [EMP ametiasutuse] vahel koostöö hõlbustamiseks ja teabevahetuseks;]]⁶

³ Need määratlused tulenevad isikuandmete kaitse üldmäärusest.

⁴ Esitatakse rahvusvahelises lepingus.

⁵ Siia tuleks lisada lepingu nimi ning EMP ja kolmanda riigi kahe asjaomase asutuse nimetused.

⁶ See määratlus tuleks esitada halduskokkuleppe kontekstis, kuna rahvusvaheline leping peaks sisaldama nii andmekaitsemeetmeid kui ka asjakohaseid koostööklausleid.

j) „isikuandmetega seotud rikkumine” – turvanõuete rikkumine, mis põhjustab edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu;

k) „profiilianalüüs” – igasugune isikuandmete automatiseeritud töötlemine, mis hõlmab isikuandmete kasutamist füüsilise isikuga seotud teatavate isiklike aspektide hindamiseks, eelkõige selliste aspektide analüüsimiseks või prognoosimiseks, mis on seotud asjaomase füüsilise isiku töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste, huvide, usaldusväärseuse, käitumise, asukoha või liikumisega;

l) „andmesubjekti õigused” viitab käesolevas lepingus järgmisele:

– „õigus teabele” – andmesubjekti õigus saada teavet temaga seotud isikuandmete töötlemise kohta kokkuvõtlikul, läbipaistval, arusaadaval ja kergesti kättesaadaval kujul;

– „juurdepääsuõigus” – andmesubjekti õigus saada pädevalt asutuselt, kes saadab andmeid või võtab neid vastu, kinnitus selle kohta, kas teda käsitlevaid isikuandmeid töödeldakse või mitte, samuti õigus saada konkreetset teavet töötlemise kohta, sealhulgas töötlemise eesmärgi, asjaomaste isikuandmete kategooriate, vastuvõtjate, kellele isikuandmed avaldatakse, kavandatud säilitamisaja ja õiguskaitsevõimaluste kohta, ning õigus vajaduse korral tutvuda tema kohta kogutud isikuandmetega ning kasutada seda õigust hõlpsasti ja mõistlike ajavahemike järel, et olla teadlik töötlemise seaduslikkusest ja seda kontrollida;

– „õigus nõuda andmete parandamist” – andmesubjekti õigus nõuda oma ebatäpsete isikuandmete parandamist või täiendamist lepingupoole poolt põhjendamatu viivitusega;

– „õigus nõuda andmete kustutamist” – andmesubjekti õigus nõuda oma isikuandmete kustutamist lepingupoole poolt, kui isikuandmed ei ole enam vajalikud sellel eesmärgil, milleks neid koguti või töödeldi, või kui andmeid on kogutud või töödeldud ebaseaduslikult;

– „õigus esitada vastuväiteid” – andmesubjekti õigus esitada oma konkreetse olukorraga seotud põhjustel igal ajal vastuväiteid teda käsitlevate isikuandmete töötlemisele lepingupoole poolt, mille tagajärjel asjaomane pool lõpetab andmete töötlemise, välja arvatud juhul, kui pool tõendab, et töötlemine toimub mõjuvatel õiguspärastel põhjustel, mis kaaluvad üles andmesubjekti huvid, õigused ja vabadused, või et töötlemine on vajalik õigusnõude koostamiseks, esitamiseks või kaitsmiseks;

– „õigus töötlemist piirata” – andmesubjekti õigus piirata oma isikuandmete töötlemist, kui ta on isikuandmete täpsuse vaidlustanud, ajavahemikuks, mis võimaldab vastutaval töötlejal kontrollida isikuandmete täpsust; kui töötlemine on ebaseaduslik ja andmesubjekt on isikuandmete kustutamise vastu ja taotleb selle asemel nende kasutamise piiramist; kui lepingupool ei vaja enam isikuandmeid sel eesmärgil, milleks need koguti, ja andmesubjekt on andmete kustutamise vastu, kuid andmesubjekt vajab neid õigusnõude koostamiseks, esitamiseks või kaitsmiseks;

– „õigus välistada automatiseeritud otsused, sealhulgas profiilianalüüs” – andmesubjekti õigus nõuda, et tema suhtes ei tehta otsuseid, mis põhinevad üksnes automatiseeritud töötlemisel, sealhulgas profiilianalüüsil, ning millel on teda puudutavad õiguslikud tagajärjed või mis teda sarnasel viisil oluliselt mõjutavad.

II – DOKUMENDI EESMÄRK JA KOHALDAMISALA

Käesoleva dokumendi eesmärk on näha ette asjakohased kaitsemeetmed [ja asjakohane konfidentsiaalsuse kaitse⁷] seoses isikuandmetega, mille asutus [X] edastab asutusele [Y] isikuandmete kaitse üldmääruse artikli 46 lõike 3 kohaselt, ning [täitmise tagamise alase koostöölepingu / käesoleva dokumendi] kohase koostöö käigus. [Täitmise tagamise alase koostöölepingu / käesoleva dokumendi] alusel mõjutatud, edastatavate ja töödeldavate isikuandmete kategooriad on lepingupooled loetlenud eraldi lisas.

Lepingupooled lepivad kokku, et [täitmise tagamise alases koostöölepingus / käesolevas dokumendis] sätestatud isikuandmete edastamist asutuste [X] ja [Y] vahel reguleeritakse käesoleva dokumendi sätetega [täitetoimingute teostamisel]⁸ / [seoses vastavate täitetoimingute teostamisega pädevate asutuste poolt]⁹. [Käesoleva dokumendi eesmärk on täiendada täitmise tagamise koostöölepingut asutuste [X] ja [Y] vahel.]¹⁰

[X] ja [Y] kinnitavad, et neil on volitused tegutseda kooskõlas käesoleva õigusakti tingimustega ning et neil ei ole põhjust uskuda, et kehtivad kohaldatavad õiguslikud nõuded seda takistavad.

[X] ja [Y] kinnitavad, et nad saavad kohaldatavate õiguslike nõuete alusel täielikult järgida käesolevas dokumendis sätestatud kaitsemeetmeid. [X] ja [Y] näevad ette kaitsemeetmed isikuandmete kaitseks, kombineerides selleks seadusi ja määrusi ning oma sise-eeskirju ja menetlusi.]¹¹

[Iga lepingupool tagab, et pädev asutus tegutseb kooskõlas käesoleva dokumendi tingimustega ja et ükski kohaldatav õigusnõue ei takista pädevat asutust seda tegemast]¹².

III – ANDMETÖÖTLUSE PÕHIMÕTTED

1. Eesmärgi piiramine: asutuste [X] ja [Y] vahel edastatud isikuandmeid võib andmeid vastu võttev pädev asutus ise töödelda üksnes selleks, et täita oma täitmise tagamise ülesandeid kooskõlas asutuse [X] puhul isikuandmete kaitse üldmäärusega ja asutuse [Y] puhul [kolmanda riigi kohaldatavate õigusaktidega], eesmärgiga tagada andmekaitsestandardite täitmine asutuste [Y] ja [X] jurisdiktsioonis. Selliste andmete edasijagamist, kui see on vajalik otseselt seotud uurimiste/kohtumenetluste jaoks, sealhulgas sellise jagamise eesmärki, reguleeritakse allpool punktis 7 ja see toimub asutuse [Y] poolt kooskõlas [kolmanda riigi asjakohaste kohaldatavate õigusaktidega] ja asutuse [X] poolt kooskõlas isikuandmete kaitse üldmääruse ja kohaldatavate siseriiklike õigusaktidega. [Y] ei töötle [X]-lt saadud isikuandmeid ühelgi muul eesmärgil, kui on käesolevas dokumendis sätestatud, ning vastastikkuse põhimõtte alusel ei töötle [X] [Y]-lt saadud isikuandmeid ühelgi muul eesmärgil, kui on käesolevas õigusaktis sätestatud.

⁷ Vt allpool dokumendi lõpus punkt IIIa, milles käsitletakse konfidentsiaalsuse ja ametisaladuse kaitset ja mis tuleb vajaduse korral lisada, sõltuvalt ka kolmanda riigi õigusaktidest.

⁸ Halduskokkuleppes.

⁹ Rahvusvahelises lepingus.

¹⁰ See tuleks ette näha halduskokkuleppe kontekstis.

¹¹ See tuleks lisada halduskokkuleppesse.

¹² Võib esitada rahvusvahelises lepingus.

2. Andmete kvaliteet ja proportsionaalsus: asutuste [X] ja [Y] edastatud isikuandmed peavad olema täpsed, piisavad, asjakohased ega tohi minna kaugemale nende edastamise ja hilisema töötlemise eesmärkidest. Pädev asutus teavitab teist pädevat asutust, kui ta saab teada, et varem edastatud või saadud teave on ebatäpne (ebaõige või aegunud) ja/või seda tuleb ajakohastada. Sellisel juhul teevad pädevad asutused kõik asjakohased parandused, võttes arvesse isikuandmete edastamise eesmärki; see võib vastavalt vajadusele hõlmata isikuandmete täiendamist, kustutamist, töötlemise piiramist, parandamist või muul viisil korrigeerimist.

Isikuandmeid tuleb säilitada kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik eesmärgil, milleks andmeid koguti või milleks neid edasi töödeldakse, või sellise aja jooksul, nagu on nõutud kohaldatavates õigusnormides, tingimusel, et asutus [X] on asutust [Y] teavitanud EMPs kohaldatavatest eeskirjadest ja nendes sätestatud maksimaalsest isikuandmete säilitamisajast, ning et asutus [Y] on asutust [X] teavitanud kohaldatavatest õigusnormidest ja nendes sätestatud maksimaalsest isikuandmete säilitamisajast ning seda maksimaalset ajavahemikku peetakse demokraatlikus ühiskonnas proportsionaalseks ja vajalikuks kooskõlas ELi standarditega. See teave esitatakse käesoleva dokumendi lisas. Lepingupooled kehtestavad asjakohase korra käesoleva dokumendi kohaselt saadud teabe lõplikuks hävitamiseks.

3. Läbipaistvus: [X] ja [Y] esitavad üldise teabe, avaldades käesoleva dokumendi oma veebisaidil. [Nii X kui ka Y] annavad andmesubjektidele teavet isikuandmete edastamise ja edasise töötlemise kohta. [Nii X kui ka Y] esitavad andmesubjektidele põhimõtteliselt üldise teabe järgmise kohta: a) kuidas ja miks ta võib isikuandmeid töödelda ja edastada; b) üksuste liigid, kellele võib selliseid andmeid edastada, c) kohaldatavate õiguslike nõuete kohaselt andmesubjektidele kättesaadavad õigused, sealhulgas see, kuidas neid õigusi kasutada; d) teave mis tahes kohaldatavate viivituste või piirangute kohta selliste õiguste kasutamisel, sealhulgas piirangute kohta, mida kohaldatakse isikuandmete edastamisel, ning e) kontaktandmed vaide või nõude esitamiseks. Teatamine jõustub, kui [X ja Y] avaldavad selle teabe koos käesoleva dokumendiga oma veebisaidil.

[X] esitab andmesubjektidele individuaalset teavet kooskõlas isikuandmete kaitse üldmääruses sätestatud teavitamisnõuete ning kohaldatavate erandite ja piirangutega (nagu on sätestatud isikuandmete kaitse üldmääruse artiklites 14 ja 23). Edasijagamise ja edasisaatmise korral esitab ka [Y] individuaalset teavet ja vastastikkuse põhimõtte alusel esitab [X] andmete edasijagamise ja edasisaatmise korral teavet [Y]-le.

Kui [X] jõuab pärast individuaalse teatamise suhtes kohaldatavate erandite kaalumist ja [Y]-ga peetud arutelusid arvesse võttes järeldusele, et isikuandmete kaitse üldmääruse kohaselt on ta kohustatud teavitama andmesubjekti tema isikuandmete jagamisest või edastamisest [Y]-le, teavitab [X] eelnevalt asutust [Y] sellisest individuaalsest teatamisest.

4. Turvalisus ja konfidentsiaalsus: [X] ja [Y] tunnistavad, et **I lisas** on [X] esitanud teavet, milles kirjeldatakse tema tehnilisi ja korralduslikke meetmeid kooskõlas isikuandmete kaitse üldmäärusega, ning et [Y] on esitanud teavet, milles kirjeldatakse tema tehnilisi ja korralduslikke turvameetmeid, mida [X] peab piisavaks, et kaitsta isikuandmeid juhusliku või ebaseadusliku hävitamise, kaotamineku, muutmise, avalikustamise või neile juurdepääsu eest. [Y] nõustub teavitama asutust [X] kõigist tehnilistes ja korralduslikes turvameetmetes tehtud muudatustest, mis võivad kahjustada käesoleva lepinguga tagatud isikuandmete kaitse taset, ning ajakohastab selliste muudatuste korral **I lisas** esitatud teavet. Sellisel juhul esitab [Y] sellise teate [X]-le vähemalt kaks kuud enne jõustumist.

Vastastikkuse põhimõtte alusel teavitab [X] samadel tingimustel asutust [Y] ja ajakohastab vastavalt I lisa.

[Y] on esitanud [X]-le kirjelduse oma kohaldatavatest konfidentsiaalsust käsitlevatest seadustest ja/või eeskirjadest ning mitteavaliku või konfidentsiaalse teabe ebaseadusliku avalikustamise tagajärgedest või nende seaduste ja/või eeskirjade rikkumise kahtlustest ja vastastikkuse põhimõtte alusel on [X] esitanud sama teabe [Y]-le^{13, 14}.

Kui vastuvõttev pädev asutus saab teada käesoleva dokumendi alusel edastatud isikuandmeid mõjutavast rikkumisest, teavitab ta sellest teist pädevat asutust põhjendamatu viivitusega ja võimaluse korral 24 tunni jooksul pärast seda, kui ta on saanud teada, et see mõjutab selliseid isikuandmeid. Samuti kasutab teavitav pädev asutus võimalikult kiiresti mõistlikke ja asjakohaseid vahendeid isikuandmetega seotud rikkumise lõpetamiseks ja võimaliku kahjuliku mõju minimeerimiseks.

[X] ja [Y] teavitavad ilma põhjendamatu viivitusega andmesubjekti isikuandmetega seotud rikkumisest, kui rikkumise tagajärjel tekib tõenäoliselt suur oht füüsilise isiku õigustele ja vabadustele, et võimaldada andmesubjektil võtta vajalikke ettevaatusabinõusid. Teatistes tuleb kirjeldada isikuandmetega seotud rikkumise olemust, samuti tuleks anda asjaomasele füüsilisele isikule soovitusi võimaliku kahjuliku mõju leevendamiseks. Sellised teatisted edastatakse andmesubjektidele niipea, kui see on mõistlikult võimalik, välja arvatud juhul, kui pädev asutus on rakendanud asjakohaseid tehnilisi ja korralduslikke kaitsemeetmeid ning neid meetmeid on kohaldatud isikuandmetega seotud rikkumisest mõjutatud isikuandmete suhtes, või kui ta on võtnud edasisi meetmeid, millega tagatakse, et suur oht andmesubjektide õigustele ja vabadustele tõenäoliselt ei realiseeru, või kui see nõuaks ebaproportsionaalseid jõupingutusi.

5. Andmesubjekti õigused: andmesubjekt, kelle isikuandmed on edastatud [Y]-le, võib kasutada oma andmesubjekti õigusi, mis on määratletud I artikli punktis j seoses dokumendi alusel saadud ja töödeldud andmetega.

Andmesubjekt võib esitada taotluse otse [X]-le või [Y]-le:

Asutuse [X] kontaktandmed:

– e-posti teel aadressil Xxx;

– posti teel aadressil:

XXXxxx

Asutuse [Y] kontaktandmed:

– e-posti teel aadressil Xxx;

– posti teel aadressil:

XXXxxx

¹³ Vt I lisa.

¹⁴ Rahvusvahelises lepingus: rahvusvaheline leping võib täiendada asutuse [Y] suhtes kohaldatavaid seadusi ja/või eeskirju, kui need asutuse [Y] õigusraamistikus puuduvad või on ebapiisavad, et tagada kaitsemeetmete asjakohane tase.

Andmesubjekt võib ka nõuda, et [X] teeks kindlaks kõik [Y]-le edastatud isikuandmed, ja taotleda, et [X] kinnitaks asutuse [Y] juures üle, et isikuandmed on täielikud, täpsed ja ajakohased ning et töötlemine toimub kooskõlas käesolevas dokumendis sätestatud isikuandmete töötlemise põhimõtetega. [Y] käsitleb mõistlikul ja õigeaegsel viisil kõiki selliseid asutuse [X] esitatud taotlusi seoses [X]-lt [Y]-le edastatavate isikuandmetega. Andmesubjekti taotluse saamisel võib [X] taotleda [Y]-lt teavet ka selliste isikuandmete edasijagamise ja -saatmise kohta, kui seda on vaja selleks, et [X] täidaks andmesubjekti vastu [isikuandmete kaitse üldmäärusest ja asutuse [Y] suhtes kohaldatavatest siseriiklikest õigusaktidest]¹⁵ / [käesolevast dokumendist]¹⁶ tulenevaid avalikustamiskohustusi. [X]-lt sellise taotluse saamisel esitab [Y] [X]-le kogu teabe, mis on tehtud [Y]-le kättesaadavaks seoses selliste isikuandmete töötlemisega kolmanda isiku poolt, kellega [Y] on selliseid isikuandmeid jaganud või kellele neid edastanud. [Y] käsitleb mõistlikul ja õigeaegsel viisil ka kõiki selliseid asutuse [X] esitatud taotlusi seoses [X]-lt [Y]-le edastatavate isikuandmetega.

[X] annab andmesubjektile ühe kuu jooksul pärast tema isikuandmete edastamist ka teavet tema taotluse alusel võetud meetmete kohta. [X] teatab andmesubjektile ühe kuu jooksul alates taotluse saamisest ka meetmete võtmata jätmise põhjused ning teavitab teda kaebuse esitamise ja õiguskaitsevahendi kasutamise võimalusest. [X] ja [Y] võivad võtta asjakohaseid meetmeid, näiteks küsida mõistlikke tasusid halduskulude katmiseks või keelduda tegutsemast andmesubjekti taotluse alusel, mis on ilmselgelt põhjendamatu või ülemäärane.

Andmesubjekti õigusi võib piirata, et vältida avalikku võimu teostavate pädevate asutuste järelevalve- või täitmise tagamise ülesannete kahjustamist; üldist avalikku huvi pakkuvatel olulistel eesmärkidel, mida tunnustatakse [asutuse Y kolmandas riigis] ja [pädevas liikmesriigis] või Euroopa Liidus, sealhulgas rahvusvahelise koostöö vastastikkuse põhimõttest juhindudes. Piirang peaks olema vajalik, proportsionaalne ja seadusega ette nähtud ning seda tuleb kohaldada ainult seni, kuni piirangu põhjus püsib.

Andmesubjekt võib esitada mis tahes vaide või nõude seoses oma isikuandmete töötlemisega käesoleva dokumendi alusel vastavalt vajadusele kas [X]-le, [Y]-le või mõlemale vastavalt 8. jaotises sätestatule.

[X] ja [Y] lepivad kokku, et nad ei tee andmesubjekti suhtes õiguslikku otsust, mis põhineb üksnes isikuandmete automatiseeritud töötlemisel, sealhulgas profiilialüüsil, ilma inimese osaluseta.

6. Eriliiki isikuandmed/tundlikud isikuandmed: [X] ei edasta punkti I alapunktis e määratletud eriliiki isikuandmeid /tundlikke isikuandmeid [Y]-le, välja arvatud juhul, kui need on vajalikud kaebuste menetlemiseks, andmekaitse-eeskirjade võimalike rikkumiste uurimiseks ja vajaduse korral parandusmeetmete kehtestamiseks. Kui neid edastatakse, kehtestab [Y] täiendavad kaitsemeetmed, mis määratakse kindlaks igal üksikjuhul eraldi, näiteks juurdepääsupiirangud, teabe töötlemise eesmärkide piirangud, edasisaatmise piirangud või konkreetsed kaitsemeetmed, näiteks täiendavad turvameetmed, milleks on nõutav teabele juurdepääsu omavate töötajate eriväljaõpe.

¹⁵ Halduskokkuleppes.

¹⁶ Rahvusvahelises lepingus.

7. Isikuandmete edasijagamine: [Y] jagab [X]-lt saadud andmeid ainult ¹⁷ [täitmise tagamise alases koostöölepingus]¹⁸ / [käesolevas dokumendis]¹⁹ nimetatud üksustega ja kui see on vajalik konkreetse täitemeetme jaoks.

Kui [Y] kavatses jagada isikuandmeid mis tahes [täitmise tagamise alases koostöölepingus]²⁰ / [käesolevas dokumendis]²¹ nimetatud kolmanda isikuga, taotleb [Y] [X]-lt eelnevalt kirjalikku luba ja jagab selliseid isikuandmeid üksnes juhul, kui kolmas isik kohustub järgima samu andmekaitse põhimõtteid ja kaitsemeetmeid, nagu on ette nähtud käesoleva dokumendiga. Sellise eelneva kirjaliku loa taotlemisel peaks [Y] märkima isikuandmete liigi, mida ta kavatses jagada, ning põhjused ja eesmärgid, miks [Y] kavatses isikuandmeid jagada. Kui [X] ei anna selliseks jagamiseks kirjalikku luba mõistliku aja jooksul, mis ei ületa kümnet päeva, konsulteerib [Y] [X]-ga ja kaalub võimalikke vastuväiteid. Kui [Y] otsustab jagada isikuandmeid ilma asutuse [X] kirjaliku loata, teavitab asutus [Y] asutust [X] oma kavatsusest andmeid jagada. [X] võib seejärel otsustada, kas peatada isikuandmete edastamine.

[Y] võib isikuandmeid jagada kolmanda isikuga ilma eelneva kirjaliku loata ja asjakohaste kinnitusteta erandjuhtudel, kui see on vajalik asutuse [Y] suhtes kohaldatavate juriidiliste kohustuste täitmiseks või kohtumenetluse raames, avalikust huvist tulenevatel kaalukatel põhjustel, mida on tunnustatud [asutuse Y kolmandas riigis] ja [asutuse X liikmesriigis] või Euroopa Liidus, või kui jagamine on vajalik õigusnõuete koostamiseks, esitamiseks või kaitsmiseks. Sellistel juhtudel teavitab [Y] korrapäraselt asutust [X] jagatud isikuandmete laadist ja nende jagamise põhjusest, kui [Y] on jaganud käesoleva dokumendi kohaldamisalasse kuuluvaid isikuandmeid [kolmandate isikutega], kui sellise teabe andmine ei ohusta käimasolevat uurimist. Selline käimasoleva uurimise teabega seotud piirang kehtib ainult seni, kuni püsib piirangu põhjus.

Vastastikkuse põhimõtte alusel võib [Y] nõuda, et [X] kohaldaks käesoleva dokumendi raames [Y]-lt saadud andmete edasise jagamise suhtes samu eeskirju ja kaitsemeetmeid.

8. Isikuandmete edasisaatmine: [Y] edastab [X]-lt saadud isikuandmeid kolmandate riikide pädevatele asutustele üksnes samadel eesmärkidel, milleks andmed talle edastati.

Juhul kui [Y] kavatses edastada mis tahes isikuandmeid kolmandas riigis asuvale kolmandale isikule, taotleb [Y] [X]-lt eelnevalt kirjalikku luba ja edastab sellised isikuandmed üksnes juhul, kui isikuandmete kaitse taset ei kahjustata, näiteks kui kolmas isik kohustub järgima samu andmekaitse põhimõtteid ja kaitsemeetmeid, mis on sätestatud käesolevas lepingus, või kui on tehtud asjakohane kaitse piisavuse otsus²². Sellise eelneva kirjaliku loa taotlemisel peaks [Y] märkima isikuandmete liigi, mida ta kavatses edastada, ning põhjused ja eesmärgid, miks [Y] kavatses isikuandmeid edastada. Kui [X] ei anna selliseks edastamiseks kirjalikku luba mõistliku aja jooksul, mis ei ületa kümnet päeva, konsulteerib [Y] [X]-ga ja kaalub võimalikke vastuväiteid. Vastastikkuse põhimõtte alusel võib [Y]

¹⁷ Vt ka II lisa.

¹⁸ Halduskokkuleppes.

¹⁹ Rahvusvahelises lepingus.

²⁰ Halduskokkuleppes.

²¹ Rahvusvahelises lepingus.

²² „Asjaomane kaitse piisavuse otsus“ – ELi piisavuse otsus, millega tunnistatakse, et edastatavate andmete suhtes kohaldatakse kaitsetaset, mis on sisuliselt samaväärne ELis pakutava tasemega, kui neid andmeid töötlevad kolmandas riigis asuvad vastuvõtjad.

kohaldada sama menetlust asutuse [X] suhtes asutuse [X] poolt käesoleva dokumendi raames [Y]-lt saadud andmete edasisel edastamisel.

9. Tõhus õiguskaitse: [Y] esitab [X]-le teabe oma kohaldatava õiguse kohta, millega nähakse ette andmesubjektide õiguskaitse, ning vastastikkuse põhimõtte alusel annab [X] [Y]-le teavet oma kohaldatava õiguse kohta, millega nähakse ette andmesubjektide õiguskaitse. See teave esitatakse käesoleva dokumendi lisas. Andmesubjekt võib esitada mis tahes vaide või nõude seoses tema isikuandmete töötlemisega käesoleva dokumendi alusel vastavalt vajadusele kas [X]-le, [Y]-le või mõlemale. Iga pädev asutus teavitab teist pädevat asutust igast sellisest vaidlusest või nõudest ning teeb kõik endast oleneva, et vaidlus või nõue õigeaegselt rahumeelselt lahendada²³.

[Iga kaebust menetleb [X] kooskõlas isikuandmete kaitse üldmääruse ja siseriikliku õigusega. [Y] ja [X] võivad esitada üksteisele kaebuste käsitlemise mehhanismi ja selle suhtes kohaldatava menetluse üksikasjaliku kirjelduse.

Näide:

kõik mured või kaebused, mis on seotud isikuandmete töötlemisega asutuse [Y] poolt, võib edastada otse [asutuse Y siseorganile / täitmise eest vastutavale talitusele / kaebuste esitamise talitusele], eelkõige [kaebuste esitamiseks mõeldud kanali] kaudu, kui teavet võib esitada veebivormi kaudu veebisaidil, elektronposti, kirja või telefoni teel, või [X]-le, saates selle teabe kaebuste käsitlemise osakonnale ja andmekaitseametnikule. [Y] teavitab asutust [X] teadetest, mille ta on saanud andmesubjektidelt selliste isikuandmete töötlemise kohta, mille [Y] on saanud [X]-lt, ning konsulteerib [X]-ga küsimusele vastamise üle. Vastastikkuse põhimõtte alusel teavitab [X] asutust [Y] kaebustest, mille ta on saanud andmesubjektidelt selliste isikuandmete töötlemise kohta, mille [X] sai [Y]-lt, ning konsulteerib [Y]-ga küsimusele vastamise üle. [X] and [Y] vastavad andmesubjektide taotlustele mõistlikul ja õigeaegsel viisil.]²⁴

Andmesubjektil on õigus saada [käesoleva dokumendi]²⁵ / [isikuandmete kaitse üldmääruse ja asutuse [X] siseriikliku õiguse ja asutuse [Y] vastu esitatud taotluste puhul [kohaldatavate siseriiklike õigusaktide] alusel]²⁶ õiguskaitset (sealhulgas saada juurdepääs isikuandmetele, neid parandada või need kustutada ning saada hüvitist kahju eest), kui ei järgita käesolevas dokumendis sätestatud kaitsemeetmeid. Olukorras, kus [X] on seisukohal, et [Y] ei ole tegutsenud kooskõlas käesolevas dokumendis sätestatud kaitsemeetmetega, võib [X] peatada isikuandmete edastamise käesoleva dokumendi alusel, kuni küsimus on rahuldavalt lahendatud, ja teavitada sellest andmesubjekti. Enne edastamise peatamist arutab [X] küsimust [Y]-ga ja [Y] vastab põhjendamatult viivitusega. Vastastikkuse põhimõtte alusel võib [Y] peatada isikuandmete edastamise käesoleva dokumendi alusel samadel põhjustel ja samal viisil.

²³ Rahvusvahelises lepingus: rahvusvaheline leping võib täiendada asutuse [Y] suhtes kohaldatavaid seadusi ja/või eeskirju, kui need asutuse [Y] õigusraamistikus puuduvad või on ebapiisavad, et tagada kaitsemeetmete asjakohane tase.

²⁴ See tuleb esitada halduskokkuleppe raames. Rahvusvahelise lepingu raames nähakse ette täpsemad eeskirjad, millega tagatakse, et lepingu rikkumise kohta esitatud kaebusi menetlevad pädevad asutused, ja menetlemise viis.

²⁵ Rahvusvahelise lepingu puhul.

²⁶ Halduskokkuleppe puhul.

10. Järelevalve: [X] ja [Y] vaatavad korrapäraselt läbi oma põhimõtted ja menetlused, millega rakendatakse dokumendis kirjeldatud kaitsemeetmeid isikuandmete suhtes. Teise pädeva asutuse põhjendatud taotluse korral vaatab pädev asutus läbi oma põhimõtted ja menetlused, et teha kindlaks ja kinnitada, et käesolevas dokumendis sätestatud kaitsemeetmeid rakendatakse tõhusalt, ning saadab läbivaatamise kokkuvõtte teisele pädevale asutusele²⁷.

IV – JÕUSTUMINE JA LÕPETAMINE

Käesolev õigusakt jõustub selle allkirjastamise kuupäeval [ja jääb jõusse üksnes selle aja vältel, kui ka täitmise tagamise koostööleping on jõus]²⁸. Lepingupooled võivad käesoleva dokumendi tingimuste suhtes konsulteerida ja neid muuta [samadel tingimustel, mis on sätestatud täitmise tagamise koostöölepingus]²⁹.

Kumbki lepingupool võib käesoleva dokumendi kehtivuse igal ajal lõpetada. Eelkõige tuleks käesoleva dokumendi kehtivus lõpetada niipea, kui üks pädevatest asutustest ei suuda enam tagada käesolevas õigusaktis sätestatud kaitsemeetmeid. Kõnealune pädev asutus peaks teavitama lõpetamisest ka teist pädevat asutust. Samuti tuleks käesoleva dokumendi kehtivus lõpetada niipea, kui üks pädevatest asutustest saab teada, et teine pädev asutus ei suuda enam tagada dokumendis sätestatud kaitsemeetmeid. Kõnealune pädev asutus peaks teavitama lõpetamisest ka teist pädevat asutust. Pärast käesoleva dokumendi kehtivuse lõpetamist säilitavad pädevad asutused [kooskõlas täitmise tagamise koostöölepinguga]³⁰ kogu [käesoleva dokumendi]³¹ [täitmise tagamise koostöölepingu]³² alusel esitatud teabe konfidentsiaalsuse ka edaspidi. Pärast käesoleva dokumendi kehtivuse lõpetamist jätkab [Y] käesoleva õigusakti alusel varem edastatud isikuandmete töötlemist vastavalt käesolevas õigusaktis sätestatud kaitsemeetmetele.

V- MUU

Käesolev dokument ja selle lisad koostatakse [...] ja [...], kusjuures mõlemad tekstid / kõik tekstid on võrdselt autentised.

*

* *

²⁷ Seoses pädeva asutuse sõltumatuse nõudega: kui see nõue on täidetud vastavalt Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu poolt esitatud kriteeriumidele, ei ole väline järelevalve nõutav. Kui kolmanda riigi pädeval asutusel puuduvad aga ELis nõutavad sõltumatuse tagatised, viidatakse vajadusele teha (välist) sõltumatut järelevalvet.

²⁸ Halduskokkuleppe puhul.

²⁹ Halduskokkuleppe puhul lisatakse see viide, kuid rahvusvahelises lepingus tuleks seda siin üksikasjalikult kirjeldada.

³⁰ Halduskokkuleppe puhul. Rahvusvahelise lepingu puhul esitatakse siin viide rahvusvahelisele lepingule endale.

³¹ Rahvusvahelise lepingu puhul.

³² Halduskokkuleppe puhul.

Vajaduse korral lisada eraldi klausel konfidentsiaalsuse ja ametisaladuse kohta, sõltuvalt vastuvõtva asutuse riigi õigusraamistiku analüüsist:

IIIa (lisatakse IV ette). Asutuse (Y) poolt vastu võetud teabe konfidentsiaalsus ja ametisaladus

1) (Y) käsitleb kogu käesoleva dokumendi alusel saadud teavet konfidentsiaalsena,

- (i) käsitades käesoleva kokkuleppe kohaselt saadud teavet või abitaotlusi konfidentsiaalsena, sealhulgas teavet selle kohta, et mõni teine asutus kaalub täitmise tagamise uurimist, on selle algatanud või osaleb selles, ning võttes vajaduse korral täiendavaid meetmeid, et täita saatva poole siseriiklikke õiguslikke nõudeid;
- (ii) tagades, et kui [Y] saab kolmandalt isikult (nt üksikisikult, kohtuasutuselt või muult õiguskaitseasutuselt) taotluse [X]-lt käesoleva kokkuleppe kohaselt saadud konfidentsiaalse teabe avaldamiseks, peaks [Y]:
 - a. säilitama mis tahes sellise teabe konfidentsiaalsuse;
 - b. teavitama sellest viivitamata teabe esitanud asutust [X];
 - c. saama [X]-lt nõusoleku kõnealuse teabe avaldamiseks;
 - d. teavitama asutust [X] sellest, kas teabe avaldamiseks kohustab mõni siseriiklik õigusakt;
- (iii) käesolevast kokkuleppes taganedes säilitama mis tahes sellise konfidentsiaalse teabe konfidentsiaalsuse, mis [X] on temaga käesoleva kokkuleppe kohaselt jaganud, selle tagastama ja kustutama;
- (iv) tagama, et võetakse kõik asjakohased tehnilised ja korralduslikud meetmed, et hoida talle käesoleva kokkuleppe alusel edastatud teave turvalisena. See hõlmab teabe tagastamist või käitlemist vastavalt asutuse [X] nõusolekule.

2) [X] võib nõuda, et käesoleva kokkuleppe alusel esitatud teavet kasutataks või avalikustataks ainult vastavalt asutuse [X] täpsustatud eritingimustele. Kui [Y] kavatses seda võimalust kasutada, teavitab ta sellest asutust [X] ja kui [X] nõustub nende tingimustega, peab ta neid järgima. Vastasel juhul võib [X] keelduda taotlusele vastamast.

3) Asutuse [Y] liikmel või liikmetel ja töötajatel on ametisaladuse hoidmise kohustus või konfidentsiaalsuskohustus nii ametiaja jooksul kui ka pärast seda seoses mis tahes konfidentsiaalse teabega, mis on neile teatavaks saanud nende ülesannete täitmisel või volituste kasutamisel. Nende ametiaja jooksul kehtib ametisaladuse hoidmise kohustus eelkõige juhul, kui füüsilised isikud teatavad oma riigi asjakohase kohaldatava õigusraamistiku rikkumisest.

*

* *

Dokumendi lisad

Lisa. Töötlemise kirjeldus, eesmärk, andmekategooriad, vastuvõtjad

Näiteks:

X: [Identifitseerimis- ja kontaktandmed]

1. Nimi: ...

Aadress: ...

Kontaktisiku nimi, ametikoht ja kontaktandmed: ...

Allkiri ja kuupäev: ...

Y: [Identifitseerimis- ja kontaktandmed]

1. Nimi: ...

Aadress: ...

Kontaktisiku nimi, ametikoht ja kontaktandmed: ...

Allkiri ja kuupäev: ...

Edastamise kirjeldus

Nende andmesubjektide kategooriad, kelle isikuandmeid töödeldakse

.....

Edastatavate isikuandmete liigid

.....

Edastatavad tundlikud andmed (vajaduse korral) ja kohaldatavad piirangud või kaitsemeetmed, milles võetakse täielikult arvesse andmete laadi ja kaasnevaid ohte, näiteks range eesmärgikohasus, juurdepääsupiirangud (sealhulgas juurdepääs üksnes eriväljaõppega töötajatele), andmete juurdepääsu registri pidamine, andmete edasisaatmise piirangud või täiendavad turvameetmed.

.....

Edastamise sagedus (nt kas andmeid edastatakse üks kord või pidevalt).

.....

Töötlemise laad

.....

Andmeedastuse eesmärk (eesmärgid) ja edasine töötlemine

.....

Isikuandmete säilitamise ajavahemik või kui see ei ole võimalik, siis sellise ajavahemiku määramise kriteeriumid

.....

I lisa. Kohaldatavate õigusaktide ning asjakohaste tehniliste ja korralduslike turvameetmete kirjeldus

Tehnilisi ja korralduslikke meetmeid tuleb kirjeldada konkreetselt (mitte üldjoontes). Samuti on vaja selgelt märkida, milliseid meetmeid kohaldatakse iga edastamise / edastamiste kogumi suhtes.

Asutuste X ja Y poolt rakendatavate selliste tehniliste ja korralduslike turvameetmete kirjeldus, millega tagatakse vajalik turvalisuse tase, võttes arvesse töötlemise laadi, ulatust, konteksti ja eesmärki ning ohtu füüsiliste isikute õigustele ja vabadustele.

[Võimalike meetmete näited:

isikuandmete pseudonüümimise ja krüpteerimise meetmed;

meetmed, millega tagatakse isikuandmeid töötlevate süsteemide ja teenuste kestev konfidentsiaalsus, terviklus, kättesaadavus ja vastupidavus;

meetmed, millega tagatakse võime taastada õigeaegselt isikuandmete kättesaadavus ja neile juurdepääs füüsilise või tehnilise vahejuhtumi korral;

isikuandmete töötlemise turvalisuse tagamise tehniliste ja korralduslike meetmete toimivuse korrapärase kontrollimise ja hindamise kord;

kasutaja tuvastamise ja autoriseerimise meetmed;

meetmed andmete kaitsmiseks edastamise ajal;

meetmed andmete kaitsmiseks säilitamise ajal;

meetmed isikuandmete töötlemise kohtade füüsilise julgeoleku tagamiseks;

meetmed sündmuste logimise tagamiseks;

meetmed süsteemi konfiguratsiooni, sealhulgas vaikekonfiguratsiooni tagamiseks;

sisemise IT ning IT-turbe valitsemise ja haldamise meetmed;

protsesside ja toodete sertifitseerimise/tagamise meetmed;

meetmed, millega tagatakse võimalikult väheste andmete kogumine;

andmete kvaliteedi tagamise meetmed;

andmete piiratud säilitamise tagamise meetmed;

vastutuse tagamise meetmed;

meetmed andmete porditavuse võimaldamiseks ja kustutamise tagamiseks.]

II lisa. Loetelu üksustest, kellega [Y]-l on lubatud konfidentsiaalset teavet jagada

III lisa. Õiguskaitset käsitleva kohaldatava õigusraamistiku kirjeldus