EUROOPA LIIDU JA RAHVUSVAHELISTE ÕIGUSAKTIDE ANALÜÜS IDENTITEEDIHALDUSE VALDKONNAS

03.12.2018

SORAINEN

SISUKORD

1. SISSEJUHATUS

Eesti siseturvalisuse arengukava[1] üks alaeesmärke on usaldusväärne ja turvaline identiteedihaldus. Riik võtab vastutuse isiku õiguspärase tuvastamise eest, andes välja isikut tõendava dokumendi ning luues võimalused isiku füüsiliseks ja digitaalseks identifitseerimiseks, erinevate avalike ja erateenuste kasutamiseks ning digitaalallkirja andmiseks.[2] Isiku tõsikindla identifitseerimise peamiseks meetodiks on tema biomeetriliste andmete töötlemine[3]. Riikide praktika biomeetriliste andmete töötlemisel erineb märgatavalt tulenevalt konkreetse riigi õigussüsteemist, poliitilistest prioriteetidest ning tehnoloogia arengust ja kättesaadavusest. Seejuures on ka biomeetriliste andmete töötlemise eesmärgid erinevad. Levinud on isiku näokujutise või foto ning sõrmejälgede töötlemine dokumendimenetluses (s.o. passi ja reisidokumentide väljastamiseks), sõrmejälgede ja DNA töötlemine kriminaalmenetluses, kuid järjest arenev tehnoloogia võimaldab töödelda ja tuvastada isikut ka silmaiirise ja hääle järgi. Erialases kirjanduses räägitakse ka ajuaktiivsuse ja südamerütmi põhisest tuvastamisest tulevikus[4].

Eestis on hetkel mitu erinevat andmekogu, kus töödeldakse erinevatel eesmärkidel erinevaid biomeetrilisi andmeid (nt isikut tõendavate dokumentide andmekogu, vangiregister, riiklik sõrmejälgede register, riiklik DNA-register jms). Seejuures on andmekogud erinevate ministeeriumite haldusalas, andmete kvaliteet ja formaat erinev ning süsteemide tarkvara arendatud erinevatel aegadel. Seetõttu on Siseministeerium esitanud ettepaneku luua üks tsentraalne biomeetrilisi andmeid koondav andmekogu (Automaatne biomeetriline identifitseerimissüsteem ehk ABIS), mis võimaldaks biomeetrilisi andmeid töödelda ja kasutada senisest efektiivsemalt ja koordineeritumalt.

Käesoleva analüüsi eesmärk on analüüsida Euroopa Liidu ja rahvusvahelist õigust seoses biomeetriliste andmete hõivamisega ning nende andmete kasutamist isiku tuvastamise ja isikusamasuse kontrollimiseks. Samuti on eesmärgiks välja selgitada, kas ja kuidas on Euroopa Liidu ja rahvusvaheliste õiguse õigusaktide alusel lubatud erinevate avalik-õiguslike menetluste käigus kogutud biomeetriliste andmete ristkasutamine suhetes riigiga ning rahvusvaheliste organisatsioonidega, kuid ka eraõiguslikes suhetes.

Vastavalt tellija esitatud läheülesandele esitab alljärgnev analüüs vastused eelkõige järgmistele tellija esitatud küsimustele:

1) Kas Euroopa Liidu ja rahvusvahelistest õigusest tulenevad piirangud erinevate menetluste raames hõivatud biomeetriliste andmete töötlemiseks ühes andmekogus?
2) Millised riistvaralised ja tarkvaralised andmekaitse ja turvanõuded on seatud biomeetriliste andmete töötlemisele?
3) Millised on Euroopa Liidu ja rahvusvahelisest õigusest tulenevad kohustused, mida siseriiklikus õiguses peab järgima biomeetriliste andmete töötlemisel?

---

[1] Siseturvalisuse arengukava 2015-2020, https://www.siseministeerium.ee/sites/default/files/dokumendid/Arengukavad/siseturvalisuse_arengukava_2015-2020_kodulehele.pdf (26.11.2018)

[2] *Ibid*, lk 102 (26.11.2018)

[3] Tellija lähteülesanne

[4] Fletcher, Bevin. Brainprints: The Biometric of the Future? Laboratory Equipment, September 2016, vol 53, issue 4, lk 20-21

4) Millistes avalik-õiguslikes menetlustes, millisel õiguslikul alusel ja millistel tingimustel ning mahus on riik kohustatud töötlema isiku biomeetrilisi andmeid?
5) Millistes avalik-õiguslikes menetlustes, millisel õiguslikul alusel ja millistel tingimustel ning mahus on riigil lubatud töödelda isiku biomeetrilisi andmeid?
6) Millised on Euroopa Liidu ja rahvusvahelisest õigusest tulenevad kohustused, mida siseriiklikus õiguses peab järgima biomeetriliste andmete ristkasutamises?
7) Kas ja kui, siis millistel tingimustel on lubatud erinevate avalik-õiguslike menetluste käigus kogutud isiku biomeetriliste andmete ristkasutamine teistes avalik-õiguslikes menetlustes isiku tuvastamiseks või isikusamasuse kontrollimiseks?
8) Kas ja kui, siis millistel tingimustel on lubatud erinevate avalik-õiguslike menetluste käigus kogutud isiku biomeetriliste andmete edastamine eraõiguslikele isikutele isiku tuvastamiseks või isikusamasuse kontrollimiseks?
9) Kas ja kui, siis millistel tingimustel on lubatud erinevate avalik-õiguslike menetluste käigus kogutud isiku biomeetriliste andmete edastamine teistele riikidele ja rahvusvahelistele organisatsioonidele isiku tuvastamiseks või isikusamasuse kontrollimiseks?
10) Kas eraõiguslikel juriidilistel isikutel on eraõiguslikes suhetes õigus koguda, säilitada ja kolmandatele isikutele edasi anda isiku biomeetrilisi andmeid ja kui, siis millises ulatuses ja millistel tingimustel?

Arvestades lähteülesannet on käesolevas analüüsis biomeetrilistest andmetest keskendutud eelkõige isiku sõrmejälgi käsitlevale regulatsioonile (kui see on eristatud), aga ka näokujutisele/fotole. Õiguslikult hõlmavad biomeetriliste andmete definitsioonid erinevates õigusaktides üldjuhul alati sõrmejälgi. Seega kui kasutatakse mõistet „biomeetrilised andmed“ on selle all kindlasti mõeldud sõrmejälgi, kuid vastavalt konkreetse õigusakti definitsioonile võib see hõlmata ka teisi biomeetrilisi andmeid. Arvestades käesoleva analüüsi eset ja mahtu, on analüüsist välja jäetud muude biomeetriliste andmete töötlemist puudutav õiguslik analüüs (nt silmaiiris, DNA jms), välja arvatud, kui neid on selgesõnaliselt mainitud. DNA andmete puhul on tegemist geneetiliste andmetega, millega kaasneb oluliselt suurem risk andmesubjektile (sisaldavad oluliselt rohkem informatsiooni, kui see, mis on vajalik isiku unikaalseks identifitseerimiseks), DNA andmete hõivamiseks on vaja geneetilist materjali, mistõttu on nende andmete töötlemine ja kasutamine juba oluliselt spetsiifilisem ning väljub käesoleva analüüsi ulatusest.

Käesolev analüüs põhineb õigusaktidel ja muudel materjalidel sellises sõnastuses, mis on kehtivad analüüsi koostamise ajahetkel. Lisaks on viidatud ka tellija märgitud algatustele. Mõnel juhul puuduvad õigusaktidel ja materjalidel ametlikud eestikeelsed tõlked ning seetõttu oleme lähtunud internetis avaldatud mitteametlikest tõlgetest või tõlkinud need ise vastavalt vajadusele. Me ei vastuta selliste tõlgete vastavuse eest ametlikule tõlkele, mida võidakse avaldada tulevikus.

Analüüsi raamest jääb välja Eesti õiguse põhjalik analüüs, eetikaga seotud küsimused, riskianalüüs, samuti majanduslikku mõju puudutavad küsimused ning tehnoloogiliste infrastruktuuride korraldusega seotud küsimused.

Analüüs on jagatud seitsmeks suuremaks sisuliseks alateemaks (peatükid 3-9), mis on omakorda valdavalt jagatud kaheks: rahvusvahelist õigust analüüsiv osa ning Euroopa Liidu õigust analüüsiv osa. Erandiks on peatükk 6, mis on jagatud alateemadeks vastavalt

konkreetsetele avalik-õiguslikele menetlustele. Kuna vastavad menetlused põhinevad Euroopa Liidu õigusel, ei ole meie hinnangul vajalik antud kontekstis täiendavalt käsitleda rahvusvahelist õigust (vt täpsemalt peatükk 6).

Iga alateema alguses on välja toodud vastavat teemad reguleerivad olulisimad õigusaktid ja sätted või muu informatsioon mis selle kontekstis relevantne on. Samuti oleme välja toonud peamised järeldused vastava alateema kohta. Analüüsi algusesse (peatükk 2) on koondatud analüüsi terviklik kokkuvõte ja lõppjäreldused.

Õigusanalüüsi koostas Advokaadibüroo SORAINEN AS.

Mihkel Miidla Vandeadvokaat	Kaupo Lepasepp Vandeadvokaat	Cathriin Torop Vandeadvokaat

2. ANALÜÜSI KOKKUVÕTE JA JÄRELDUSED

Kas Euroopa Liidu ja rahvusvahelistest õigusest tulenevad piirangud erinevate menetluste raames hõivatud biomeetriliste andmete töötlemiseks ühes andmekogus?	Jah. Andmete töötlemisel ühes andmekogus tuleb järgida üldisi rahvusvahelise õiguse ja Euroopa Liidu õiguse printsiipe isikuandmete töötlemisele, ennekõike eesmärgi piirang, seaduslikkus, andmete minimaalsus, töötlemise läbipaistvus, säilitamise piirang ja kaitsemeetmete rakendamine. Need printsiibid piiravad biomeetriliste andmete töötlemist ühes andmekogus. On võimalik tugineda eranditele, kuid nende rakendamine eeldab riigi poolt kaalumist ja vastava kaalumise tulemusena tingimustele vastava õigusliku aluse kehtestamist. Eelnevalt väljatoodud piirangutele võib vastata lahendus, kus ühes andmekogus hoitavate andmete osas on piiratud nende töötlemine ja kasutamine (nt läbi piiratud volituste ja ligipääsude haldamise).
Millised riistvaralised ja tarkvaralised andmekaitse ja turvanõuded on seatud biomeetriliste andmete töötlemisele?	Andmekaitse ja turvanõuded biomeetriliste andmete töötlemisele on rahvusvahelises õiguses määratud üksnes printsiipide tasemel ning Euroopa Liidu õiguses üksnes üldiste meetmete tasemel. Konkreetsed kohustuslikke standardeid riistvarale ja tarkvarale õigusaktide tasandil kehtestatud ei ole. Mõlemad õigussüsteemid arvestavad seejuures tehnoloogia neutraalsuse põhimõtet, mis võimaldab paindlikkust arvestades erineva tehnoloogiataseme ja -traditsioonidega riike. Rakendatavate turvameetmete valikul peab vastutav töötleja rakendama riskipõhist lähenemist, hinnates töötlemisega kaasnevaid võimalikke ohte. Neid ohte tuleb hinnata andmesubjekti vaatenurgast.
Millised on Euroopa Liidu ja rahvusvahelisest õigusest tulenevad kohustused, mida siseriiklikus õiguses peab järgima biomeetriliste andmete töötlemisel?	Rahvusvahelises õiguses on isikuandmete kaitse nõuded sõnastatud printsiipide tasandil ning osalisriikidele on jäetud võrdlemisi suur kaalutlusruum konkreetsete reeglite kehtestamiseks siseriiklikus õiguses. Lisaks tuleb silmas pidada ka mittesiduva õiguse instrumente, eriti selliseid, millega Eesti on ühinenud. Nendes on sõnastatud poliitilised suuniseid, mida tuleks arvesse võtta siseriikliku õigusliku regulatsiooni kehtestamisel.

	Biomeetriliste andmete töötlemiseks peab olema õiguslik alus. Üldjuhul on biomeetriliste andmete töötlemine keelatud, v.a. kui kohaldub erand. Biomeetriliste andmete töötlemise õiguslik alus ABIS-süsteemi kontekstis võiks olla isikuandmete kaitse üldmääruse art 9(2)(g). Olulise avaliku huviga seotud põhjusel biomeetriliste isikuandmete töötlemisele peab vastav õiguslik alus olema EL-i või liikmesriigi õiguses (eriseaduses) sätestatud. Enne erialuse kehtestamist siseriiklikus (või EL-i) õiguses tuleb seadusandjal läbi viia vastav kaalumine, s.t. hinnata, kas soovitud isikuandmete töötlemine (selleks loodav õiguslik alus) on: a. proportsionaalne taotletava eesmärgiga; b. austab isikuandmete kaitse õiguse olemust; ja c. tagab sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks.
Millistes avalik-õiguslikes menetlustes, millisel õiguslikul alusel ja millistel tingimustel ning mahus on riik kohustatud töötlema isiku biomeetrilisi andmeid?	Enamasti on riigil kohustus töödelda biomeetrilisi andmeid menetlustes, mis on EL-i pädevuses (ning mis on seotud eelkõige migratsiooniga). Olemuselt on sellised käesolevas analüüsis välja toodud menetlused valdavalt haldusmenetlused ning nende haldusmenetluste raames on riigil vastavalt menetlusele kas kohustus või õigus biomeetrilisi andmeid töödelda. Teatud juhtudel võib riik biomeetrilisi andmeid töödelda ja teatud juhul peab riik ka omalt poolt andmed kättesaadavaks tegema süütegudega seotud menetlustes. Riik on kohustatud töötlema biomeetrilisi andmeid järgmistes avalik-õiguslikes menetlustes alljärgnevas mahus: 1. **Dokumendimenetlus** (st haldusmenetluses dokumentide väljastamisel: näokujutis + 2 sõrmejälge otsevajutusega) Õiguslik alus: - Euroopa Parlamendi ja Nõukogu määrus (EÜ) nr 444/2009, 28. mai 2009, millega muudetakse nõukogu määrust (EÜ) nr 2252/2004 liikmesriikide väljastatud passide

	ja reisidokumentide turvaelementide ja biomeetria standardite kohta - Nõukogu määrus (EÜ) nr 380/2008, 18. aprill 2008, millega muudetakse määrust (EÜ) nr 1030/2002, millega kehtestatakse ühtne elamisloavorm kolmandate riikide kodanike jaoks 2. **Viisamenetlus** (st haldusmenetluses viisataotluste menetlemisel ja väljastamisel: foto + 10 sõrmejälge otsevajutusega) Õiguslik alus: - Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 810/2009, 13. juuli 2009, millega kehtestatakse ühenduse viisaeeskiri (viisaeeskiri) - Euroopa Parlamendi ja Nõukogu määrus (EÜ) nr 767/2008, 9. juuli 2008, mis käsitleb viisainfosüsteemi (VIS) ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta (VIS-määrus) - Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 390/2009, 23. aprill 2009, millega muudetakse viisasid käsitlevaid ühiseid konsulaarjuhiseid diplomaatilistele ja konsulaaresindustele seoses biomeetria kasutuselevõtmisega ning viisataotluste vastuvõtmise ja menetlemise korraldamise sätete lisamisega 3. **Piiriületusega seotud menetlused** (st haldusmenetluses piirikontrolli raames: näokujutis / foto + sõrmejäljed mahus sõltuvalt andmebaasist, kuhu andmed edastatakse) Õiguslik alus: - Euroopa Parlamendi ja nõukogu määrus (EL) 2016/399, 9. märts 2016, mis käsitleb isikute üle piiri liikumist reguleerivaid liidu eeskirju (Schengeni piirieeskirjad) - Euroopa Parlamendi ja nõukogu määrus (EL) 2017/2226, 30. november 2017, millega luuakse riiki sisenemise ja riigist lahkumise süsteem liikmesriikide välispiire ületavate kolmandate riikide kodanike riiki sisenemise ja riigist lahkumise andmete ja sisenemiskeeluandmete registreerimiseks ning määratakse kindlaks riiki sisenemise ja

	riigist lahkumise süsteemile õiguskaitse eesmärgil juurdepääsu andmise tingimused ning millega muudetakse Schengeni lepingu rakendamise konventsiooni ning määruseid (EÜ) nr 767/2008 ja (EL) nr 1077/2011 (EES määrus) - Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1987/2006, 20. detsember 2006, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist (SIS II määrus) 4. **Varjupaiga ja rahvusvahelise kaitse menetlus** (st haldusmenetluses taotluste menetlemisel: 10 sõrmejälge) Õiguslik alus: - Euroopa Parlamendi ja nõukogu määrus (EL) nr 603/2013, 26. juuni 2013 , millega luuakse sõrmejälgede võrdlemise Eurodac-süsteem määruse (EL) nr 604/2013 (millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku või kodakondsuseta isiku esitatud rahvusvahelise kaitse taotluse läbivaatamise eest) tõhusaks kohaldamiseks ning mis käsitleb liikmesriikide õiguskaitseasutuste ja Europoli taotlusi sõrmejälgede andmete võrdlemiseks Eurodac-süsteemi andmetega õiguskaitse eesmärgil ning millega muudetakse määrust (EL) nr 1077/2011, millega asutatakse Euroopa amet vabadusel, turvalisusel ja õigusel rajaneva ala suuremahuliste IT-süsteemide operatiivjuhtimiseks (Eurodac määrus) - Euroopa Parlamendi ja nõukogu määrus (EL) nr 604/2013, 26. juuni 2013 , millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku või kodakondsuseta isiku esitatud rahvusvahelise kaitse taotluse läbivaatamise eest 5. **Illegaalimenetlus** (st haldusmenetluses Schengeni välispiiri ületamisel kinni peetud või liikmesriigi territooriumil tabatud kolmandate riikide kodanikud või kodakondsuseta isikud: 10 sõrmejälge või

	vähemalt nimetissõrmed, nende puudumisel kõik muud sõrmejäljed) Õiguslik alus: - Eurodac määrus - VIS määrus - SIS II määrus - EES määrus - Euroopa Parlamendi ja nõukogu määrus (EL) 2018/1240, 12. september 2018, millega luuakse Euroopa reisiinfo ja -lubade süsteem (ETIAS) ning muudetakse määrusi (EL) nr 1077/2011, (EL) nr 515/2014, (EL) 2016/399, (EL) 2016/1624 ja (EL) 2017/2226 (ETIAS määrus) (ei töödelda biomeetrilisi andmeid) 6. **Süütegudega seotud menetlused** Õiguslik alus: - Prümi leping ja seda EL-i õigusesse rakendav otsus 2008/615/JSK (kohustus teha kättesaadavaks sõrmejäljed, viiteandmed) Töötlemise täpsemad tingimused on toodud ptk-s 6 ja Lisas 1.
Millistes avalik-õiguslikes menetlustes, millisel õiguslikul alusel ja millistel tingimustel ning mahus on riigil lubatud töödelda isiku biomeetrilisi andmeid?	Süütegudega seotud menetlused, kui riigile on antud ligipääs EL-i infosüsteemile andmete pärimiseks süütegude uurimise, avastamise jms eesmärgil. Näiteks on VIS süsteemist sel eesmärgil biomeetriliste andmete töötlemise õiguslik alus: - Nõukogu otsus 2008/633/JSK, 23. juuni 2008, mis käsitleb liikmesriikide määratud ametiasutuste ja Europoli juurdepääsu viisainfosüsteemile (VIS) terroriaktide ja muude raskete kuritegude vältimise, avastamise ja uurimise eesmärkidel: VIS-ist saadud isikuandmed Vt Lisas 1 töötlemise õiguslikku alust, tingimusi ja andmete mahuga seonduvat.
Millised on Euroopa Liidu ja rahvusvahelisest õigusest tulenevad kohustused, mida siseriiklikus õiguses peab järgima biomeetriliste andmete ristkasutamises?	Andmete edasise kasutamise olulisim kohustus on eesmärgipärasuse põhimõtte järgimine, s.t. andmeid tohib töödelda selle algselt sõnastatud eesmärgil või, kui töötlemine ei vasta sellele eesmärgile, peab edasiseks töötlemiseks olema iseseisev õiguslik alus. Kui andmed kasutatakse seaduses sätestatud erandi alusel (avalikes

	huvides teaduse, ajaloo või statistika eesmärkidel võib töödelda ilma täiendavat õiguslikku alust kehtestamata), tuleb rakendada asjakohaseid kaitsemeetmeid (nt anonüümiseerimine). Pädevate asutuste poolt süütegude tõkestamiseks, uurimiseks, avastamiseks, nende eest vastutusele võtmiseks või kriminaalkaristuste täitmisele pööramiseks kogutud andmeid ei või üldjuhul edasi töödelda. Erandiks on olukord, kus EL-i või liikmesriigi õigus lubab edasist töötlemist.
Kas ja kui, siis millistel tingimustel on lubatud erinevate avalik-õiguslike menetluste käigus kogutud isiku biomeetriliste andmete ristkasutamine teistes avalik-õiguslikes menetlustes isiku tuvastamiseks või isikusamasuse kontrollimiseks?	Biomeetriliste andmete töötlemine isiku tuvastamiseks ja isikusamasuse tuvastamiseks avalik-õiguslike menetluste raames on EL-i õiguse tasandil reguleeritud selliste menetluste raames, mis on EL-i pädevuses (nt illegaalimenetlus, piiriületuse menetlus, viisamenetlus). EL-i andmebaasidest saadud andmeid võib reeglina töödelda üksnes sellel eesmärgil, milleks päring tehti, edasine töötlemine on üldjuhul keelatud või piiratud konkreetse üksikjuhtumi vajadusega. Kolmandatele isikutele nende menetluste käigus saadud andmete avaldamine on reeglina keelatud. Erandiks võib olla erakorraline terroriaktide või raskete kuritegudega seotud olukord (vt Lisa 1 konkreetsete menetluste osas). Siseriiklike avalik-õiguslike menetluste raames kogutud isikuandmete ristkasutamist siseriiklikult reguleeritud menetluste raames EL-i õigus spetsiifiliselt ei reguleeri.
Kas ja kui, siis millistel tingimustel on lubatud erinevate avalik-õiguslike menetluste käigus kogutud isiku biomeetriliste andmete edastamine eraõiguslikele isikutele isiku tuvastamiseks või isikusamasuse kontrollimiseks?	EL-i õigus ei loo õiguslikku alust avalik-õiguslikes menetlustes hõivatud isikuandmete edastamisele eraõiguslikele isikutele isiku tuvastamise või isikusamasuse kontrollimise eesmärgil. Siseriiklikult reguleeritud avalik-õiguslikes menetlustes hõivatud biomeetriliste andmete edastamisele on riigil võimalik vastavalt isikuandmete kaitse üldmäärusele luua vastav õiguslik alus, kui see vastab artikli 9 ja artikli 6(4) tingimustele, sh tuleb läbi viia vastav kaalumine, ning mis vastab artiklis 23 toodud eesmärkidele. EL-i pädevusse kuuluvate avalik-õiguslike menetluste käigus kogutud biomeetriliste andmete edastamine kolmandatele isikutele võib olla keelatud või piiratud teatud eeldustega (vt Lisa 1).

Kas ja kui, siis millistel tingimustel on lubatud erinevate avalik-õiguslike menetluste käigus kogutud isiku biomeetriliste andmete edastamine teistele riikidele ja rahvusvahelistele organisatsioonidele isiku tuvastamiseks või isikusamasuse kontrollimiseks?	Avalik-õiguslikes menetlustes hõivatud biomeetriliste andmete edastamine teistele riikidele või rahvusvahelistele organisatsioonidele isiku tuvastamiseks või isikusamasuse kontrollimiseks ei ole keelatud, kui täidetud on biomeetriliste andmete töötlemise üldnõuded ning andmete edastamise eeldused, sh täiendavate kaitsemeetmete rakendamine. EL-i pädevusse kuuluvate avalik-õiguslike menetluste käigus kogutud biomeetriliste andmete edastamine kolmandatele isikutele võib olla keelatud või piiratud teatud eeldustega. Siseriiklikult reguleeritud avalik-õiguslikes menetlustes hõivatud biomeetriliste andmete edastamisele on riigil võimalik kui vastavalt isikuandmete kaitse üldmäärusele luua vastav õiguslik alus, mis vastab artikli 9 ja artikli 6(4) tingimustele, sh tuleb läbi viia vastav kaalumine, ning vastab artiklis 23 toodud eesmärkidele.
Kas eraõiguslikel juriidilistel isikutel on eraõiguslikes suhetes õigus koguda, säilitada ja kolmandatele isikutele edasi anda isiku biomeetrilisi andmeid ja kui, siis millises ulatuses ja millistel tingimustel?	Euroopa Liidu õigus ei loo õiguslikku alust avalik-õiguslikes menetlustes hõivatud isikuandmete edastamisele eraõiguslikele isikutele eraõiguslikus suhtes kasutamise eesmärgi. Eraõiguslikus suhtes biomeetriliste andmete töötlemine võib aset leida andmesubjekti nõusolekul või muu õigusliku aluse olemasolul.

3. ÜLDISED NÕUDED BIOMEETRILISTE ANDMETE TÖÖTLEMISEKS

Käesolev peatükk keskendub biomeetriliste andmete töötlemise üldistele nõuetele: s.t. siin on analüüsitud nõudeid, mis on universaalsed biomeetriliste andmete mis tahes töötlemisele sõltumata konkreetsest menetluse liigist või andmetöötluse tegevusest. Sellised nõuded loovad raami järgnevatele peatükkidele, sest iga konkreetsema andmetöötluse tegevuse puhul tuleb arvestada alljärgnevalt toodud üldist õiguslikku raamistikku ja konteksti.

Sisuliselt keskendume nii õigusaktidele kui ka mittesiduvatele õigusaktidele ning juhistele ja suunistele, mis aitavad regulatsiooni tõlgendada ning täpsustada seadusandja tahet.

3.1. Rahvusvaheline õigus

Õigusakt	Säte	Sõnastus
Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt (ICCPR)	Artikkel 17	1. Kellegi isiklikku või perekonnaellu ei tohi meelevaldselt või ebaseaduslikult vahele segada, kellegi kodu puutumatusele, kirjavahetuse saladusele, aule ja reputatsioonile ei tohi meelevaldselt või ebaseaduslikult kallale kippuda. 2. Igal inimesel on õigus seaduse kaitsele selliste vahelesegamiste ja kallalekippumiste eest.
Euroopa inimõiguste ja põhivabaduste kaitse konventsioon **(EIÕK)**	Artikkel 8	1. Igaühel on õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning sõnumite saladust. 2. Ametivõimud ei sekku selle õiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks.
Isikuandmete töötlemisel isiku kaitse moderniseeritud konventsioon 108[5] **(Konventsioon 108+)**	Artikkel 5	1. Andmete töötlemine peab olema taotletava õiguspärase eesmärgiga proportsionaalne ning töötlemise igal sammul peegeldama õiglast tasakaalu kõigi huvide vahel, sõltumata sellest, kas need on avalikud või erasfääris, ning kaalul olevate õiguste ja vabaduste vahel. 2. Iga osapool tagab, et andmete töötlemine saab põhineda andmesubjekti vabal, konkreetsel, informeeritud ning ühemõttelisel nõusolekul või mõnel muul seaduses sätestatud õiguslikul alusel. 3. Isikuandmed tuleb töödelda seaduslikult.

[5] Konventsiooni tõlge eesti keelde on läbivalt käesolevas analüüsis mitteametlik.

		4. Töödeldavad isikuandmed peavad olema: a. töödeldud ausal ja läbipaistval viisil; b. kogutud selgesõnalisel, konkreetsel ja õigustatud eesmärgil ning mitte olla töödeldud nende eesmärkidega mittesobival eesmärgil; edasine töötlemine arhiveerimise eesmärgil avalikes huvides, teadusliku või ajaloolise uurimuse eesmärgil või statistilisel eesmärgil peab olema teostatud asjakohaste kaitsemeetmete abil, mis vastavad nendele eesmärkidele; c. olema piisavad, asjakohased ja mitte ülemäärased vastavalt nende eesmärkidele, milleks neid töödeldakse; d. olema täpsed ja, kus vajalik, ajakohased; e. säilitatud vormis, mis lubab andmesubjekti teha kindlaks mitte kauemaks, kui perioodiks, mis on vajalik andmete töötlemise eesmärkide saavutamiseks.
	Artikkel 6	1. Järgmiste andmete töötlemine: - geneetilised andmed; - isikuandmed, mis seonduvad süütegude, kriminaalmenetluse ja süüdimõistmisega ning seotud turvalisuse meetmetega; - biomeetrilised andmed, mis unikaalselt tuvastavad isiku; - isikuandmed seoses teabega, mida nad avaldavad rassilise või etnilise kuuluvuse osas, poliitiliste vaadete, ametiühingu liikmeks olemise, usuliste või muude vaadete, tervise või seksuaalelu kohta, on lubatud ainult siis kui asjakohased kaitsemeetmed on seaduses sätestatud, mis täiendavad Konventsioonis toodud kaitsemeetmeid. 2. Sellised kaitsemeetmed kaitsevad riskide vastu, mida delikaatsete andmete töötlemine võib tekitada andmesubjektide huvidele, õigustele ja põhivabadustele, eelkõige diskrimineerimise vastu.
Mittesiduva õiguse instrumendid		
Dokument	**Sisu**	

ÜRO Inimõiguste Ülddeklaratsioon (UDHR)	Artikkel 12	Kellegi era- ja perekonnaellu, kodupuutumatusse või kirjavahetusse ei tohi meelevaldselt sekkuda ega teotada kellegi au ja head nime. Igaühel on õigus saada seaduselt kaitset sellise sekkumise või teotamise korral.
ÜRO Peaassamblee ja ÜRO Inimõiguse Komitee resolutsioonid seoses privaatsusega digiajastul (A/C.3/71/L.39/Rev.1, A/HRC/34/L.7/Rev.1)	Kutsutakse riike üles üle vaatama oma menetlusi, praktikat ja õigusakte sidekanalite jälgimise, nende pealtkuulamisel ja isikuandmete kogumisel, sh massjälgimisel, pealtkuulamisel ja kogumisel, eesmärgiga austada õigust privaatsusele tagades täielik ja efektiivne kõigi rahvusvaheliste inimõiguste õigusaktidest tulenevate kohustuste rakendamine.	

Kokkuvõte

- Rahvusvahelises õiguses on õigus isikuandmete kaitsele osa õigusest eraelu kaitsele ega ole selgelt eristatud. Erandiks on Konventsioon 108+, mis on sisult sarnane isikuandmete kaitse üldmäärusega ning kasutab ka mõistet „biomeetrilised andmed“, kuid ei täpsusta biomeetriliste andmete kataloogi.
- Rahvusvahelises õiguses on isikuandmete kaitse nõuded sõnastatud printsiipide tasandil ning osalisriikidele on jäetud võrdlemisi suur kaalutlusruum konkreetsete reeglite kehtestamiseks siseriiklikus õiguses.
- Lisaks siduvatele õigusaktidele tuleb silmas pidada ka mittesiduva õiguse instrumente, eriti selliseid, millega Eesti on ühinenud. Nendes on sõnastatud poliitilised suuniseid, mida tuleks arvesse võtta siseriikliku õigusliku regulatsiooni kehtestamisel.

3.1.1. Õigusaktid

Rahvusvaheline õigus ei reguleeri üldjuhul spetsiifiliselt biomeetriliste andmete töötlemist. Rahvusvahelise õiguse õigusaktid räägivad üldiselt isiku õigusest eraelu kaitsele, millest on tuletatav õigus privaatsusele ja isikuandmete kaitsele. Kuna biomeetrilised andmed ei ole selles kontekstis eraldatavad ning on osa isikuandmetest, peab eraelu kaitsega seotud printsiipe igal juhul arvesse võtma ka biomeetriliste andmete töötlemisel.

(a) ICCPR

ICCPR keelab meelevaldse või ebaseadusliku sekkumise isiku perekonnaellu, kodu puutumatusele, kirjavahetuse saladusele, aule ja reputatsioonile. See tähendab, et sekkumine peab põhinema seadusel (ei tohi olla *ebaseaduslik*), kuid ka seadusel põhinev sekkumine ei tohi olla *meelevaldne*, s.t. see peab vastama ICCPR-i tingimustele ja eesmärkidele ning peaks igal juhul konkreetseid asjaolusid arvestades olema mõistlik[6] ja proportsionaalne.

(b) EIÕK

Sarnaselt ICCPR-le, ei sisalda EIÕK eraldi põhiõigusena õigust isikuandmete kaitsele. Isikuandmete kaitse on osa laiemast põhiõigusest, s.t. õigusest eraelu kaitsele. Õigus eraelu kaitsele ei ole seejuures absoluutne ning seda võib piirata. Piiramine saab toimuda üksnes

[6] ÜRO Inimõiguste Komitee “CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8.04.1988”

kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik. Teisisõnu peab piirang olema:

a. ette nähtud seadusega;

b. õiguspärase eesmärgi huvides, milleks võib olla riigi julgeolek, ühiskondlik turvalisus, riigi majanduslik heaolu, korratus, kuriteo ärahoidmine, tervise või kõlbluse või teiste isikute õiguste ja vabaduste kaitse;

c. olema demokraatlikus ühiskonnas vajalik, sh proportsionaalne, sellise õiguspärase eesmärgi saavutamiseks.[7]

Seega peab mis tahes piirang isikuandmete kaitse õigusele vastama nendele tingimustele ning riik peab seda õigust piirates tegema vastama kaalumisotsuse.

(c) Konventsioon 108+

Isikuandmete töötlemist reguleerib ka Euroopa Nõukogu isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon (Konventsioon 108), millest on käesoleval hetkel välja töötatud nn moderniseeritud Konventsioon 108 (Konventsioon 108+)[8]. Konventsioon 108+ loodi Konventsioon 108 lisaprotokolliga ning asendab Konventsiooni 108. Kui Konventsioon 108 puudutas üksnes isikuandmete automatiseeritud töötlemist[9], siis Konventsioon 108+ reguleerib isikuandmete töötlemist laiemalt. Konventsioon 108+ on seejuures täielikult kooskõlas isikuandmete kaitse üldmäärusega[10] ja on sellega ülesehituselt võrdlemisi sarnane. On oluline märkida, et Konventsioon 108+ kohaldamisala ei ole – erinevalt isikuandmete kaitse üldmäärusest – piiratud julgeoleku ja riigikaitse valdkonnas. Seega kehtivad julgeoleku ja riigikaitse valdkonnas igal juhul ka Konventsioon 108+ sätestatud tingimused, isegi kui isikuandmete kaitse üldmäärus ei kohaldu. Julgeoleku ja riigikaitse kaalutlustel on siiski võimalik teha teatud erandeid Konventsioonis 108+ toodud nõuetest (vt lk 19).

Konventsioon 108+ loob kohustused selle osalisriikidele, kellel on kohustus Konventsioonis toodud kohustused üle võtta siseriiklikusse õigusesse. Konventsioon 108+ ei ole käesoleva analüüsi teostamise hetkeks veel Eesti poolt ratifitseeritud, kuid Euroopa Liidu Nõukogu menetluses on otsus, mis võimaldab EL-i liikmesriikidel see ratifitseerida.[11] Käesoleva analüüsi valmimise hetkel on Eesti seega üksnes Konventsioon 108 osalisriik, kuid võib eeldada, et liitub lähitulevikus Konventsiooniga 108+. Seetõttu oleme käesolevas analüüsis keskendunud Konventsioon 108+ sätetele, mis eelduslikult hakkavad asendama Konventsiooni 108.

Konventsioonis 108+ on isikuandmete töötlemine defineeritud kui „isikuandmetega tehtav toiming või toimingute kogum, nagu kogumine, säilitamine, hoidmine, muutmine, päringute tegemine, avalikustamine, kättesaadavaks tegemine, kustutamine või hävitamine, või andmete

[7] Handbook on European Data Protection Law. 2018 Edition. Luxembourg: Publications office of the European Union, 2018, lk 37-42. Kättesaadav: http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law (19.11.2018).

[8] Kättesaadav: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf (21.11.2018). Konventsioon 108 varasem (moderniseerimata) tekst on eesti keeles kättesaadav: https://www.riigiteataja.ee/akt/78300 (19.11.2018)

[9] Automatiseeritud töötlemine on Konventsioonis 108 defineeritud kui „järgmised täielikult või osaliselt automatiseeritud toimingud: andmete kogumine, andmete loogiline ja/või matemaatiline töötlemine, muutmine, kustutamine, väljavõtete tegemine või levitamine“.

[10] https://eur-lex.europa.eu/legal-content/ET/ALL/?uri=CELEX:52018PC0451, p 2.2. (21.11.2018)

[11] *Ibid* (21.11.2018)

loogiline ja/või aritmeetiline töötlemine“.[12] Oma sisult on Konventsioon 108+ märkimisväärselt spetsiifilisem kui teised rahvusvahelise õiguse instrumendid, kuid samas säilitab rahvusvahelise õigusele omase printsiipide-põhise lähenemise ning jätab osalisriikidele kaalutlusruumi konkreetse regulatsiooni kehtestamisel. Kuna dokumendi väljatöötamisel on teadlikult püütud tagada kooskõla Euroopa Liidu isikuandmete kaitse üldmäärusega, on konventsioonis sõnastatud printsiibid sarnased isikuandmete kaitse üldmääruses sätestatuga.

Konventsioon 108+ näeb ette järgmised isikuandmete töötlemise põhimõtted:

a. töödeldavad isikuandmed tuleb hankida ja töödelda ausal, läbipaistval ning seaduslikul teel. Töötlemise seaduslikkus tähendab, et isikuandmete töötlemiseks peab olema vabatahtlik, konkreetne, teadlik ja ühemõtteline nõusolek või muu õiguslik alus (analoogne isikuandmete kaitse üldmääruse artiklis 5 toodud põhimõttega „seaduslikkus, õiglus ja läbipaistvus“);

b. töödeldavad isikuandmed tuleb koguda seaduspäraselt ja täpselt ja selgelt määratletud eesmärkidel ning kasutada vastavalt nendele eesmärkidele (analoogne isikuandmete kaitse üldmääruse artiklis 5 toodud põhimõttega „eesmärgi piirang“);

c. töödeldavad isikuandmed peavad olema adekvaatsed, asjakohased, piisavad vastavalt töötlemise eesmärkidele (analoogne isikuandmete kaitse üldmääruse artiklis 5 toodud põhimõttega „võimalikult väheste andmete kogumine“);

d. töödeldavad isikuandmed peavad olema õiged ja vajadusel täiendatavad (analoogne isikuandmete kaitse üldmääruse artiklis 5 toodud põhimõttega „õigsus“);

e. töödeldavad isikuandmed peavad olema säilitatud vormis, mis lubab andmesubjekti teha kindlaks mitte kauemaks, kui perioodiks, mis on vajalik andmete töötlemise eesmärkide saavutamiseks (analoogne isikuandmete kaitse üldmääruse artiklis 5 toodud põhimõttega „säilitamise piirang“);

f. isikuandmete töötlemine peab olema proportsionaalne taotletava õiguspärase eesmärgiga ning igas töötlemise etapis peegeldama õiglast tasakaalu kõigi asjakohaste huvide (nii avalike kui erahuvide), õiguste ja vabaduste vahel;[13]

g. isikuandmete tahtmatu või tahtliku hävitamise, kaotsimineku, aga ka omavolilise juurdepääsu, muutmise või levitamise eest kaitsmiseks võetakse kasutusele kohased turvameetmed (analoogne isikuandmete kaitse üldmääruse artiklis 5 toodud põhimõttega „usaldusväärsus ja konfidentsiaalsus“).[14]

Konventsioon 108+ mainib ka eriliigiliste isikuandmete töötlemist ning spetsiifiliselt liigitab nende hulka „biomeetrilised andmed, mis võimaldavad unikaalselt isikut identifitseerida“. Konventsioon 108+ kohaselt on biomeetriliste andmete töötlemine lubatud üksnes siis, kui siseriiklikus õiguses tagatakse lisaks üldistele nõuetele ka nende andmete asjakohane kaitse, mis täiendavad Konventsioonis toodud meetmeid. Sellised kaitsemeetmed peavad kaitsma andmesubjekti tema huvidele, põhiõigustele ja vabadustele kaasnevate riskide vastu, eelkõige diskrimineerimise vastu.[15]

[12] Konventsioon 108+, art 2 lg b.

[13] *Ibid*, art 5.

[14] *Ibid*, art 7.

[15] *Ibid*, art 6.

Andmesubjektile peab olema Konventsioon 108+ alusel tagatud õigus andmetega tutvuda, õigus andmete parandamisele, õigus andmete kustutamisele, õigus isikuandmete töötlemise piiramisele, õigus esitada vastuväiteid, õigus järelevalveasutuse abile, õigus kasutada õiguskaitsevahendeid, õigus, et tema kohta ei võetaks vastu üksnes automatiseeritud töötlusel põhinevaid talle märkimisväärset mõju avaldavaid otsuseid.[16] Need õigused on sisult väga sarnased isikuandmete kaitse üldmääruses sisalduvate andmesubjekti õigustega.

Ülaltoodud põhimõtteid (töötlemise printsiipe ja andmesubjekti õiguseid) võib kitsendada juhul kui kitsendused on lubatud osalisriigi siseriikliku õigusega, austavad põhiõiguste ja -vabaduste põhiolemust, ning osutuvad demokraatlikus ühiskonnas vajalikeks ja proportsionaalseteks, et:

a. kaitsta riigi julgeolekut ja kaitsevõimet, avalikku korda, riigi olulisi majanduslikke ja finantshuve, kohtusüsteemi erapooletust ja iseseisvust, ennetada, uurida ja võtta isikuid vastutusele kuritegude eest ning jõustada kriminaalkaristusi, või muudeks üldistes avalikes huvides olevateks eesmärkideks; või
b. kaitsta andmesubjekti või muu isiku põhiõigusi ja -vabadusi, eelkõige väljendusvabadust.[17]

Seega võib teatud juhtudel ka Konventsioonis 108+ toodud printsiipe ja andmesubjekti õigusi piirata kui see on avalikes huvides (s.t. ka riigikaitse ja julgeoleku kaalutlustel). Piirangu kehtestamine aga eeldab riigi poolt vastava kaalumise läbiviimist.

3.1.2. Mittesiduva õiguse instrumendid

Lisaks eeltoodud õigusaktidele kasutab rahvusvaheline õigus ka nö leebe õiguse instrumente, mille sisuks on eelkõige poliitiliste tahte manifesteerimine ning mille vahetu eesmärk ei ole riikidele õiguslikult siduvaid kohustusi panna. Selliseid instrumente kasutatakse eelkõige olukordades, kus konsensuse saavutamine riikide vahel on keeruline või on teema poliitiliselt delikaatne.

Käesoleva analüüsi eset arvestades on olulisimad mittesiduva õiguse instrumendid UDHR ning ÜRO Peaassamblee ja Inimõiguse Komitee resolutsioonid. UDHR-s on õigus privaatsusele tuletatav (sarnaselt teistele rahvusvahelise õiguse õigusallikatele) õigusest eraelu kaitsele. Ehkki UDHR ei ole õiguslikult siduv, peetakse selles toodud kohustusi riikidele siduvaks, sh mõnede õigusteadlaste arvates ka rahvusvaheliseks tavaõiguseks.

Arvestades digitaalse ajastuga seotud väljakutseid ning viimasel kümnendil asetleidnud skandaale inimeste jälgimise osas, on ka ÜRO Peaassamblee ning ÜRO Inimõiguste Komitee avaldanud mittesiduvad resolutsioone, milles on rõhutatud vajadust austada inimeste privaatsust. Ehkki resolutsioonid ei keskendu konkreetselt biomeetrilistele andmetele, on selles toodud põhimõtted ja üleskutsed kaudselt seotud või põhjustatud ka biomeetriliste andmete ülemäärasest või invasiivsest töötlemisest riikide poolt (nt kõigi kodanike kohustuslik DNA-testimine ja andmete salvestamine Kuveidi poolt). Eesti on nimetatud resolutsioonidega ühinenud ning seetõttu tuleb õigusraamistiku kujundamisel arvestada ka nendes dokumentides sõnastatud eesmärke.

[16] Konventsioon 108+, art 9.

[17] *Ibid*, art 9 lg 2.

3.2. Euroopa Liidu õigus

Euroopa Liidu õigus		
Euroopa Liidu põhiõiguste harta	Artikkel 8	1. Igaühel on õigus oma isikuandmete kaitsele. 2. Selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. Igaühel on õigus tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist. 3. Nende sätete täitmist kontrollib sõltumatu asutus.
	Artikkel 52 (1)	1. Hartaga tunnustatud õiguste ja vabaduste teostamist tohib piirata ainult seadusega ning arvestades nimetatud õiguste ja vabaduste olemust. Proportsionaalsuse põhimõtte kohaselt võib piiranguid seada üksnes juhul, kui need on vajalikud ning vastavad tegelikult liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või kui on vaja kaitsta teiste isikute õigusi ja vabadusi.
	Artikkel 53	Harta sätteid ei või tõlgendada neid inimõigusi või põhivabadusi kitsendavate või kahjustavatena, mida asjaomastes kohaldamisvaldkondades on tunnustatud rahvusvahelise õiguse ja rahvusvaheliste lepingutega, millega on ühinenud liit või kõik liikmesriigid, kaasa arvatud Euroopa inimõiguste ja põhivabaduste kaitse konventsioon, ning liikmesriikide põhiseadustega.
Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta **(isikuandmete kaitse üldmäärus)**	Põhjenduspunkt 16	Käesolevas määruses ei käsitleta põhiõiguste ja -vabaduste kaitse küsimusi ega andmete vaba liikumist, mis on seotud väljapoole liidu õiguse kohaldamisala jääva tegevusega, näiteks riigi julgeolekut puudutava tegevusega, ega isikuandmete töötlemist liikmesriikide poolt liidu ühise välis- ja julgeolekupoliitikaga seonduva tegevuse läbiviimisel.
	Artikkel 5	1. Isikuandmete töötlemisel tagatakse, et a. töötlemine on seaduslik, õiglane ja andmesubjektile läbipaistev („seaduslikkus, õiglus ja läbipaistvus“); b. isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning

		õiguspärastel eesmärkidel ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus; isikuandmete edasist töötlemist avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgil ei loeta artikli 89 lõike 1 kohaselt algsete eesmärkidega vastuolus olevaks („eesmärgi piirang“); c. isikuandmed on asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt („võimalikult väheste andmete kogumine“); d. isikuandmed on õiged ja vajaduse korral ajakohastatud ning et võetakse kõik mõistlikud meetmed, et töötlemise eesmärgi seisukohast ebaõiged isikuandmed kustutaks või parandataks viivitamata („õigsus“); e. isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse; isikuandmeid võib kauem säilitada juhul, kui isikuandmeid töödeldakse üksnes avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgil vastavalt artikli 89 lõikele 1, eeldusel et andmesubjektide õiguste ja vabaduste kaitseks rakendatakse käesoleva määrusega ettenähtud asjakohaseid tehnilisi ja korralduslikke meetmeid („säilitamise piirang“); f. isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid („usaldusväärsus ja konfidentsiaalsus“); 2. Lõike 1 täitmise eest vastutab ja on võimeline selle täitmist tõendama vastutav töötleja („vastutus“).
	Artikkel 9 (1) ja 9 (2) (g)	1. Keelatud on töödelda isikuandmeid, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või

		filosoofilised veendumused või ametiühingusse kuulumine, geneetilisi andmeid, füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid, terviseandmeid või andmeid füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta. 2. Lõiget 1 ei kohaldata, kui kehtib üks järgmistest asjaoludest: g. töötlemine on vajalik olulise avaliku huviga seotud põhjustel liidu või liikmesriigi õiguse alusel ning on proportsionaalne saavutatava eesmärgiga, austab isikuandmete kaitse õiguse olemust ja tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks;
	Artikkel 9 (4)	4. Liikmesriigid võivad säilitada või kehtestada täiendavad tingimused, sealhulgas piirangud seoses geneetiliste, biomeetriliste või terviseandmete töötlemisega.

Kokkuvõte

- EL-i õigus, eelkõige isikuandmete kaitse üldmäärus, sätestab biomeetriliste andmete töötlemise põhimõtted ning lubatud õiguslikud alused.
- Biomeetriliste andmete töötlemise õiguslik alus ABIS-süsteemi kontekstis saab olla isikuandmete kaitse üldmääruse art 9(2)(g).
- Biomeetriliste andmete töötlemiseks olulise avaliku huviga seotud põhjusel peab vastav alus olema EL-i või liikmesriigi õiguses. Teisisõnu, erialused biomeetriliste andmete töötlemisel võivad tuleneda eriseadustest, sh nii Euroopa Liidu õigusaktidest kui ka liikmesriikide siseriiklikust õigusest.
- Enne erialuse kehtestamist siseriiklikus (või EL-i) õiguses tuleb läbi viia vastav kaalumine, s.t. hinnata, kas soovitud õiguslik alus on: a) proportsionaalne taotletava eesmärgiga; b) austab isikuandmete kaitse õiguse olemust; ja c) tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks.
- Isikuandmete kaitse üldmääruse kohaselt on liikmesriikidel õigus sätestada täiendavaid tingimusi, sh piiranguid, biomeetriliste andmete töötlemiseks.

(a) Euroopa Liidu põhiõiguste harta

Euroopa Liidu põhiõiguste harta[18] sätestab isikuandmete kaitse põhiõiguse. Sarnaselt enamike rahvusvaheliste instrumentidega, ei reguleeri harta spetsiifiliselt biomeetriliste andmete töötlemist. Seega kehtivad hartas toodud üldised põhimõtted ka biomeetriliste andmete kui isikuandmete eriliigi töötlemise suhtes. Õigust isikuandmete kaitsele tohib piirata üksnes hartas toodud tingimustel ning harta sätteid ei tohi tõlgendada kitsendavalt viisil, mida vastavas kohaldamisvaldkonnas on tunnustatud rahvusvahelise õiguse ja rahvusvaheliste lepingutega, millega on ühinenud liit või kõik liikmesriigid, ning liikmesriikide põhiseadustega.

See tähendab, et isikuandmete töötlemine, sh biomeetriliste andmete töötlemine, peab vastama järgnevatele kriteeriumidele:

a. piirang peab olema ette nähtud seadusega;[19]
b. piirang peab arvestama andmekaitse õiguse olemusega;[20]
c. piirang peab vastama liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või peab olema vajalik kaitsmaks teiste isikute õigusi ja vabadusi;
d. piirang peab olema selleks eesmärgiks vajalik; ning
e. piirang peab olema selle eesmärgiga proportsionaalne.

Punktis c. nimetatud *üldist huvi pakkuv eesmärk* või *teiste isikute õigused ja vabadused* peavad olema piisavalt konkreetselt määratletud, et oleks võimalik hinnata, kas piirang on selle eesmärgi täitmiseks vajalik ja sellega proportsionaalne. Piirang on eesmärgi täitmiseks *vajalik,* kui valitud on kõige vähem põhiõiguseid riivav meede. Piirang on eesmärgiga *proportsionaalne*, kui piirangust tulenev kasu kaalub üles põhiõiguste piiramisega kaasneva kahju.[21] Nende hartas toodud kriteeriumide analüüsimisel tuleb arvesse võtta isikuandmete töötlemise põhimõtteid, mis on täpsustatud mh isikuandmete kaitse üldmääruses ja õiguskaitseasutuste direktiivis.

(b) Isikuandmete kaitse üldmäärus

Isikuandmete kaitse üldmäärust kohaldatakse isikuandmete täielikult või osaliselt automatiseeritud töötlemise suhtes ja isikuandmete automatiseerimata töötlemise suhtes, kui

[18] Euroopa Liidu põhiõiguste harta, https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A12012P%2FTXT (03.12.2018)

[19] See tähendab, et piirangud peavad põhinema õiguslikul alusel, mis on kättesaadav, ettenähtav ja piisavalt täpne, et isikud saaks mõista oma kohustusi ja suunata oma käitumist. Õiguslik alus peab selgelt määratlema isikuandmete töötlemise ulatuse ja viisi asutuste pädevuste teostamiseks, et kaitsta andmesubjekte liialdaste riivete eest. Seaduslikku alust sisustatakse sarnaselt Euroopa inimõiguste ja põhivabaduste konventsiooni artikkel 8 lg 2 elemendiga, mille kohaselt piirang eraelu kaitsele peab olema „kooskõlas seadusega“. Vt Handbook on European Data Protection Law, lk 42-43.

[20] Euroopa Komisjon on leidnud, et Euroopa infosüsteemide koostalitlusvõime korral on isikuandmete (sh biomeetriliste andmete) töötlemine kooskõlas põhiõiguse olemusega. Vt Commission Staff Working Document SWD(2017) 473. Impact assessment accompanying the document „PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226“ and „PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)“, p 36.

[21] Handbook on European Data Protection Law, p 46.

kõnealused isikuandmed kuuluvad andmete kogumisse või kui need kavatsetakse kogumisse kanda.

Isikuandmete kaitse üldmääruse kohaldamisalasse ei kuulu isikuandmete töötlemine järgmistel juhtudel: a) töötlemine EL-i õiguse kohaldamisalasse mittekuuluva tegevuse käigus; b) töötlemine ühise välis- ja julgeolekupoliitika teostamise käigus; c) töötlemine pädevate asutuste poolt süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise, sh avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil.[22] Viimasel juhul kohaldatakse õiguskaitseasutuste direktiivi (vt ptk 6.6.1).[23] Kuna isikuandmete kaitse üldmääruse kohaldamisalasse jääb kõik, mille osas EL-i pädevus ei ole välistatud, võimaldab see määruse kohaldamisala osas laiendavat tõlgendamist.

Isikuandmete kaitse üldmääruses sisalduv seaduslikkuse nõue tähendab, et isikuandmete töötlemiseks peab alati olema õiguslik alus. Õiguslik alus on kas andmesubjekti nõusolek või muu õigusaktist tulenev alus. Biomeetriliste andmete, mis on isikuandmete eriliigiks isikuandmete üldmääruse mõttes, töötlemise võimalikud õiguslikud alused on nimetatud isikuandmete kaitse üldmääruse art-s 9(2). Asjakohane õiguslik alus biomeetriliste andmete kogumiseks infosüsteemi ABIS kontekstis oleks tõenäoliselt art 9 (2)(g) – töötlemine on vajalik olulise avaliku huviga seotud põhjustel liidu või liikmesriigi õiguse alusel ning on proportsionaalne saavutatava eesmärgiga, austab isikuandmete kaitse õiguse olemust ja tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks.

- *Andmesubjekti nõusolek õigusliku alusena*

Lisaks võib teatud tingimustel biomeetriliste andmete töötlemisel õiguslikuks aluseks olla andmesubjekti selgesõnaline nõusolek[24]. Nõusolekule kui õiguslikule alusele tuginemine on aga enamikes olukordades avalik-õigusliku suhte puhul problemaatiline, sest nõusolek peab olema muu hulgas *vabatahtlik*[25] tahteavaldus. Avalik-õiguslikus suhtes ei saa aga enamikel juhtudel pidada nõusolekut vabatahtlikult antuks. Nõusolek ei saa olla vabatahtlik, kui andmesubjekt ja vastutav töötleja on selgelt ebavõrdses olukorras, seda näiteks juhul kui vastutav töötleja on avaliku sektori asutus. Olukorras, kus andmesubjekti on vastamisi avalikku võimu teostava isikuandmete töötlejaga, on kaheldav, et nõusolek antakse konkreetse olukorra kõiki asjaolusid arvestades vabatahtlikult.[26]

Lisaks sellele on andmesubjektil õigus nõusolek igal ajal tagasi võtta, mille järel ei saa vastutav töötleja enam edasise töötlemise osas nõusolekule tugineda. ABIS-e puhul ei ole nõusolek ka sel põhjusel soovitud eesmärgi täitmiseks sobiv lahendus, sest igal ajahetkel võib andmesubjekt tema isikuandmete edasise töötlemise osas nõusoleku tagasi võtta ning sellisel juhul tuleb isikuandmete töötlemine lõpetada või leida selleks muu õiguslik alus. Isegi kui nõusolekule tuginemine oleks teoreetiliselt võimalik, tekitaks nõusolekute haldamine riigile suurt administratiivset koormust. Seega tuleks ABIS-e süsteemis isikuandmete töötlemiseks leida vastav õiguslik alus seadusest (või vajadusel ja võimalusel see luua).

- *Andmesubjekti õigused ja nende piiramine*

[22] Isikuandmete kaitse üldmääruse art 2(1), (2) (a), (b), (d)

[23] Õiguskaitseasutuste direktiiv art 1(1)

[24] Isikuandmete kaitse üldmääruse art 9(2)(a)

[25] Isikuandmete kaitse üldmääruse art 4(11).

[26] Isikuandmete kaitse üldmääruse pp 43.

Vastutav töötleja peab tagama isikuandmete kaitse üldmääruse III peatükis sätestatud andmesubjekti õiguste realiseerimise võimaluse. Liikmesriik võib üldmääruse art-le 23 tuginedes seadusandliku meetmega piirata andmesubjekti õiguseid, kui selline piirang austab põhiõiguste ja -vabaduste olemust ning on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede, et tagada:

a. riigi julgeolek;
b. riigikaitse;
c. avalik julgeolek;
d. süütegude tõkestamine, uurimine, avastamine või nende eest vastutusele võtmine või kriminaalkaristuste täitmisele pööramine, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmine ja nende ennetamine;
e. liidu või liikmesriigi muud üldist avalikku huvi pakkuvad olulised eesmärgid, eelkõige liidu või liikmesriigi oluline majanduslik või finantshuvi, sealhulgas rahandus-, eelarve- ja maksuküsimused, rahvatervis ja sotsiaalkindlustus;
f. kohtusüsteemi sõltumatuse ja kohtumenetluse kaitse;
g. reguleeritud kutsealade ametieetika rikkumiste ennetamine, uurimine, avastamine ja nende eest vastutusele võtmine;
h. jälgimine, kontrollimine või regulatiivsete ülesannete täitmine, mis on kas või juhtumipõhiselt seotud avaliku võimu teostamisega eelnimetatud juhtudel, v.a kohtusüsteemi sõltumatuse ja kohtumenetluse kaitsega;
i. andmesubjekti kaitse või teiste isikute õiguste ja vabaduste kaitse;
j. tsiviilõiguslike nõuete täitmise tagamine.[27]

Selline seadusandlik andmesubjekti õigusi ja vabadusi piirav meede peab sisaldama teatud konkreetseid sätteid vähemalt järgmise kohta:

a. töötlemise või selle kategooriate eesmärgid;
b. isikuandmete liigid;
c. kehtestatud piirangute ulatus;
d. kuritarvitamist või ebaseaduslikku andmetega tutvumist või nende edastamist tõkestavad kaitsemeetmed;
e. vastutava töötleja või vastutavate töötlejate kategooriate määratlus;
f. säilitamise ajavahemikud ja kohaldatavad kaitsemeetmed, võttes arvesse töötlemise või selle kategooriate laadi, ulatust ja eesmärki;
g. andmesubjektide õigusi ja vabadusi ähvardavad ohud ning
h. andmesubjektide õigus olla piirangust teavitatud, välja arvatud juhul, kui see võib mõjutada piirangu eesmärki.

Seega tuleks vastavat seadusandlikku regulatsiooni planeerides lähtuda isikuandmete kaitse üldmääruses toodud täpsustustest, mis annavad õiguse andmesubjekti õigusi teatud tingimustel piirata.

[27] Isikuandmete kaitse üldmääruse art 23(1)

4. BIOMEETRILISTE ANDMETE TÖÖTLEMINE ÜHES ANDMEKOGUS

Biomeetriliste andmete koondamine ühte riiklikusse andmekogusse võimaldab ühelt poolt riigil korrastada olemasolevaid andmeid ning tagada nende töötlemisele tsentraalne ja ühetaoline lähenemine. Ehkki käesoleval hetkel töötleb ja kogub riik juba hulga biomeetrilisi isikuandmeid, on nende andmete töötlemise infrastruktuur hetkel hajutatud ega võimalda nende võrdset ja ühetaolist haldamist, sh andmete turvalisuse tagamist. Samuti on praegused isiku tuvastamise ja isikusamasuse kontrollimise infotehnoloogilised lahendused on vananenud ning vajavad uuendamist.

Käesolevas peatükis analüüsime, kas ja milliseid piiranguid seab rahvusvaheline õigus ja Euroopa Liidu õigus erinevate biomeetriliste andmete töötlemisele ühes andmekogus. Seejuures on fookus isikuandmete töötlemist reguleerivatel üldise iseloomuga õigusaktidel, mitte konkreetsete menetlusliikidega seotud regulatsioonil (st ei analüüsita, kas dokumendimenetluses kogutud andmeid võib konkreetse valdkonna õigusaktidest tulenevalt hoida samas andmekogus süüteomenetluses kogutud andmetega).

4.1. Rahvusvaheline õigus

Õigusakt	Säte	Sõnastus
Konventsioon 108+	Artikkel 5	1. Andmete töötlemine peab olema taotletava õiguspärase eesmärgiga proportsionaalne ning töötlemise igal sammul peegeldama õiglast tasakaalu kõigi huvide vahel, sõltumata sellest, kas need on avalikud või erasfääris, ning kaalul olevate õiguste ja vabaduste vahel. 2. Iga osapool tagab, et andmete töötlemine saab põhineda andesubjekti vabal, konkreetsel, informeeritud ning ühemõttelisel nõusolekul või mõnel muul seaduses sätestatud õiguslikul alusel. 3. Isikuandmed tuleb töödelda seaduslikult. 4. Töödeldavad isikuandmed peavad olema: a. töödeldud ausal ja läbipaistval viisil; b. kogutud selgesõnalisel, konkreetsel ja õigustatud eesmärgil ning mitte olla töödeldud nende eesmärkidega mittesobival eesmärgil; edasine töötlemine arhiveerimise eesmärgil avalikes huvides, teadusliku või ajaloolise uurimuse eesmärgil või statistilisel eesmärgil peab olema teostatud asjakohaste kaitsemeetmete abil, mis vastavad nendele eesmärkidele. c. olema piisavad, asjakohased ja mitte ülemäärased vastavalt nende eesmärkidele, milleks neid töödeldakse;

		d. olema täpsed ja, kus vajalik, ajakohased. e. säilitatud vormis, mis lubab andmesubjekti teha kindlaks mitte kauemaks, kui perioodiks, mis on vajalik andmete töötlemise eesmärkide saavutamiseks.
EIÕK	Artikkel 8	1. Igaühel on õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning sõnumite saladust. 2. Ametivõimud ei sekku selle õiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks.

Kokkuvõte:

- Rahvusvaheline õigus ei reguleeri konkreetselt erinevatest menetlustest hõivatud biomeetriliste andmete töötlemist ühes andmekogus.
- Andmete töötlemisel ühes andmekogus tuleb järgida üldisi printsiipe isikuandmete töötlemisele, ennekõike eesmärgi piirang, seaduslik alus, töötlemise läbipaistvus ja õiglus.
- Rahvusvahelisest õigusest tulenevad printsiibid piiravad biomeetriliste andmete töötlemist ühes andmekogus.
- Nendest piirangutest ülesaamiseks on teatud juhtudel kehtestatud erandid, kuid nende rakendamine eeldab riigi poolt kaalumist ja vastava kaalumise tulemusena tingimustele vastava õigusliku aluse kehtestamist.

Ühtsete andmekogude loomist ei ole rahvusvahelises õiguses spetsiifiliselt käsitletud, seega tuleb lähtuda rahvusvahelise õiguse õigusaktides toodud põhiprintsiipidest, mida käsitlesime täpsemalt peatükis 3.1.

Näiteks tuleneb Konventsioonist 108+, et andmete töötlemine peab olema legitiimse eesmärgiga proportsionaalne igas andmetöötluse etapis ning seejuures tuleb kaaluda avalikke ja erahuve ning õigusi ja vabadusi. Töötlemiseks vajaliku õigusliku aluse nõue hõlmab Konventsioon 108+ seletuskirja järgi ka andmete töötlemist avalikes huvides. Teisisõnu peab avalikes huvides töötlemise alus olema seaduses sätestatud. Isikuandmete töötlemine peab toimuma seadusega kooskõlas, õiglaselt ja läbipaistval viisil.

Andmete kogumine on Konventsiooni 108+ kohaselt lubatud ainult selgelt defineeritud legitiimsel eesmärgil ning töötlemine peab neile eesmärkidele vastama. Legitiimse eesmärgi määratlemine sõltub asjaoludest, kuna eesmärgiks on tagada kõigi õiguste ja vabaduse ning huvide tasakaal – ühelt poolt andmesubjekti õigused ja teiselt poolt andmetöötleja või ühiskonna huvid. Töötlemise eesmärgiks võivad olla valdkonniti näiteks rahandus-, eelarve- ja maksuküsimused, rahvatervis ja sotsiaalkindlustus, kuritegude ennetamine, uurimine,

avastamine ja nende eest vastutusele võtmine ning kriminaalkaristuste täitmine, reguleeritud kutsealade eetikarikkumise tuvastamine, riikliku julgeoleku kaitse, tsiviilõiguslike nõuete täitmise tagamine ning kohtuliku sõltumatuse ja kohtumenetluse kaitse. Kuid enne seadusliku aluse kehtestamist tuleb igal juhul vastavat eesmärki kaaluda kõigi osapoolte huvide ja õiguste vastu.

Isikuandmete edasine töötlemine (st teisene töötlemine) avalikes huvides on printsiibis lubatud, kui selleks on nõuetele vastav õiguslik alus ning rakendatakse asjakohaseid kaitsemeetmeid (nt saladuse hoidmise kohustus, andmetele juurdepääsu piiravad normid ja andmevahetuse piirangud). Andmed peavad olema korrektsed ja ajakohased. Kui andmete töötlemise eesmärk on saavutatud, tuleks andmed kustutada või säilitada neid viisil, mille puhul on tagatud, et andmesubjekti identifitseerimine pole võimalik.[28] Andmete edasisest töötlemisest räägib täpsemalt peatükk 7.

Eriliigilisi andmeid (sh biomeetrilisi andmeid) võib töödelda ainult asjakohaste seadusega sätestatud kaitsemeetmete olemasolul. Konventsioon 108+ seletuskirjas on täpsustatud, et biomeetrilised andmed on eriliigilised tundlikud andmed, kui neid kasutatakse andmesubjekti tuvastamiseks.[29]

Seega ei ole ühise andmekogu loomine ja selles sisalduvate biomeetriliste andmete töötlemine (sh edasine töötlemine) rahvusvahelise õiguse alusel keelatud. Selleks peab aga olema õiguslik alus, mis on kooskõlas mh rahvusvahelises õiguses kehtestatud printsiipidega, ning rakendada tuleb täiendavaid kaitsemeetmeid selliste andmekogude turvalisuse tagamiseks.

4.2. Euroopa Liidu õigus

Õigusakt	**Säte**	**Sõnastus**
Isikuandmete kaitse üldmäärus	Artikkel 9 (1) ja 9 (2) (g)	1. Keelatud on töödelda isikuandmeid, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilisi andmeid, füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid, terviseandmeid või andmeid füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta. 2. Lõiget 1 ei kohaldata, kui kehtib üks järgmistest asjaoludest: g. töötlemine on vajalik olulise avaliku huviga seotud põhjustel liidu või liikmesriigi õiguse alusel ning on proportsionaalne saavutatava eesmärgiga, austab isikuandmete kaitse õiguse olemust ja tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks

[28] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, p-d 46-53 (10.10.2018)

[29] *Ibid*, p 58

Kokkuvõte

- EL-i õigus ei keela erinevate menetluste käigus hõivatud biomeetriliste andmete töötlemist ühes andmekogus.
- EL-i õigusest tulenevad piiranguid (seaduslikkuse ja eesmärgipärasuse põhimõte, andmete minimaalsuse põhimõte, usaldusväärsus ja konfidentsiaalsus, säilitamise piirang, kaitsemeetmete rakendamine jms), mis mõjutavad sellise andmekogu loomist ja käitamist.
- EL-i õigusest tulenevatele piirangutele võib vastata lahendus, kus ühes andmekogus hoitavate andmete osas on piiratud nende töötlemine ja kasutamine (nt läbi piiratud volituste ja ligipääsuõiguste haldamise).

EL-i õigusest ei tulene otsest keeldu erinevate menetluste raames hõivatud biomeetriliste andmete töötlemiseks ühes andmekogus. Siiski on mitmed piirangud, millega sellise andmekogu loomisel tuleb arvestada.

Üldreeglina on biomeetriliste andmete töötlemine keelatud (isikuandmete kaitse üldmääruse art 9(1)). Biomeetriliste andmete töötlemine võib olla erandina lubatud, kui töötlemine on vajalik olulise avaliku huviga seotud põhjustel liidu või liikmesriigi õiguse alusel ning on proportsionaalne saavutatava eesmärgiga, austab isikuandmete kaitse õiguse olemust ja tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks. Kuivõrd andmete töötlemine ABIS-e süsteemis võiks olla põhjendatud olulise avaliku huviga, tuleks antud erandi sobivust õigusliku alusena vastavat seadusandlikku akti luues põhjalikumalt analüüsida (vt ptk 3.2(b)).

Vajab märkimist, et EL ei reguleeri siseriiklike andmebaaside loomise ja käitamisega seotud küsimusi. Ehkki juhul kui see on vajalik tehniliseks ühildamiseks EL-i andmebaasiga, võib EL kehtestada teatud ühtsed standardid sellise infosüsteemide koostalituse tagamiseks. Ühtlasi on EL-i pädevuses selliste reeglite kehtestamine, mis puudutab EL-i andmebaaside käitamist (kuhu ka liikmesriigid saadavad andmeid, sh biomeetrilisi andmeid).

(a) Euroopa Liidu andmebaaside koostalitusvõime

Analoogia korras võib ära märkida EL-i enda tsentraalsete andmebaaside toimimise. Euroopa Liidu Põhiõiguste Amet (FRA) on analüüsinud EL-i enda hallatavate andmebaaside koostalitlusvõime loomist. Koostalitlusvõime loomine erinevate andmebaaside vahel ei tähenda küll koondandmebaasi plaanitava ABIS-ega sarnasel kujul, kuid FRA poolt analüüsitud riskid isikuandmete kaitsele on ülekantavad ka koondandmebaasi loomise ja käitamise konteksti. Koostalitlusvõime osas on kirjeldatud mitut võimalikku opereerimise varianti: 1) üks otsinguliides, mis otsib erinevatest süsteemidest ja näitab tulemusi koos; 2) ühine biomeetriliste andmete võrdlemise teenus, mis võrdleb andmeid mitme andmebaasiga ja võimaldab isiku identifitseerida; 3) ühine andmebaas, mis vahetab infot mitmete andmebaaside vahel ja võimaldab saada kogu info isiku kohta ka siis, kui tal on andmebaasides mitu identiteeti; ning 4) infosüsteemide omavaheline ühildamine, milles ühte andmebaasi sisestatud andmeid võrreldaks automaatselt teiste süsteemidega.

Mis tahes koostalitlusvõimeline lahendus peab vastama isikuandmete kaitse nõuetele. Seejuures tuleb silmas pidada, et biomeetriliste andmete puhul on tegemist eriliigiliste isikuandmetega, mis nõuavad töötlemisel täiendavat kaitset. Andmebaaside koostalitlusvõime loomine kõrgendab riski andmete kvaliteedi ja usaldusväärsuse osas. Samuti suureneb ühise

andmebaasi rünnaku risk. Muu hulgas ei tohi andmebaaside koostalitlusvõime loomine FRA hinnangul viia selleni, et töödeldakse rohkem andmeid, kui andmete töötlemise eesmärgi saavutamiseks vaja on. Tehnilised lahendused peavad võimaldama andmebaasidele juurdepääsu ainult volitatud isikutele ja lubatud eesmärkidel. Samuti peab tehniline lahendus võimaldama andmete automaatset kustutamist, et pidada kinni andmete säilitamise tähtaegadest. EL-i andmekogude planeeritav ühine andmete võrdlemisteenus (*Biometric Matching Service, BMS*) ja otsinguliides peaks FRA raportite kohaselt olema programmeeritud andmeid võrdlema, kuid mitte neid võrdlusandmeid säilitama.[30]

Isikuandmeid tuleb kaitsta nii, et volitamata isikutel puuduks juurdepääs. See põhimõte on sätestatud nii isikuandmete kaitse üldmääruses (art 28 ja 32) kui ka Konventsioonis 108+. EL-i andmebaaside kontekstis on näiteks andmete vastutaval töötlejal kohustus pidada logi kõigi andmebaasi päringute osas, samuti tuleb luua kindlad reeglid selles osas, kellel on ligipääs kogutud andmetele.

Andmebaaside koostalitlusvõime osas on eriti oluline aspekt laste õiguste kaitse arvestades nende erilist seisundit. Laste andmete töötlemine nõuab eriti rangelt eesmärgipiirangust kinnipidamist. Laste andmete töötlemisel ei tohiks ametnikud saada teada, kui isiku kohta on veel andmeid, millele neile juurdepääsu ei ole.[31] Laste puhul on andmete usaldusväärsus pideva füüsilise arengu tõttu väiksem kui täiskasvanute puhul. Sellest tulenevalt peaks kõiki lapsi puudutavaid rohkem kui 5 aasta taguseid andmeid täiendavalt kontrollima. Samuti on FRA väljendanud seisukohta, et kriminaalkuritegude puhul ei peaks laste kohta käivad andmed olema ristkasutatavad või siis peaks võimalik olema saada vaid väga piiratud andmeid, nt eriti raskete kuritegude puhul.[32] Vastavalt ÜRO standardsetele miinimumeeskirjadele alaealiste asjades õigusemõistmise kohta (nn Pekingi eeskirjadele)[33], tuleb alaealiste õigusrikkujate toimikuid hoida konfidentsiaalsena ning sama isiku suhtes täiskasvanueas toimuvas menetluses ei tohiks neid andmeid hiljem kasutada. Põhimõtet on korratud ka ÜRO lapse õiguste konventsioonis.

Andmebaaside koostalitlusvõime puhul on üks probleemküsimus, millal peaks ametnik saama teada, et andmebaasis on infot, kuid tal ei ole volitust selle vaatamiseks. Kuigi ametnik ei näe infot, võib siiski ka asjaolu, et ta näeb, et info on olemas, anda talle lisateadmise, mida ta muidu ei saaks. Europol on selliseks olukorraks arendanud süsteemi, mis võimaldab teatud juhtudel varjata ametniku eest, kellel volitust ei ole, ka asjaolu, et süsteemis on info. Sellises olukorras saab liikmesriik, kellele info kuulub, kõigepealt teate ning saab siis otsustada, kas reageerib sellele.[34]

Kuna EL ei reguleeri siseriiklike andmebaasidega seotud küsimusi, ei selgita FRA juhised ka siseriiklike andmebaaside koostalitlusvõimet. Samas kehtivad ka siseriiklikes andmebaasides isikuandmete töötlemisele samad isikuandmete kaitse nõuded ja põhimõtted, mis tulenevad rahvusvahelisest ja EL-i õigusest. Seega võib FRA juhistes toodud soovitustest tuua paralleele ka siseriiklike andmekogude käitamisele, kuid konkreetsemalt põhineb siseriiklike andmekogude koostalitlusvõime loomine iga riigi siseriiklikul õigusel. Seejuures tuleb järgida

[30] European Union Agency for Fundamental Rights (FRA). Fundamental rights and the interoperability of EU information systems: borders and security (2017), lk 24

[31] FRA, lk 35

[32] FRA, lk 38

[33] United Nations. Standard Minimum Rules for the Administration of Juvenile Justice ("The Beijing Rules"). 29.11.1985, rule 21

[34] FRA, lk 23, Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/794 art 20(2)

kõiki turvanõudeid, mis EL-i õigusest tulenevad ja ühise infokogumi loomine muudab nõuded veel veidi karmimaks, kuivõrd riskid suurenevad.

4.2.2. Kohtupraktika

Järgnevalt toome välja kohtupraktikat, milles on sisustatud eespool käsitletud printsiipe ja põhimõtteid isikuandmete töötlemisel EIÕK ja EL-i õiguse alusel.

(a) Isikut tõendavate dokumentide menetluses kogutud andmete tsentraalne hoiustamine

Biomeetriliste passide tarbeks töödeldavate isikuandmete osas on Euroopa Kohus leidnud, et andmete keskse hoiustamise puhul tuleb järgida karmimaid nõudeid, kui andmete passis (s.o. andmekandjal ehk kiibil) hoidmisel.[35] Lahendis *M.K. vs. Prantsusmaa* leidis Euroopa Inimõiguste Kohus, et sõrmejälgede säilitamine ainult tulevikus identiteedivarguse vältimiseks oleks praktikas samaväärne, nagu kogu elanikkonnalt süstemaatiliselt selliste andmete kogumine, mis on ilmselgelt ülemäärane.[36] Ka Euroopa Andmekaitseinspektor on rõhutanud, et kõik süsteemid, milles töödeldakse biomeetrilisi andmeid, peavad olema efektiivselt kaitstud vigade ning ebaseadusliku juurdepääsu ja kasutamise eest.[37]

Põhimõtted, mida mh tuleb keskse andmebaasi loomisel järgida, on võimalikult väheste andmete kogumine, eesmärgi piirang ja säilitamise piirang. Eesmärgi piirang on keskse süsteemi puhul peamine probleemkoht. Eesmärgi piirangu kohaselt kogutakse isikuandmeid täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei tohi hiljem töödelda viisil, mis erineb eelnevalt kindlaksmääratud eesmärgist.[38] Isikul, kelle andmeid töödeldakse, peaks olema võimalik ette näha eesmärke, millel tema andmeid töödeldakse.[39]

Eraldiseisvad infosüsteemid toimivad juba iseenesest kaitsemeetmena lubamatul eesmärgil andmete töötlemise vastu. Euroopa Komisjon on rõhutanud, et üldine EL-i infosüsteem kujutaks endast jämedat isikute õiguse eraelu ja andmekaitsele rikkumist ning oleks suur väljakutse arenduse ning toimimise osas.[40] Sama muret on väljendanud ka Euroopa Inimõiguste Kohus[41] ning Euroopa Kohus[42], kes on toonud välja, et isikuandmete detsentraliseeritud hoidmine vähendab andmete lubamatul eesmärgil kasutamise riski. Euroopa Inimõiguste Kohus on viidatud lahendis välja toonud, et kuritegevuse ennetamise eesmärgil sõrmejälgede kogumine võib üles kaaluda isiku õiguse isikuandmete kaitsele. See ei tähenda aga, et igal eesmärgil andmete töötlemine kaaluks üles isikute õiguse isikuandmete kaitsele.

(b) Eesmärgi piirang ja andmete säilitamine

[35] C-291/12, Schwarz v. Bochum, 17.10.2013, p 59-63

[36] Euroopa Inimõiguste Kohus (ECtHR) M.K. v. France, No. 76100/13, 18.04.2013, p 40

[37] EDPS. Opinion on the Second EU Smart Borders Package (2016), p 38

[38] FRA, lk 46

[39] Euroopa Kohus (CJEU) C-275/06, Promusicae v. Telefónica de España SAU, kohtujuristi arvamus 18.07.2007, p 53

[40] Euroopa Komisjon. Ülevaade teabehaldusest vabadusel, turvalisusel ja õigusel rajaneval alal, 20.07.2010, p 3, lk 21-24

[41] ECtHR, S. and Marper v. United Kingdom, Nos. 30562/04, 30566/04, 04.12.2008, p 103-104

[42] CJEU, C-291/12, Schwarz v. Bochum, 17.10.2013, p 55

Lahendis, millega Euroopa Kohus tunnistas kehtetuks andmete säilitamise direktiivi (2006/24/EÜ), osutas kohus asjaolule, et direktiiv ei sätestanud selgesõnaliselt, et juurdepääs andmetele ja andmete hilisem kasutamine peaksid olema rangelt piiratud eesmärgiga ennetada ja avastada täpselt piiritletud raskeid kuritegusid või viia läbi nendega seotud menetlusi. Direktiiv sätestas vaid, et iga liikmesriik kehtestab menetluse ja tingimused, mida tuleb järgida. Kohtu hinnangul ei olnud seadusandja objektiivseid kriteeriumeid ning piiratud isikute ringi määratlenud, mis on aga taotletava eesmärgi seisukohast vajalik.[43]

Säilitamise piirangu osas on Euroopa Inimõiguste Kohus leidnud, et sõrmejälgede säilitamine andmebaasis 25 aastat seoses kõigi kuritegudega hoolimata nende raskusastmest, on ebaproportsionaalne sekkumine isiku eraellu ning seda ei saa käsitleda demokraatlikus ühiskonnas vajalikuna.[44] Samuti on kohus olnud seisukohal, et isikute, keda on kahtlustatud, kuid pole süüdi mõistetud, biomeetriliste andmete säilitamine piiramatu aja kestel ei ole põhjendatud, kuivõrd isiku ning avalikkuse huvid ei ole sellisel juhul tasakaalus.[45]

(c) Isikuandmete kaitsemeetmed

Euroopa Kohus on selgitanud, et isikuandmeid tuleb efektiivselt kaitsta kuritarvitamise ja ebaseadusliku juurdepääsu võimaldamise eest. Andmete hulka ja iseloomu tuleb arvesse võtta. Vajadus kaitsemeetmete järgi on suurem, kui isikuandmeid töödeldakse automaatselt ning on pidev risk, et andmetele on võimalik ligi pääseda volitamata isikutel. Sellisel juhul peavad olema selged ja ranged reeglid, mis tagavad konfidentsiaalsuse.[46] Euroopa Kohus on toonud välja, et riigisisene õigus peab põhinema objektiivsetel kriteeriumitel, mille põhjal määratletakse tingimused, mille alusel antakse ligipääs andmetele.[47]

[43] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd and Seitlinger and Others, 8 April 2014, p 61-62

[44] ECtHR M.K. v. France, No. 76100/13, 18.04.2013, p 45

[45] ECtHR, S. and Marper v. United Kingdom, Nos. 30562/04 and 30566/04, 4 December 2008, p 125

[46] CJEU, liidetud kohtuasjad C-293/12 ja C-594/12, Digital Rights Ireland Ltd ja Seitlinger jt, 08.04.2014, p 54

[47] CJEU, liidetud kohtuasjad C-203/15 ja C-698/15, Tele2 Sverige and Secretary of State for the Home Department, 21.12.2016, p 119

5. RIISTVARALISED JA TARKVARALISED ANDMEKAITSE- JA TURVANÕUDED BIOMEETRILISTE ANDMETE TÖÖTLEMISEKS

Turvameetmete rakendamine on osa isiku privaatsusõiguse tagamisest. Ühiskonnas elades peab iga isik arvestama, et paratamatult ühes või teises olukorras töödeldakse tema isikuandmeid (nii teiste isikute poolt kui ka enda riigi poolt). Demokraatlikus- ja liberaalses ühiskonnas on kodanikel seejuures eeldus, et tema isikuandmeid ei töödelda meelevaldselt ega suvaliselt, vaid tema privaatsust austatakse. Seega eeldab igasugune isikuandmete töötlemine teatud turvameetmete rakendamist. Sellised turvanõuded võivad olla ühiskonnas välja kujunenud sotsiaalse suhtlemise tulemusena (nt hoitakse teise isiku usaldatud saladusi) või need võivad olla ka ette nähtud seadusega (ametialane konfidentsiaalsuskohustus, organisatoorsed ja tehnilised turvameetmed).

Käesolevas peatükis keskendutakse õigusaktides toodud turvameetmetele, mille detailsusaste rahvusvahelistes ja EL-i õigusaktides on pigem üldine. Arvestades kohustatud isikute (riikide) erinevat tehnoloogiaalast arengutaset on hetkel veel võimatu ette kujutada olukorda, kus kõikidel riikidel oleks kohustus rakendada nt konkreetset ISO standardit. Sageli võivad ka riikides endis olla ajalooliselt välja kujunenud standardid, mis nende andmetöötluse tegevusi ja ulatust arvestades on kõige sobivamad (nt Eestis rakendatav infosüsteemide turvameetmete süsteem ISKE). Sellised siseriiklikult kehtestatud standardid peavad aga olema kooskõlas väliselt võetud kohustustega, mida olemegi käsitlenud allolevas analüüsis. Seejuures oleme vastavalt ülesande püstitusele analüüsinud nõudeid riistvarale ja tarkvarale (st välja on jäetud organisatoorsed nõuded), mida riik peaks järgima biomeetriliste andmete töötlemisel.

5.1. Rahvusvaheline õigus

Õigusakt	Säte	Sõnastus
EIÕK	Artikkel 8	1. Igaühel on õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning sõnumite saladust. 2. Ametivõimud ei sekku selle õiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks.
Konventsioon 108+	Artikkel 7	1. Iga osalisriik tagab, et vastutav töötleja, ja sobival juhul volitatud töötleja, rakendab asjakohaseid kaitsemeetmeid selliste riskide vastu nagu isikuandmete juhuslik või volitamata ligipääs, hävitamine, kaotamine, kasutamine, muutmine või avalikustamine. 2. Iga osalisriik tagab, et vastutav töötleja teavitab viivitamatult pädevat järelevalveasutust käesoleva Konventsiooni artikkel 15 tähenduses vähemalt nendest isikuandmete töötlemise rikkumistest, mis

		võivad kujutada tõsist ohtu andmesubjektide õigustele ja põhivabadustele.
Mittesiduva õiguse instrumendid		
OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data		

Kokkuvõte:

- Andmekaitse ja turvanõuded biomeetriliste andmete töötlemisele on rahvusvahelises õiguses määratud üksnes printsiipide tasemel, konkreetsed meetmed on jäetud riikide otsustada. Konkreetsed kohustuslikke standardeid riistvarale ja tarkvarale õigusaktide tasandil kehtestatud ei ole.
- Rahvusvahelise õiguse kontekstis on olulised ka mittesiduvad juhised, mis aitavad täpsustada ja mõista regulatsiooni konteksti või esitavad soovituslikke standardeid, mida eeskujuks võtta.
- Kohtupraktika kohaselt tuleb riigile selge kohustus tagada andmete töötlemise turvalisus ka rahvusvahelises õigusest (EIÕK).

5.1.1. Õigusaktid

Rahvusvahelises õiguses on turvanõuded tuletatavad rahvusvahelise õiguse õigusaktide üldprintsiipidest. Konkreetseid riistvaralisi või tarkvaralisi nõudeid ei ole kehtestatud ning selles osas on riikidel endal võimalik nõudeid täpsustada. Konventsioon 108+ kohaselt on biomeetriliste andmete töötlemine lubatud vaid siseriikliku õigusega tagatud asjakohase kaitse korral. Konventsiooni art 6(2) selgitab, et taolise kaitse eesmärk on hoida ära oht, mida tundliku teabe töötlemine võib andmesubjekti huvidele, õigustele ja põhivabadustele avaldada, eelkõige diskrimineerimise ohtu.

Konventsioon 108+ lisab osalisriigile kohustuse teavitada viivitamatult riiklikku andmekaitse inspektsiooni isikuandmetega seotud rikkumisest, mis võivad tõsiselt riivata andmesubjektide õigusi ja põhivabadusi. Konventsiooni seletuskiri täpsustab, et andmeturve tuleb tagada tehniliste ja korralduslike meetmetega, mis võtavad muuhulgas arvesse isikuandmete laadi ja mahtu ning võimalikke kahjulikke tagajärgi andmesubjektile. Andmeturbemeetmed peaksid arvestama andmetöötluse valdkonna kaasaegsete meetodite ja tehnikaga ning meetmete kulu peaks vastama võimalike riskide tõsidusele ja tõenäosusele. Eriliigiliste isikuandmete töötlemisel peaks seletuskirja kohaselt kahjulike tagajärgede ärahoidmiseks olema rakendatud asjakohased kaitsemeetmed, nt (koos või eraldi) andmesubjekti nõusolek, seadus, mis sätestab andmete töötlemise erialused, konfidentsiaalsuskohustus, riskianalüüsil tuvastatud meetmed, eelkõige kõrgendatud organisatoorsed või tehnilised meetodid (nt andmete krüpteerimine).[48]

Seega sätestab Konventsioon 108+ osalisriikidele isikuandmete kaitsele üldised suunised ja tingimused ilma konkreetseid riist- või tarkvaralisi nõudeid esitamata.

[48] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, lk 10-11, arvutivõrgus: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a

5.1.2. Mittesiduva õiguse instrumendid

OECD on võtnud vastu eraelu kaitse ning piiriüleste isikuandmevoogude juhendi[49], mis sätestab printsiipide tasemel üldised andmekaitse soovitused. Juhendi eesmärk on aidata kaasa rahvusvaheliste siduvate lepete sõlmimisele, sealhulgas Konventsiooni 108+ sõlmimisele.[50] Juhend ise pole õiguslikult siduv.[51] OECD suunised ei täpsusta turvameetmete nõudeid ega sea liikmesriikidele kohustusi järgida sätestatud andmekaitse printsiipide saavutamiseks konkreetseid standardeid või meetmeid. Ehkki juhendi fookus on piiriülesele andmevahetusel, on see hea näide sellest, millised on rahvusvaheliselt tunnustatud turvalisuse põhimõtted ja raamid.

Juhendi kohaselt peaksid riigid rakendama turvameetmeid, et kaitsta isiklikke andmeid selliste ohtude eest nagu andmete kadumine või volitamata juurdepääs, hävitamine, kasutamine, muutmine või andmete avalikustamine. Juhend käsitleb ka riiklikke rakendusmeetmeid ning soovitab riikidel juhendi täitmiseks muuhulgas töötada välja ühtne valitusasutuste andmekaitsestrateegia, võtta vastu siseriiklikud andmekaitseseadused ning asutada nõuete jõustamiseks andmekaitse inspektsioon. Lisaks soovitab juhend riikidel edendada tehniliste andmekaitse standardite kasutamist.

OECD on juhendi seletuskirjas viidanud andmeturbe rakendamises osas ISO, ETSI, ANSI ja CEN/ISSS organisatsioonidele, kelle väljastatud standardid peaksid abistama organisatsioone isikuandmete kaitse tugevdamises.[52] Riski hindamise ja analüüsi osas on OECD raport lähtunud ISO standardites kehtestatud metodoloogiast ning toonud välja ISO/IEC 27000 kui infosüsteemide turvalisust ja riskianalüüsi integreeriva standardi.[53] Konkreetsete andmekaitse ja turvameetmete rakendamine on jäetud aga osalisriikide endi otsustada.

5.1.3. Kohtupraktika

Organisatoorsete nõuete seisukohast on märkimisväärne Euroopa Inimõiguste Kohtu lahend 20511/03 *I v Soome*, mis tuletab riigi kohustused andmekaitse meetmete rakendamiseks EIÕK artiklist 8. Nimetatud asjas[54] on selgitanud riigil lasuvat kohustust piirata kõrvaliste isikute ligipääsu delikaatsetele isikuandmete.

Asjas oli hageja HIV-positiivne riikliku haigla töötaja, kes käis samas haiglas ravivastuvõttudel. Haigla töötajatel oli seejuures ligipääs kõigi patsientide raviandmetele ning andmesüsteem salvestas vaid viimase viie ravikonsultatsiooni logifailid koos juurdepääsu taotlenud raviosakonna infoga.[55] EIK leidis, et riigil lasub EIÕK art-st 8(1) tulenevalt positiivne kohustus

---

[49] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, arvutivõrgus: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[50] The OECD Privacy Framework, 2013, lk 33, arvutivõrgus: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[51] *Ibid*, lk 46.

[52] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, lk 113, arvutivõrgus: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[53] OECD, Managing Digital Security and Privacy Risk, lk 16 ja 18, arvutivõrgus: https://www.oecd-ilibrary.org/docserver/5jlwt49ccklt-en.pdf?expires=1542805200&id=id&accname=guest&checksum=20EFFDAA28188261B78DAA5F9E61E836

[54] EIK lahend nr 20511/03 *I v Soome,* arvutivõrgus: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-87510%22]}

[55] *Ibid*, p 7 ja 9.

kaitsta isikuandmeid andmekaitse eeskirjade ja kaitsemeetmete abil.[56] Kohus leidis, et vajalike kaitsemeetmete rakendamata jätmisega rikkus Soome EIÕK art 8 lg 1 sätestatud kohustust tagada isiku eraelu saladus.[57]

5.2. Euroopa Liidu õigusaktid

Õigusakt	Säte	Sõnastus
Isikuandmete kaitse üldmäärus	Artikkel 5 (1) (f)	1. Isikuandmete töötlemisel tagatakse, et f. isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid („usaldusväärsus ja konfidentsiaalsus“)
	Artikkel 32	1. Võttes arvesse teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning arvestades isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke, samuti erineva tõenäosuse ja suurusega ohte füüsiliste isikute õigustele ja vabadustele, rakendavad vastutav töötleja ja volitatud töötleja ohule vastava turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid, hõlmates muu hulgas vastavalt vajadusele järgmist: a. isikuandmete pseudonümiseerimine ja krüpteerimine; b. võime tagada isikuandmeid töötlevate süsteemide ja teenuste kestev konfidentsiaalsus, terviklus, kättesaadavus ja vastupidavus; c. võime taastada õigeaegselt isikuandmete kättesaadavus ja juurdepääs andmetele füüsilise või tehnilise vahejuhtumi korral; d. tehniliste ja korralduslike meetmete tõhususe korrapärase testimise ja hindamise kord isikuandmete töötlemise turvalisuse tagamiseks. 2. Vajaliku turvalisuse taseme hindamisel võetakse eelkõige arvesse isikuandmete töötlemisest tulenevaid ohte, eelkõige

[56] *Ibid*, p 37.

[57] *Ibid*, p 48.

		edastatavate, salvestatavate või muul viisil töödeldavate isikuandmete juhuslikku või ebaseaduslikku hävitamist, kaotsiminekut, muutmist ja loata avalikustamist või neile juurdepääsu. 3. Käesoleva artikli lõikes 1 osutatud nõuete järgimise tõendamise elemendina võib kasutada artiklis 40 osutatud heakskiidetud toimimisjuhendite või artiklis 42 osutatud heakskiidetud sertifitseerimismehhanismi järgimist. 4. Vastutav töötleja ja volitatud töötleja võtavad meetmeid selleks, et tagada, et vastutava töötleja või volitatud töötleja volituse alusel tegutsevad isikud, kellel on juurdepääs isikuandmetele, töötlevad isikuandmeid ainult vastutava töötleja juhiste alusel, välja arvatud juhul, kui liidu või liikmesriigi õigus neid selleks kohustab.
	Artikkel 35	1. Kui teatavat tüüpi isikuandmete töötlemise, eelkõige uut tehnoloogiat kasutava töötlemise tulemusena ning isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke arvesse võttes tekib tõenäoliselt füüsiliste isikute õigustele ja vabadustele suur oht, hindab vastutav töötleja enne isikuandmete töötlemist kavandatavate isikuandmete töötlemise toimingute mõju isikuandmete kaitsele. Endast sarnast suurt ohtu kujutavaid sarnaseid isikuandmete töötlemise toiminguid võib hinnata koos.
Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148, 6. juuli 2016, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus **(võrgu- ja infoturbe direktiiv, *NIS Direktiiv*)**	Artikkel 7 (1) 1.lause	1. Iga liikmesriik võtab vastu riikliku võrgu- ja infosüsteemide turvalisuse strateegia, milles määratletakse strateegilised eesmärgid ning asjakohased poliitilised ja regulatiivsed meetmed, mille abil saavutada võrgu- ja infosüsteemide turvalisuse kõrge tase ja seda säilitada, ning mis hõlmab vähemalt II lisas osutatud sektoreid ja III lisas osutatud teenuseid. [...]
Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude	Artikkel 4 (1) (f)	1. Liikmesriigid näevad ette järgmist: f. isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kadumise, hävimise või kahjustumise eest, kasutades

tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK **(õiguskaitseasutuste direktiiv)**		asjakohaseid tehnilisi või korralduslikke meetmeid.
	Artikkel 19 (1)	1. Liikmesriigid näevad ette, et vastutav töötleja rakendab isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke, samuti füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohte arvesse võttes asjakohaseid tehnilisi ja korralduslikke meetmeid tagamaks, et isikuandmeid töödeldakse kooskõlas käesoleva direktiiviga, ja olemaks võimeline seda ka tõendama. Vajaduse korral vaadatakse kõnealused meetmed läbi ja neid ajakohastatakse.
	Artikkel 20 (1)	1. Liikmesriigid näevad ette, et vastutav töötleja rakendab teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke, samuti isikuandmete töötlemisest tulenevaid füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohtusid arvesse võttes nii isikuandmete töötlemisvahendite kindlaksmääramisel kui ka isikuandmete töötlemise ajal asjakohaseid tehnilisi ja korralduslikke meetmeid, nagu pseudonüümiseerimine, mis on vajalikud andmekaitsepõhimõtete (nagu võimalikult väheste andmete kogumine) tõhusaks rakendamiseks ja vajalike kaitsemeetmete lõimimiseks isikuandmete töötlemisse, et täita käesoleva direktiivi nõudeid ja kaitsta andmesubjektide õigusi.
	Artikkel 29	1. Liikmesriigid näevad ette, et vastutav töötleja ja volitatud töötleja rakendavad teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke, samuti erineva tõenäosuse ja suurusega ohtusid füüsiliste isikute õigustele ja vabadustele arvesse võttes ohule vastava turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid, eelkõige seoses artiklis 10 osutatud isikuandmete eriliikide töötlemisega. 2. Liikmesriigid näevad ette, et vastutav töötleja ja volitatud töötleja rakendavad ohuhindamise alusel automatiseeritud andmetöötluse suhtes meetmeid, et: a. keelata volitamata isikute juurdepääs isikuandmete töötlemiseks

		kasutatavatele andmetöötlusseadmetele (töövahenditele juurdepääsu kontroll); b. hoida ära andmekandjate loata lugemine, kopeerimine, muutmine või kõrvaldamine (andmekandjate kontroll); c. hoida ära isikuandmete loata sisestamine ja säilitatavate isikuandmetega tutvumine, nende muutmine või kustutamine (säilitamise kontroll); d. hoida ära automatiseeritud andmetöötlussüsteemi andmesidevahendite abil kasutamine volitamata isikute poolt (kasutajate kontroll); e. tagada, et automatiseeritud andmetöötlussüsteemi kasutamise loaga isikutel oleks juurdepääs üksnes nendele isikuandmetele, mida hõlmab nende juurdepääsuluba (juurdepääsukontroll); f. tagada võimalus tõendada ja kindlaks määrata, millistele asutustele on isikuandmeid andmesidevahendite kaudu edastatud või kättesaadavaks tehtud või millistele asutustele võib neid edastada või kättesaadavaks teha (andmeedastuse kontroll); g. tagada võimalus hiljem tõendada ja kindlaks teha, milliseid isikuandmeid on automatiseeritud andmetöötlussüsteemi sisestatud ning millal ja kelle poolt need sisestati (sisestamise kontroll); h. hoida ära isikuandmete loata lugemine, kopeerimine, muutmine või kustutamine isikuandmete edastamise või andmekandjate vedamise ajal (transpordi kontroll); i. tagada, et paigaldatud süsteeme on võimalik katkestuse korral taastada (taastamine); j. tagada, et süsteem toimib, et selles ilmnevatest toimimisvigadest teatatakse (töökindlus) ja et süsteemirikked ei põhjustaks säilitatavate isikuandmete moonutamist (terviklus).
Mittesiduva õiguse instrumendid		
Euroopa Liidu Võrgu- ja Infoturbeameti (ENISA) juhised		

Kokkuvõte:

- Andmete turvalisuse tagamine on oluline nõue ning eeldus biomeetriliste andmete töötlemiseks.
- Andmekaitse ja turvanõuded biomeetriliste andmete töötlemisele on EL-i õiguses määratud üksnes üldiste meetmete tasemel, arvestades tehnoloogia neutraalsuse põhimõtet. Konkreetsed kohustuslikke standardeid riistvarale ja tarkvarale õigusaktide tasandil kehtestatud ei ole.
- Rakendatavate turvameetmete valikul peab vastutav töötleja rakendama riskipõhist lähenemist, hinnates töötlemisega kaasnevaid võimalikke ohte. Ohte tuleb hinnata andmesubjekti vaatenurgast.

(a) Isikuandmete kaitse üldmäärus

Isikuandmete kaitse üldmäärus kohustab isikuandmeid töötlema viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid.

Isikuandmete kaitse üldmäärus ei täpsusta asjakohaste tehniliste ja korralduslike meetmete tarkvaralisi või riistvaralisi nõudeid. Vajaliku turvalisuse taseme hindamisel võetakse eelkõige arvesse isikuandmete töötlemisest tulenevaid ohte, mis sisuliselt tähendab riskipõhist lähenemist turvameetmete valikule ja rakendamisele. Seejuures tuleb ohte hinnata andmesubjekti vaatenurgast. Üldnõuded tehnilistele ja korralduslikele meetmetele on toodud artiklis 32.

Tehniliste ja korralduslike meetmete nõuete järgimist võib tõendada riikliku järelevalveasutusse heakskiidetud toimimisjuhendi[58] või andmekaitsenõukogu, ekspertteadmistega sertifitseerimisasutuse või riikliku järelevalveasutuse heakskiidetud sertifitseerimismehhanismi alusel.[59] Euroopa Komisjonil on pädevus rakendusaktidega otsustada, et komisjonile esitatud heakskiidetud toimimisjuhend kehtib terves Euroopa Liidus.[60] Seni pole Euroopa Komisjon ühtegi toimimisjuhendeid heaks kiitnud.

Andmekaitse Inspektsioon on kinnitanud Isikuandmete töötleja üldjuhendi[61], mis sisaldab olulisemaid suuniseid kõigile sektoritele ega hõlma endas andmeturbe tehnilise lahenduse detailseid soovitusi. Juhend ei anna suuniseid biomeetriliste isikuandmete töötlemise osas, vaid selgitab üldiselt lõimitud andmekaitse põhimõtteid. Juhend lisab, et sõltuvalt andmete tundlikkusest ja ohtudest võib olla vajalik rakendada taolisi tehnilisi kaitsemeetmeid nagu

[58] Euroopa Andmekaitsenõukogu isikuandmete kaitse üldmäärus suunised, soovitused, parimad tavad on kättesaadav: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_et

[59] Isikuandmete kaitse üldmäärus art 40(1) ja (2), art 42(5).

[60] *Ibid*, art 40(9).

[61] Isikuandmete töötleja üldjuhend, Andmekaitse Inspektsioon, 2018, arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/2018.09.28%20andmet%C3%B6%C3%B6tleja%20%C3%BCldjuhend.pdf

kasutaja kaheastmeline tuvastus, TLS või VPN andmeedastus, andmete pseudonüümimine või krüptimine jne.[62]

Lisaks sätestab isikuandmete kaitse üldmäärus andmekaitsealase mõjuhinnangu koostamise kohustuse, kui isikuandmete töötlemise, eelkõige uut tehnoloogiat kasutava töötlemise tulemusena ning isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke arvesse võttes tekib tõenäoliselt füüsiliste isikute õigustele ja vabadustele suur oht. Mõjuhinnangu tegemine on nõutav füüsiliste isiklike aspektide süstemaatilise ja ulatusliku hindamise korral, mis põhineb automaatsel isikuandmete töötlemisel, sealhulgas profiilianalüüsil, ja millel põhinevad otsused, millel on füüsilise isiku jaoks õiguslikud tagajärjed või mis samaväärselt mõjutavad oluliselt füüsilist isikut. Kuivõrd biomeetriliste andmete tsentraliseeritud andmekogusse koondamine ning nende ristkasutus erinevates menetlustes võib hõlmata isiku jaoks õiguslikke tagajärgi, on taolise andmekogu loomisel mõjuanalüüsi koostamine kohustuslik. Seejuures peab mõjuhinnang hõlmama ka ohtude käsitlemiseks kavandatud turvameetmeid.

Isikuandmete töötlemise toimingute mõju hindamisel ning eelkõige andmekaitsealase mõjuhinnangu koostamisel on kohustus võtta asjakohaselt arvesse eelnimetatud heakskiidetud toimimisjuhendeid.[63] Euroopa Andmekaitsenõukogu on väljastanud automatiseeritud isikuandmete töötluse ja profiilianalüüsi suunised, mis selgitavad mõjuhinnangu koostamise kohustust, kuid ei täpsusta mõjuanalüüsist tulenevate turvameetmete nõudeid.[64] Andmekaitse Inspektsiooni üldjuhendi kohaselt on soovitatav ühitada isikuandmete kaitse alane riskianalüüs küberturvalisuse seaduses sätestatud riskianalüüsiga, kui viimane on seaduse kohaselt nõutav.[65] Võrgu-ja infoturbe direktiivist (vt järgmine alapeatükk (b)) lähtuvat riskianalüüsi kohustust on selgitatud analüüsi järgmises peatükis.

Seega ei sätesta isikuandmete kaitse üldmäärus biomeetriliste andmete töötlemisele spetsiifilisi andmekaitse- või turvanõudeid. Konkreetsed tarkvaralised ja riistvaralised andmekaitse ja turvanõuded on jäetud vastutava töötleja kehtestada, arvestades mõjuanalüüsi tulemusi ning andmebaasis isikuandmete töötlemisele tekkivat võimalikku ohtu.

(b) Võrgu- ja infoturbe direktiiv

Võrgu- ja infoturbe direktiiv (praktikas ka NIS-direktiiv) reguleerib meetmeid, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu EL-s. Direktiiv kohustab iga liikmesriiki võtma vastu riikliku võrgu- ja infosüsteemide turvalisuse strateegia, milles määratletakse strateegilised eesmärgid ning asjakohased poliitilised ja regulatiivsed meetmed, et saavutada võrgu- ja infosüsteemide turvalisuse kõrge tase ja seda säilitada.

Euroopa Komisjon on avaldanud teatise direktiivi tulemuslikumaks rakendamiseks ning seejuures selgitanud, et direktiiv ei täpsusta riikliku küberjulgeoleku strateegia, mis hõlmab infosüsteemide turvalisust ja strateegiat ning riskihindamiskava, nõudeid ega sisu.[66] Sellest tulenevalt on Euroopa Komisjon andnud teatises soovitusi riikliku võrgu- ja infosüsteemide

[62] *Ibid*, lk 11-12.

[63] Isikuandmete kaitse üldmäärus art 35(8).

[64] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, lk 29-30, arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

[65] Isikuandmete töötleja üldjuhend, Andmekaitse Inspektsioon, 2018, lk 26

[66] Komisjoni teatis Euroopa Parlamendile ja nõukogule Parimate tulemuste saavutamine võrgu- ja infoturbe direktiivi rakendamisel – jõupingutused direktiivi (EL) 2016/1148 (meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus) tulemuslikuks rakendamiseks COM/2017/0476 final

turvalisuse strateegia väljatöötamiseks, sealhulgas kaardistanud üldisel tasemel analüüsi erinevad etapid.[67]

Seega ei tulene direktiivist otseseid riist- ja tarkvaralisi nõudeid biomeetriliste andmete töötlemiseks, vaid soovitus rakendada rahvusvaheliselt heaks kiidetud standarditega kooskõlas olevaid nõudeid. Asjakohased nõuded tuleb liikmesriigil omakorda selgitada välja riskianalüüsi tulemusel.

(c) Õiguskaitseasutuste direktiiv

Õiguskaitseasutuste direktiiv näeb ette, et isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kadumise, hävimise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid. Direktiiv kohustab liikmesriike rakendama asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada isikuandmete töötlemise kooskõla direktiiviga. Meetmeid tuleb rakendada isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke, samuti füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohte arvesse võttes.

Lisaks sätestab direktiiv lõimitud andmekaitse ja vaikimise andmekaitse üldised nõuded, mille kohaselt peab liikmesriik tagama, et isikuandmete vastutav töötleja kohaldab andmekaitsepõhimõtete rakendamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid, võttes arvesse teaduse ja tehnoloogia arengut ja kulu, töötlemise laadi, ulatust, konteksti ja eesmärke, samuti isikuandmete töötlemisest tulenevaid füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohtusid. Direktiiv ei täpsusta aga asjakohaste tehniliste ja korralduslike meetmete konkreetseid nõudeid.

Vastavalt direktiivile on liikmesriigil kohustus rakendada ohule vastava turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid. Euroopa Komisjoni ettepanek direktiivi vastuvõtmise osas selgitab, et tehniliste ja korralduslike meetmete rakendamise osas tuleks järgida lõimitud andmekaitse põhimõtteid, kuid ei ava nimetatud tehniliste ja korralduslike meetmete täpsemat sisu.[68]

Õiguskaitseasutuste direktiiv kordab ka eelnevalt mainitud andmekaitse ja infosüsteemide turvalisuse tagamiseks vajalikku riskianalüüsi teostamise vajadust, mille alusel lasub liikmesriigil kohustus konkreetseid asjakohaseid meetmeid rakendada. Sõltumata riskianalüüsi tulemustest peavad liikmesriikide kohaldatavad meetmed täitma direktiivis loetelud eesmärkide tagamise. Konkreetsed andmekaitse riistvaralised ja tarkvaralised nõuded sõltuvad seega andmekogule kehtivatest ohtudest ja riskianalüüsi tulemustest.

5.2.2. Mittesiduva õiguse instrumendid

Muuhulgas reguleerib info- ja võrguturbe direktiiv digitaalsete teenuste osutajatele kehtestatud nõudeid, sätestades et liikmesriigid innustavad võrgu- ja infosüsteemide turvalisust käsitlevate Euroopa või rahvusvaheliselt heaks kiidetud standardite ja spetsifikatsioonide kasutamist.[69] Nimetatud standardite ja spetsifikatsioonide kasutamise osas annab suuniseid ja nõuandeid Euroopa Liidu Võrgu- ja Infoturbeamet (ENISA).[70]

---

[67] *Ibid*, p 2.3.

[68] European Commission proposal COM(2012) 10 final lk 19, arvutivõrgus: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF

[69] NIS-direktiiv art 19(1)

[70] *Ibid*, art 19(2)

Riikliku küberturvalisuse strateegia väljatöötamisel soovitab ENISA liikmesriikidel turvalisuse miinimumstandardite järgimiseks töötada järjepidevalt info- ja võrgusüsteemide turvalisuse nimel ning täiendada olemasolevaid tehnilisi standardeid. Muuhulgas toob ENISA välja standardid ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL ja BSI IT-Grundschutz.[71] Sealhulgas toob ENISA Saksamaa BSI IT Grundschutz (IT Baseline Protection Manual) ja ISO/IEC 27001 standardid välja ka riskianalüüsi metoodiliste alustena.[72]

[71] ENISA, NCSS Good Practice Guide Designing and Implementing National Cyber Securit Strategies, November 2016, arvutivõrgus: https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[72] ENISA, Inventory of Risk Management / Risk Assessment Methods, arvutivõrgus: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods

6. BIOMEETRILISTE ANDMETE KASUTAMINE AVALIK-ÕIGUSLIKES MENETLUSTES

Käesolevas peatükis keskendume spetsiifilistele avalik-õiguslikele menetlustele, mille käigus riik biomeetrilisi andmeid töötleb. Seejuures ei korrata enam üldisi nõudeid biomeetriliste andmete töötlemisele, mida on käsitletud eelnevalt (nt Konventsioon 108+, EIÕK, Euroopa Liidu põhiõiguste harta, vt peatükk 3.1).

Käesoleva peatüki fookus on järgnevatel menetlustel: dokumendimenetlused (passi ja reisidokumentide menetlus, EL-i kodanike isikutunnistuste ja kodanike pereliikmete elamislubade menetlus, Schengeni elamisloa menetlus), millest on eraldatud viisamenetlus, piiriületusega seotud menetlused, varjupaiga ja rahvusvahelise kaitse menetlus, illegaalimenetlus ja süütegudega seotud menetlused. Need menetlusliigid on valitud vastavalt tellija suunistele (kui peamised menetlused, millega tellija kokku puutub või mis on tellija haldusalas).

Käesoleva peatüki eesmärkideks on: a) kaardistada asjakohased avalik-õiguslikud menetlused; b) selgitada välja biomeetriliste andmete töötlemise õiguslik alus nendes menetlustes; ning c) välja tuua tingimused biomeetriliste andmete töötlemisele, mis on spetsiifilisemad üldistest tingimustest.

Peatüki ülesehitus erineb eelnevatest, sest alajaotused on toodud konkreetsete menetluste kaupa. Eraldi ei ole välja toodud rahvusvahelise õiguse regulatsiooni, sest konkreetseid menetlusliike rahvusvaheline õigus ei reguleeri ning õiguslik raamistik tuleneb Eesti jaoks peamiselt Euroopa Liidu õigusaktidest. Siiski tuleb silmas pidada, et rahvusvahelisest õigusest tulenevad riigile kohustused, millega peab arvestama ka erinevaid menetlusi õiguslikult reguleerides (vt ptk 3.1) ning samuti võib olla rahvusvahelise õiguse õigusallikatele viidatud konkreetseid menetlusi reguleerivates Euroopa Liidu õigusaktides[73].

6.1. Dokumendimenetlused

6.1.1. Passi ja reisidokumentide menetlus

Õigusakt	Säte	Sõnastus
Euroopa Parlamendi ja Nõukogu määrus (EÜ) nr 444/2009, 28. mai 2009, millega muudetakse nõukogu määrust (EÜ) nr 2252/2004 liikmesriikide väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta	Põhjenduspunkt 5	Määrusega (EÜ) nr 2252/2004 nähakse ette, et biomeetrilisi andmeid kogutakse ja need salvestatakse passide ja reisidokumentide andmekandjale nende dokumentide väljastamise eesmärgil. See ei piira nimetatud andmete liikmesriigi siseriikliku õiguse kohast mis tahes muud kasutamist või salvestamist. Määrusega (EÜ) nr 2252/2004 ei nähta ette õiguslikku alust nende andmete salvestamiseks mõeldud andmebaaside loomiseks või pidamiseks liikmesriikides. Seda reguleerib rangelt siseriiklik õigus.

[73] Euroopa Parlamendi ja Nõukogu määrus (EÜ) nr 444/2009, 28. mai 2009, millega muudetakse nõukogu määrust (EÜ) nr 2252/2004 liikmesriikide väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta, artikkel 1a (2)

	Artikkel 1	1. Liikmesriikides väljastatavad passid ja reisidokumendid vastavad määruse lisas sätestatud minimaalsetele turvastandarditele. [...] 2. Passidele ja reisidokumentidele lisatakse äärmiselt turvaline andmekandja, mis sisaldab näokujutist. Liikmesriigid lisavad samuti koostalitlusvõimelistes vormingutes otsevajutusega võetud kaks sõrmejälge. Andmed on turvatud ja andmekandja on piisava salvestusmahu ja -võimega, et tagada andmete terviklikkus, autentsus ja konfidentsiaalsus.
	Artikkel 1a (2)	2. Liikmesriigid koguvad taotlejalt biomeetrilisi tunnuseid kooskõlas Euroopa Nõukogu inimõiguste ja põhivabaduste kaitse konventsioonis ning ÜRO lapse õiguste konventsioonis sätestatud tagatistega. Liikmesriigid tagavad, et juhuks, kui andmete registreerimisega on raskusi, on olemas sobivad menetlused, mis tagavad asjaomase isiku inimväärikuse.
	Artikkel 4 (3)	3. Biomeetrilisi andmeid kogutakse ja salvestatakse passide ja reisidokumentide andmekandjale nende dokumentide väljastamise eesmärgil. Käesoleva määruse kohaldamisel kasutatakse biomeetrilisi tunnuseid passides ja reisidokumentides üksnes järgmise kontrollimiseks: a. passi või reisidokumendi ehtsus; b. kasutaja isikusamasus otseselt kättesaadavate võrreldavate tunnuste abil, kui passi või reisidokumendi esitamine on seadusega nõutav.

Kokkuvõte:

- Õiguslik alus biomeetriliste andmete (näokujutis ja kaks otsevajutusega sõrmejälge) kogumisele tuleneb määrusest 2252/2004 ja seda muutvast määrusest 444/2009. Kogumise eesmärk on biomeetriliste andmete töötlemine passi ja reisidokumentide menetluses. Nimetatud biomeetriliste andmete kogumine sellel eesmärgil on riigile kohustuslik.
- Dokumentide väljastamiseks kogutud andmete mis tahes muud kasutamist või salvestamist siseriikliku õiguse alusel määrus ei keela, kuid ei anna selleks ka õiguslikku alust. Seega võib riigi enda poolt kogutud andmeid muul eesmärgil töödelda, kui selleks on olemas muul (siseriiklikul) õigusaktil põhinev õiguslik alus.

- Dokumendis olevaid biomeetrilisi andmeid (s.t. teiste riikide poolt kogutud andmeid) võib kasutada vaid dokumendi ehtsuse kontrollimiseks ja kasutaja isikusamasuse kontrollimiseks.

Euroopa Liidu liikmesriigid on kohustatud isikute näokujutist ja sõrmejälgi töötlema passide ja reisidokumentide väljastamisel. Käesoleva analüüsi raames on olulised eelkõige määruse 444/2009 sätted. Passid ja reisidokumendid peavad vastama määruses toodud minimaalsele turvastandardile. Vastavalt määrusele on sõrmejälgede andmise kohustusest vabastatud alla 12-aastased lapsed ja isikud, kellelt on füüsiliselt võimatu sõrmejälgi võtta.

Antud menetluse raames on oluline eristada dokumenti väljastavat riiki ja dokumendi põhjal kontrolli teostavat riiki. Dokumenti väljastaval riigil, kes kogub vastavaid biomeetrilisi andmeid, on määrusest tulenevalt volitus andmeid muul viisil koguda või salvestada, kui selleks on siseriiklikult kehtestatud õiguslik alus. Kui riik kasutab dokumendis olevaid andmeid (nt tegemaks isikusamasuse kontrolli), siis ei ole määruses sätestatud volitust selliste andmete kasutamiseks muul viisil või eesmärgil. Teisisõnu, kodanikule passi väljastades võib riik siseriikliku õigusega sätestada aluse, mille kohaselt riik salvestab neid andmeid nt siseriiklus dokumendiregistris väljastatud dokumentide üle arvestuse pidamiseks, kuid samas ei või riik isiku dokumenti kontrollides saadud andmeid teisel eesmärgil koguda.

Seega on dokumenti väljastaval riigil võimalik kehtestada siseriiklik õiguslik alus dokumendi väljastamise menetluses kogutud biomeetriliste andmete kasutamiseks muul eesmärgil (s.h. siseriiklikes andmebaasides), kuid dokumendis olevate ja seega teiste riikide poolt kogutud biomeetriliste andmete kasutamine on lubatud vaid dokumendi ehtsuse ja kasutaja isikusamasuse kontrollimiseks.

(a) Õiguslik alus

Passi ja reisidokumentide menetluses toimub biomeetriliste andmete töötlemine määruse 2252/2004 alusel, seega on biomeetriliste andmete töötlemise aluseks üldmääruse art-i 9(2)(g) mõttes EL-i õigus. Isikuandmete kaitse biomeetriliste andmete töötlemisel tuleb tagada vastavalt isikuandmete kaitse üldmäärusele.[74]

Biomeetrilisi andmeid võib koguda ja salvestada passide ja reisidokumentide väljastamise eesmärgil, kuid biomeetrilisi andmeid võib kasutada üksnes passi või dokumendi ehtsuse kontrollimiseks või kasutaja isikusamasuse kontrollimiseks otseselt kättesaadavate võrreldavate tunnuste abil, kui passi või muu reisidokumendi esitamine on seadusega nõutav.

On oluline märkida, et määrus ei piira nimetatud andmete liikmesriigi siseriikliku õiguse kohast mis tahes muud kasutamist või salvestamist. Määrusega ei nähta ette õiguslikku alust nende andmete salvestamiseks mõeldud andmebaaside loomiseks või pidamiseks liikmesriikides, seda reguleerib rangelt siseriiklik õigus.[75] See sisuliselt tähendab, et passi või reisidokumentide väljastamiseks kogutud isikuandmete töötlemine on võimalik muul eesmärgil kui dokumentide väljastamine, kui selleks on nt siseriiklikult kehtestatud õiguslik alus[76].

(b) Tingimused

Eelnevast tulenevalt on passi ja reisidokumentide menetluses riik kohustatud töötlema näokujutist ning kahte otsevajutusega sõrmejälge koostalitusvõimelises vormingus. Tegemist

[74] Määrus 2252/2004 pp 8 ja isikuandmete kaitse üldmäärus art 94

[75] Euroopa Nõukogu ja Parlamendi määrus 444/2009, mis muudab määrust 2252/2004 pp 5

[76] Vt ka Euroopa Euroopa Kohtu lahend C-446/12-C-449/12, täpsemalt raporti ptk 7.1.2(c)

on minimaalsete andmetega ning seega ei ole välistatud ka täiendavate andmete kogumine kui selleks on määrust täiendav õiguslik alus. Küll aga ütleb määruse põhjenduspunkt 8 selgelt, et passi ei tohiks kanda muud teavet kui see, mis on sätestatud määruses, selle lisas või mis on nimetatud asjaomases reisidokumendis. Seega ei saa täiendavaid andmeid koguda põhjendades seda vajadusega lisada passi täiendavaid andmeid. Lisaks määruses toodud tehnilistele nõuetele tuleb turvalisuse tagamisel järgida ka isikuandmete kaitse üldmäärusest tulenevaid nõudeid (vt peatükk 5.2).

6.1.2. EL-i kodanike isikutunnistuste ja kodanike pereliikmete elamislubade menetlus (ettepanek)

Õigusakt	Säte	Sõnastus
Ettepanek: ***Euroopa Parlamendi ja Nõukogu määrus*** ***liidu kodanike isikutunnistuste ning vaba liikumise õigust kasutavatele liidu kodanikele ja nende pereliikmetele väljaantavate elamislubade turvalisuse suurendamise kohta***	Põhjenduspunkt 9	Turvaelemendid on vajalikud selleks, et kontrollida dokumendi ehtsust ja kindlaks teha isikusamasus. Minimaalsete turvastandardite kehtestamine ning biomeetriliste andmete lisamine isikutunnistustele ja selliste pereliikmete elamisloakaartidele, kes ei ole liikmesriigi kodanikud, on tähtis samm, et muuta nende dokumentide kasutamine liidus turvalisemaks. Selliste biomeetriliste tunnuste lisamine peaks andma kodanikele võimaluse kasutada täiel määral oma vaba liikumise õigust.
	Põhjenduspunkt 18	Käesoleva määruse kohaldamise raames töödeldavate isikuandmete suhtes kohaldatakse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrust (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). Töödeldavate isikuandmete suhtes kohaldatavaid kaitsemeetmeid tuleb veel täpsustada. Andmesubjektid peaksid olema täiesti teadlikud sellest, et nende dokumendis on andmekandja, mis sisaldab nende biomeetrilisi andmeid, sealhulgas kontaktivabast juurdepääsust neile, samuti kõikidest juhtudest, kus nende isikutunnistusel ja elamisloal sisalduvaid andmeid kasutatakse. Igal juhul peaks andmesubjektidel olema juurdepääs oma isikutunnistuses ja elamisloas töödeldud isikuandmetele ning õigus lasta neid andmeid parandada.
	Põhjenduspunkt 19	Käesolevas määruses on vaja kindlaks määrata isikutunnistuse ja elamisloa andmekandjale andmete kogumise ja salvestamise alus. Liikmesriigid võivad kooskõlas riigisiseste õigusaktide või liidu õigusega salvestada andmekandjale e-teenuste jaoks või muudel

		isikutunnistuse või elamisloaga seotud eesmärkidel muid andmeid. Selliste andmete töötlemine, sealhulgas nende kogumine, ja eesmärgid, milleks neid kasutatakse, peavad olema liikmesriigi või liidu õiguse alusel lubatud. Kõik riigisisesed andmed peavad olema käesolevas määruses osutatud biomeetrilistest andmetest füüsiliselt või loogiliselt eraldatud.
	Artikkel 3 (3)	3. Isikutunnistused hõlmavad üliturvalist andmekandjat, mis sisaldab isikutunnistuse omaniku näokujutist ja kahte sõrmejälge koostalitlusvõimelises vormingus.
	Artikkel 10 (3)	3. Kogutud ja isikutunnistuse või elamisloa andmekandjale salvestatud biomeetrilisi andmeid kasutatakse kooskõlas liidu ja liikmesriigi õigusega üksnes selleks, et kontrollida a. isikutunnistuse või elamisloa ehtsust; b. kasutaja isikusamasust otseselt kättesaadavate võrreldavate tunnuste abil, kui isikutunnistuse või elamisloa esitamine on õigusaktidega nõutav.

Hetkel on menetluses eelnõu Euroopa Parlamendi ja nõukogu määruse vastuvõtmiseks, mis reguleeriks EL-i kodanike isikutunnistuste (nt ID-kaart) ning vaba liikumise õigust kasutavatele liidu kodanikele ja nende pereliikmetele väljaantavate elamislubade turvalisuse suurendamise kohta[77]. Oma olemuselt on selle põhimõtted sarnased passi ja reisidokumendi väljastamise menetlusega.

(a) Õiguslik alus

Vaatlusaluse eelnõuga sätestatakse biomeetriliste andmete kohustuslik lisamine EL-i kodanike isikutunnistustele ja liidu kodanike kolmandate riikide kodanikest pereliikmete elamislubadele. Need on dokumendid, mille väljaandmine ei pruugi igas liikmesriigis olla kohustuslik, kuid kui on antud välja isikutunnistus, mis on antud määruse kohaldamisalas[78], siis tuleks nende isikutunnistuste edasisel väljastamisel rakendada määruse ettepanekus toodud kõrgemaid turvalisuse standardeid, mh lisada nimetatud biomeetrilised andmed. Sarnaselt passide ja reisidokumentidega on nendes dokumentides andmekandja (kiip), mis sisaldaks dokumendi omaniku biomeetrilisi andmeid (omaniku näokujutis ja kaks sõrmejälge koostalitusvõimelises vormingus).

(b) Tingimused

Kogutud ja andmekandjale salvestatud biomeetrilisi andmeid kasutatakse kooskõlas liidu ja liikmesriigi õigusega üksnes selleks, et: a) kontrollida isikutunnistuse või elamisloa ehtsust; või

[77] COM(2018) 212 final - 2018/0104 (COD)

[78] *Ibid*, art 2

b) kontrollida kasutaja isikusamasust otseselt kättesaadavate võrreldavate tunniste abil, kui isikutunnistuse või elamisloa esitamine on õigusaktidega nõutav[79].

Seoses biomeetriliste andmete kohustusliku lisamisega EL-i kodanike isikutunnistustele ja liidu kodanike kolmandate riikide kodanikest pereliikmete elamislubadele kohaldatakse konkreetseid kaitsemeetmeid, mis vastavad kaitsemeetmetele, mis on kehtestatud passide ja muude reisidokumentide ning elamislubade jaoks.

6.1.3. Schengeni elamisloa menetlus

Õigusakt	Säte	Sõnastus
Nõukogu määrus (EÜ) nr 1030/2002, 13. juuni 2002, millega kehtestatakse ühtne elamisloavorm kolmandate riikide kodanike jaoks	Põhjenduspunkt 9	Liikmesriigid peaksid komisjoniga kooskõlastades rakendama vajalikke meetmeid tagamaks, et isikuandmete töötlemisel järgitaks Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivis 95/46/EÜ (üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta) sätestatud nõudeid nimetatud andmete kaitse kohta.
Nõukogu määrus (EÜ) nr 380/2008, 18. aprill 2008, millega muudetakse määrust (EÜ) nr 1030/2002, millega kehtestatakse ühtne elamisloavorm kolmandate riikide kodanike jaoks	Artikkel 1 (4)	Käesoleva määruse kohaldamisel kasutatakse elamislubadele kantud biomeetrilisi tunnuseid üksnes järgmistel eesmärkidel: c. dokumendi ehtsuse kontrollimiseks; d. kasutaja isikusamasuse kontrollimiseks otseselt kättesaadavate võrreldavate tunnuste abil, kui elamisloa esitamine on nõutav siseriiklike õigusaktide kohaselt.
	Artikkel 5a	Kui liikmesriigid kasutavad ühtset vormi muudel kui käesolevas määruses sätestatud eesmärkidel, tuleb võtta asjakohased meetmed tagamaks, et seda ei oleks võimalik segamini ajada artiklis 1 nimetatud elamisloaga ning eesmärk oleks kaardil selgelt märgitud.

Kokkuvõte:

- Õiguslik alus biomeetriliste andmete töötlemiseks Schengeni elamisloa menetluses tuleneb EL-i õigusaktidest.
- Vastavate biomeetriliste andmete töötlemine on riigile kohustuslik.
- Kogutud andmete mis tahes muud kasutamist määrus ei keela, kuid ei anna selleks ka õiguslikku alust. Seega võib liikmesriik enda kogutud andmeid muul eesmärgil töödelda, kui selleks on olemas mõnel muul (siseriiklikul) õigusaktil põhinev kehtiv õiguslik alus.

[79] *Ibid*, art 10(3)

- Elamislubadesse kantud biomeetrilisi andmeid (s.t. andmed, mis on kogutud neid väljaandnud riigi poolt) võib siiski töödelda üksnes määruses nimetatud eesmärgil ehk dokumendi ehtsuse ja kasutaja isikusamasuse kontrollimiseks. Muudel eesmärkidel on selliste biomeetriliste andmete töötlemine keelatud.

(a) Õiguslik alus

Schengeni viisaruumi elamisloa taotluste puhul on tegemist olukorraga, kus liikmesriigid on kohustatud isikuandmeid töötlema.[80] Liikmesriigid võtavad kolmandate riikide kodanikelt ja kodakondsuseta isikutelt biomeetrilised tunnused (näokujutis ja kaks sõrmejäljekujutist) dokumendi väljastamise eesmärgil.

(b) Tingimused

Järgida tuleb ka liikmesriigi tava, Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis ja ÜRO lapse õiguste konventsioonis sätestatud kaitsemeetmeid. Sõrmejäljekujutise võtmine on kohustuslik alates 6. eluaastast. Sõrmejälgede andmisest on vabastatud isikud, kellelt on füüsiliselt võimatu sõrmejälgi võtta.[81] Lisaks kehtivad isikuandmete töötlemise üldised tingimused, mis tulenevad isikuandmete kaitse üldmäärusest.[82]

6.2. Viisamenetlus

Õigusakt	Säte	Sõnastus
Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 810/2009, 13. juuli 2009, millega kehtestatakse ühenduse viisaeeskiri (viisaeeskiri)	Põhjenduspunkt 12	Käesoleva määruse kohasel isikuandmete töötlemisel kohaldavad liikmesriigid Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivi 95/46/EÜ (üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta)[83]
	Artikkel 13 (1)	Liikmesriigid koguvad andmeid taotleja biomeetriliste tunnuste kohta, mille hulka kuuluvad tema foto ja kümme sõrmejälge, kooskõlas Euroopa Nõukogu inimõiguste ja põhivabaduste kaitse konventsioonis, Euroopa Liidu põhiõiguste hartas ja ÜRO lapse õiguste konventsioonis sätestatud kaitsemeetmetega.
Euroopa Parlamendi ja Nõukogu määrus (EÜ) nr 767/2008, 9. juuli 2008, mis käsitleb viisainfosüsteemi (VIS) ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta	Artikkel 9 (5)	Viisasid väljastav asutus sisestab taotlustoimikusse järgmised andmed: 5. taotleja sõrmejäljed vastavalt ühiste konsulaarjuhiste asjakohastele sätetele.

[80] Sellele viitab määruse 1030/2002 art 1 lg 1 – „liikmesriigid peavad järgima ühtset vormi“

[81] Määruse 1030/2002 art 4b, mis on kehtestatud määrusega 380/2008

[82] Määruse 1030/2002 pp 9; isikuandmete kaitse üldmääruse art 94

[83] Vastavalt isikuandmete kaitse üldmääruse art-le 94 koheldakse viiteid direktiivile 95/46/EÜ viidetena isikuandmete kaitse üldmäärusele.

(VIS määrus)		
Nõukogu otsus 2008/633/JSK, 23. juuni 2008, mis käsitleb liikmesriikide määratud ametiasutuste ja Europoli juurdepääsu viisainfosüsteemile (VIS) terroriaktide ja muude raskete kuritegude vältimise, avastamise ja uurimise eesmärkidel	Artikkel 1	Käesolevas otsuses sätestatakse tingimused, mille kohaselt liikmesriikide määratud ametiasutused ja Euroopa Politseiamet (Europol) võivad saada juurdepääsu viisainfosüsteemi (VIS) andmetega tutvumiseks terroriaktide ja muude raskete kuritegude vältimise, avastamise ja uurimise eesmärkidel.
	Artikkel 8 (3)	Käesoleva otsuse kohaselt VISist saadud isikuandmeid töödeldakse üksnes terroriaktide või muude raskete kuritegude vältimise, avastamise, uurimise ja nende eest vastutusele võtmise eesmärgil.
Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 390/2009, 23. aprill 2009, millega muudetakse viisasid käsitlevaid ühiseid konsulaarjuhiseid diplomaatilistele ja konsulaaresindustele seoses biomeetria kasutuselevõtmisega ning viisataotluste vastuvõtmise ja menetlemise korraldamise sätete lisamisega	Artikkel 1 (1.2)	Esimese taotluse esitamiseks palutakse taotlejatel isiklikult kohale ilmuda. Taotluse esitamisel kogutakse andmed järgmiste biomeetriliste tunnuste kohta: — foto, mis skaneeritakse või tehakse taotluse esitamise ajal, ning — kümme sõrmejälge, mis kogutakse otsevajutusega ja registreeritakse digitaalselt.
Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1987/2006, 20. detsember 2006, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist **(SIS II määrus)**	Artikkel 27 (3)	Peale selle võivad vastavalt SIS II-te sisestatud andmetele ja kooskõlas otsuse 2006/000/JSK artikli 38 lõike 2 punktidega d ja e sisestatud ning isikutega seotud dokumente käsitlevatele andmetele juurdepääsu õigust ja nende andmete vahetu otsimise õigust kasutada viisade andmise eest vastutavad asutused, viisataotluste läbivaatamise eest vastutavad keskasutused ja asutused, kes vastutavad elamislubade andmise ja kolmandate riikide kodanikke käsitlevate õigusnormide kohaldamise eest seoses isikute liikumise alaste ühenduse õigusaktide kohaldamisega. Nende asutuste juurdepääsu andmetele reguleerib liikmesriigi õigus.
Euroopa Parlamendi ja nõukogu määrus (EL) 2017/2226, 30. november 2017, millega luuakse riiki sisenemise ja riigist lahkumise süsteem liikmesriikide välispiire ületavate kolmandate riikide kodanike riiki sisenemise ja riigist	Artikkel 24 (1) ja 24 (3)	1. Viisasid väljastavad asutused teevad riiki sisenemise ja riigist lahkumise süsteemis päringuid viisataotluste läbivaatamiseks ja nende kohta otsuste vastuvõtmiseks, sealhulgas viisa kehtetuks tunnistamise, tühistamise või kehtivusaja pikendamise otsuste vastuvõtmiseks kooskõlas määrusega (EÜ) nr 810/2009.

lahkumise andmete ja sisenemiskeeluandmete registreerimiseks ning määratakse kindlaks riiki sisenemise ja riigist lahkumise süsteemile õiguskaitse eesmärgil juurdepääsu andmise tingimused ning millega muudetakse Schengeni lepingu rakendamise konventsiooni ning määruseid (EÜ) nr 767/2008 ja (EL) nr 1077/2011 **(EES määrus)**		3. Kui lõikes 2 sätestatud andmete alusel tehtud otsingust selgub, et kolmanda riigi kodaniku andmed on riiki sisenemise ja riigist lahkumise süsteemis registreeritud, antakse viisasid väljastavatele asutustele juurdepääs päringu tegemiseks selle kolmanda riigi kodaniku isiklikus toimikus ning samuti nimetatud isikliku toimikuga seotud riiki sisenemise ja riigist lahkumise andmestikus ning sisenemiskeeluandmestikus. Viisasid väljastavatele asutustele antakse juurdepääs automaatkalkulaatorile, et kontrollida maksimaalset järelejäänud lubatud viibimisaega. Samuti saavad viisasid väljastavad asutused uute viisataotluste läbivaatamisel ja nende kohta otsuste vastuvõtmisel teha riiki sisenemise ja riigist lahkumise süsteemis ja automaatkalkulaatoris päringuid, et teha automaatselt kindlaks maksimaalne lubatud viibimisaeg.

Kokkuvõte:

- Õiguslik alus biomeetriliste andmete (foto ja kümme otsevajutusega sõrmejälge) töötlemiseks viisamenetluses tuleneb EL-i viisaeeskirjast ja sellega seotud õigusaktidest.
- Nimetatud biomeetriliste andmete töötlemine on riigile kohustuslik.
- Riigi poolt kogutud ja VIS-i saadetud andmeid võib säilitada siseriiklikes andmekogudes ning neid andmeid töödelda muul eesmärgil kui selleks on kehtiv õiguslik alus.
- VIS-ist saadud andmeid võib siseriiklikes andmekogudes säilitada vaid juhul, kui see on üksikjuhtumil vajalik ning see on kooskõlas VIS-i eesmärgi ja asjakohaste seadusesätetega.
- Viisasid menetlevad asutused omavad juurdepääsu ka teistele EL-i kesksetele andmebaasidele viisamenetluse käigus. Konkreetsed õiguslikud alused ning piirangud andmete töötlemisel on toodud vastavat infosüsteemi reguleerivas õigusaktis.

(a) Õiguslik alus

Viisade menetlemist reguleerivad EL-i määrused, mille kohaselt on biomeetriliste andmete (foto ja kümme otsevajutusega sõrmejälge) töötlemine viisataotluste menetlemise raames liikmesriikide jaoks kohustuslik. Seega erinevalt dokumendimenetlusest kogutakse viisamenetluses taotlejalt kõik 10 sõrmejälge. Viisaeeskirja kohaldatakse kolmandate riikide

kodanike suhtes, kellel peab ühenduse välispiiride ületamiseks olema viisa või transiitviisa[84]. Viisamenetluse käigus kogutud andmed sisestatakse EL-i ühtsesse viisainfosüsteemi VIS (vt täpsemalt peatükk 7.2(a)). Lisaks võib viisataotlusi väljastaval asutusel olla juurdepääs teistele EL-i andmebaasidele päringute tegemiseks, mis võimaldavad neil viisa taotleja kohta andmeid koguda. Näiteks on selline juurdepääs võimalik nii SIS II süsteemile kui ka EES süsteemile.

(b) Tingimused

VIS süsteemis säilitatakse andmeid 5 aastat. Seejuures peab iga liikmesriik ja korraldusasutus registreerima kõik VIS-is tehtavad andmetöötlustoimingud. Selliseid kirjeid võib kasutada ainult andmekaitsega seotud andmetöötluse lubatavuse järelevalve eesmärgil ja andmekaitse tagamiseks.[85] VIS määruse kohaselt on keelatud siseriiklikes toimikutes VIS-st saadud andmeid hoida, välja arvatud kui see on üksikjuhtumil vajalik, see on kooskõlas VIS-i eesmärgi ja asjakohaste seadusesätetega (sh andmekaitset reguleerivate sätetega) ning andmeid hoitakse vaid nii kaua, kui on üksikjuhtumil vajalik.[86] Seega on VIS-st saadud andmete töötlemine siseriiklikes andmekogudes lubatud vaid erandlikel juhtudel konkreetse üksikjuhtumi tarbeks. Küll aga ei ole riigil keelatud hoida oma siseriiklikes toimikutes andmeid, mida vastav riik on ise VIS-i sisestanud. Seega Eesti enda poolt VIS-i saadetud andmeid on lubatud siseriiklikus andmekogus salvestada.

Sõrmejälgede andmise nõudest on vabastatud alla 12-aastased lapsed, isikud, kellelt on füüsiliselt võimatu sõrmejälgi võtta ning riigipead või valitsusjuhid ning valitsuse liikmed ja nendega koos reisivad abikaasad ja nende ametliku delegatsiooni liikmed, kui nad on saanud ametliku küllakutse liikmesriikide valitsustelt või rahvusvahelistelt organisatsioonidelt, samuti monarhid ja kuningliku perekonna teised kõrged liikmed, kui nad on saanud ametliku küllakutse liikmesriikide valitsustelt või rahvusvahelistelt organisatsioonidelt.[87] Lisaks määruses toodud tehnilistele nõuetele tuleb turvalisuse tagamisel järgida ka isikuandmete kaitse üldmäärusest tulenevaid nõudeid (vt peatükk 5.2).

6.3. Piiriületusega seotud menetlused

Õigusakt	Säte	Sõnastus
Euroopa Parlamendi ja nõukogu määrus (EL) 2016/399, 9. märts 2016, mis käsitleb isikute üle piiri liikumist reguleerivaid liidu eeskirju **(Schengeni piirieeskirjad)**	Põhjenduspunkt 10	Ainult sõrmejälgede kontrolli põhjal saab olla kindel, et Schengeni alale siseneda sooviv isik on see isik, kellele viisa on välja antud, seetõttu tuleks kehtestada Euroopa Parlamendi ja nõukogu määruses (EÜ) nr 767/2008 ette nähtud viisainfosüsteemi (VIS) kasutamine välispiiridel.
	Põhjenduspunkt 14	VISi kasutamine peaks hõlmama süstemaatilist otsingute tegemist VISist viisakleebise numbri alusel koos sõrmejälgede kontrolliga. [...]
	Artikkel 6 (1) (d)	1. Kuni 90-päevaseks kavandatud viibimiseks liikmesriikide territooriumil mis tahes 180-

[84] Viisaeeskiri art 1(2) ja 1(3)

[85] VIS määrus art 34

[86] *Ibid*, art 30 (1)

[87] Määrus 810/2009 art 13 lg 7

		päevase ajavahemiku jooksul, mis tähendab igale viibimispäevale eelneva 180-päevase ajavahemiku arvestamist, kehtivad kolmandate riikide kodanikele järgmised territooriumile sisenemise tingimused: d. nende kohta ei ole Schengeni infosüsteemi (SIS) kantud hoiatust sisenemise keelamise eesmärgil
	Artikkel 8 (3) (b)	3. Kolmandate riikide kodanikel tuleb riiki sisenemisel ja riigist lahkumisel läbida järgnev põhjalik kontroll: b. kui kolmanda riigi kodanikul on artikli 6 lõike 1 punkti b kohane viisa, hõlmab põhjalik kontroll riiki sisenemisel ka viisaomaniku isikusamasuse ja viisa autentsuse kontrollimist, kasutades selleks viisainfosüsteemi (VIS) kooskõlas määruse (EÜ) nr 767/2008 artikliga 18
	Artikkel 8 (3) (c)	c. erandina võib VISis päringuid teha, kasutades vaid viisakleebise numbrit või kasutades juhuslikkuse alusel viisakleebise numbrit koos sõrmejälgede kontrolliga, kui: i) liiklus muutub nii tihedaks, et ooteaeg piiripunktis pikeneb liigselt, ii) kõik ressursid (st töötajad, vahendid ja organisatsioon) on võetud juba kasutusele ning iii) hinnangu põhjal puudub sisejulgeoleku ja ebaseadusliku sisserändega seotud oht. [...]
Euroopa Parlamendi ja nõukogu määrus (EL) 2017/458, 15. märts 2017, millega muudetakse määrust (EL) 2016/399 seoses asjaomastes andmebaasides tehtava kontrolli tugevdamisega välispiiridel **(Schengeni piirieeskirja muutev määrus)**	Artikkel 1 1)	Määruse (EL) 2016/399 artiklit 8 muudetakse järgmiselt: 1) lõige 2 asendatakse järgmisega: „2. Sisenemisel ja väljumisel kontrollitakse liidu õiguse alusel vaba liikumise õigust omavaid isikuid järgmiselt: a) isiku tuvastamine ning kodakondsuse ja piiriületuseks vajaliku reisidokumendi autentsuse ja kehtivuse kontroll, sealhulgas päringute tegemine asjaomastes andmebaasides, eelkõige järgmistes: 1) SIS;

		2) Interpoli varastatud ja kaotatud reisidokumentide andmebaas; 3) riigisisesed andmebaasid, mis sisaldavad teavet varastatud, õigusvastaselt omandatud, kaotatud ja kehtetuks tunnistatud reisidokumentide kohta; Nõukogu määruse (EÜ) nr 2252/2004 (*1) artikli 1 lõikes 2 osutatud andmekandjat sisaldavas passis ja reisidokumendis kontrollitakse kiibile salvestatud andmete autentsust. b) kontrollimine, et liidu õiguse alusel vaba liikumise õigust omav isik ei ohusta ühegi liikmesriigi avalikku korda, sisejulgeolekut, rahvatervist ega rahvusvahelisi suhteid, sealhulgas päringute tegemine SISis ja teistes asjaomastes liidu andmebaasides. See ei piira päringute tegemist riigisisestes ja Interpoli andmebaasides. Kui tekib kahtlus reisidokumendi autentsuses või selle kasutaja isikus, kontrollitakse vähemalt ühte biomeetrilist tunnust, mis on kantud määruse (EÜ) nr 2252/2004 alusel välja antud passi ja reisidokumenti. Võimaluse korral kontrollitakse samal viisil ka nimetatud määrusega hõlmamata reisidokumente.
	Artikkel 1 2)	2) lõike 3 punkti a alapunktid i ja ii asendatakse järgmisega: „i) kolmanda riigi kodaniku isiku tuvastamist ja kodakondsuse ning piiriületuseks vajaliku reisidokumendi autentsuse ja kehtivuse kontrollimist, sealhulgas päringute tegemist asjaomastes andmebaasides, eelkõige järgmistes: 1) SIS; 2) Interpoli varastatud ja kaotatud reisidokumentide andmebaas; 3) riigisisesed andmebaasid, mis sisaldavad teavet varastatud, õigusvastaselt omandatud, kaotatud ja kehtetuks tunnistatud reisidokumentide kohta. Andmekandjat sisaldavas passis ja reisidokumendis kontrollitakse kiibile salvestatud andmete autentsust vastavalt kehtivate sertifikaatide olemasolule;

		ii) kontrollimist, et reisidokumendiga on kaasas viisa või elamisluba, kui see on nõutav.“;
SIS II määrus	Põhjenduspunkt 10	SIS II peaks sisaldama hoiatusteateid riiki sisenemise või riigis viibimise keelamiseks. On vaja kaaluda täiendavalt selliste sätete ühtlustamist, mis käsitlevad kolmandate riikide kodanike riiki sisenemise või riigis viibimise keelamiseks väljastatud hoiatusteadete põhjuseid, ning selgitada nende kasutamist varjupaiga-, sisserände- ja tagasipöördumispoliitikate raames. Seetõttu peaks komisjon kolme aasta jooksul käesoleva määruse kohaldamise kuupäevast vaatama läbi sätted riiki sisenemise või riigis viibimise keelamist käsitlevate hoiatusteadete väljastamise eesmärkide ja tingimuste kohta.
	Artikkel 20 (2) (f)	2. Teave, mis käsitleb isikuid, kelle kohta on hoiatusteade sisestatud, sisaldab kõige rohkem järgmist: f. sõrmejäljed;
	Artikkel 22	Fotosid ja sõrmejälgi, nagu osutatud artikli 20 lõike 2 punktides e ja f, kasutatakse tingimusel, et järgitakse järgmisi sätteid: a. fotod ja sõrmejäljed sisestatakse üksnes pärast spetsiaalse kvaliteedikontrolli läbiviimist, et kindlustada andmete kvaliteedi suhtes kehtestatud miinimumstandardite järgimine. Spetsiaalse kvaliteedikontrolli määratlus kehtestatakse artikli 51 lõikes 2 osutatud korras, ilma et see piiraks korraldusasutuse moodustamist käsitleva õigusakti sätete kohaldamist; b. fotosid ja sõrmejälgi kasutatakse üksnes nende kolmanda riigi kodanike isiku tuvastamiseks, kelle andmed on leitud SIS II-s teostatud tähtnumbrilise päringu tulemusel; c. niipea kui tehnika seda võimaldab, võib sõrmejälgi samuti kasutada kolmanda riigi kodaniku isiku tuvastamiseks tema biomeetrilise tunnuse alusel. Enne nimetatud funktsiooni rakendamist SIS II-s esitab komisjon aruande nõutava tehnoloogia kättesaadavuse ja töövalmiduse kohta, mille osas konsulteeritakse Euroopa Parlamendiga.

	Artikkel 29 (1)	Käesoleva määruse kohaselt SIS II sisestatud hoiatusteateid hoitakse ainult niikaua, kui on vaja nende eesmärkide saavutamiseks, milleks hoiatusteade sisestati.
	Artikkel 31	1. Liikmesriigid võivad töödelda artiklis 20 osutatud andmeid riiki sisenemise või oma territooriumil viibimise keelamiseks. 2. Andmeid võib kopeerida ainult tehnilisel otstarbel, kui selline kopeerimine on artiklis 27 osutatud asutustele vajalik vahetu päringu teostamiseks. Kõnealuste koopiate suhtes kohaldatakse käesoleva määruse sätteid. Ühe liikmesriigi sisestatud hoiatusteateid ei tohi kopeerida N.SIS II-st teistesse siseriiklikesse andmefailidesse. 3. Lõikes 2 osutatud tehnilisi koopiaid, mille tulemusena moodustuvad *off-line* andmebaasid, võib säilitada ajavahemikuks, mis ei ületa 48 tundi. Hädaolukorras võib seda ajavahemikku pikendada kuni hädaolukorra lõppemiseni. Olenemata esimesest lõigust ei ole tehnilised koopiad, mille tulemusena moodustuvad viisasid välja andvate asutuste poolt kasutatavavad *off-line* andmebaasid, enam lubatud ühe aasta möödumisel vastava asutuse edukast ühendamisest viisainfosüsteemi sideinfrastruktuuriga, nagu see sätestatakse tulevases määruses, mis käsitleb viisainfosüsteemi (VIS) ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta, välja arvatud koopiate puhul, mis on tehtud üksnes sellises hädaolukorras kasutamiseks, mil võrk on olnud enam kui 24 tunni jooksul ligipääsmatu. Liikmesriigid peavad kõnealuste koopiate ajakohastatud registrit, teevad selle registri kättesaadavaks siseriiklikele järelevalveasutustele ning tagavad kõnealuste koopiate suhtes kõigi käeoleva määruse sätete, eriti artikli 10 sätete kohaldamise. 4. Taolistele andmetele antakse juurdepääsuluba üksnes artiklis 27 osutatud siseriikliku asutuse pädevuse piires ja nõuetekohaselt volitatud töötajatele. 5. Andmeid ei või kasutada halduslikel eesmärkidel. Erandina võivad käesoleva määruse kohaselt sisestatud andmeid kasutada kooskõlas iga liikmesriigi õigusaktidega artikli 27 lõikes 3 osutatud asutused oma ülesannete täitmiseks.

		6. Vastavalt käesoleva määruse artiklile 24 sisestatud andmeid ning otsuse 2006/000/JSK artikli 38 lõike 2 punktide d ja e kohaselt sisestatud isikutega seotud dokumente käsitlevaid andmeid võib kasutada käesoleva määruse artikli 27 lõikes 3 sätestatud otstarbel kooskõlas iga liikmesriigi õigusaktidega. 7. Andmekasutust, mis ei vasta lõigetele 1–6, käsitatakse iga liikmesriigi siseriikliku õiguse kohaselt väärkasutusena. 8. Iga liikmesriik edastab korraldusasutusele nende pädevate asutuste nimekirja, kellel on vastavalt käesolevale otsusele lubatud vahetult otsida SIS II-te sisestatud andmeid, ning nimekirja mis tahes hilisemad muudatused. Selles nimekirjas on iga asutuse puhul märgitud, milliseid andmeid ja millisel eesmärgil ta võib otsida. Korraldusasutus tagab nimekirja iga-aastase avaldamise Euroopa Liidu Teatajas. 9. Kui ühenduse õigusega ei nähta ette erisätteid, kohaldatakse liikmesriigi N.SIS II-te sisestatud andmete suhtes vastava liikmesriigi õigust.
EES määrus	Põhjenduspunkt 20	Riiki sisenemise ja riigist lahkumise süsteem peaks säilitama ja töötlema tähtnumbrilisi andmeid ja biomeetrilisi andmeid peamiselt selleks, et parandada välispiiride haldamist, hoida ära ebaseaduslikku sisserännet ja hõlbustada rändevoogude juhtimist. Lisaks peaksid riiki sisenemise ja riigist lahkumise süsteemi kogutud isikuandmed olema kättesaadavad terroriaktide ja muude raskete kuritegude ennetamiseks, avastamiseks ja uurimisele kaasaaitamiseks üksnes käesolevas määruses kehtestatud tingimustel. Biomeetriliste andmete kasutamine hoolimata selle mõjust reisijate privaatsusele on õigustatud kahel põhjusel. Esiteks on biomeetriliste andmete kasutamine usaldusväärne meetod nende kolmandate riikide kodanike tuvastamiseks, kellel ei ole liikmesriikide territooriumil viibides reisidokumenti või muud isikut tõendavat dokumenti, mis on ebaseaduslike rändajate puhul tavapärane. Teiseks on biomeetrilised andmed usaldusväärsemad seaduslike rändajate riiki sisenemise ja riigist lahkumise andmete võrdlemisel. Näokujutise kasutamine koos sõrmejälgedega võimaldab vähendada registreerimist vajavate sõrmejälgede, koguarvu, tagades samas täpse tuvastamise.

	Põhjenduspunkt 21	Riiki sisenemise ja riigist lahkumise süsteemi tuleks sisestada – kui see on füüsiliselt võimalik – viisanõudest vabastatud kolmanda riigi kodaniku neli sõrmejälge, et võimaldada täpset kontrolli ja tuvastamist ning teha seega kindlaks, et kolmanda riigi kodanik ei ole juba registreeritud teise isikuna või teise reisidokumendiga, ning tagada piisavate andmete olemasolu riiki sisenemise ja riigist lahkumise süsteemi eesmärkide saavutamiseks igas olukorras. Viisat omavate kolmandate riikide kodanike sõrmejälgi võrreldakse VISi andmetega. Riiki sisenemise ja riigist lahkumise süsteemi tuleks salvestada nii viisanõudest vabastatud kui ka viisat omavate kolmandate riikide kodanike näokujutised. Sõrmejälgi või näokujutist tuleks kasutada biomeetrilise tunnusena nende kolmandate riikide kodanike isikusamasuse kontrollimiseks, kes on varem riiki sisenemise ja riigist lahkumise süsteemis registreeritud ning kelle isiklikku toimikut ei ole veel kustutatud. Iga piiripunkti eripära ja eri liiki piiride arvessevõtmiseks peaksid liikmesriikide asutused iga piiripunkti puhul kindlaks määrama, kas vajaliku kontrolli läbiviimisel tuleks peamise biomeetrilise tunnusena kasutada sõrmejälgi või näokujutist.
	Artikkel 10 (2)	2. Kõik pädevad asutused tagavad, et riiki sisenemise ja riigist lahkumise süsteemi kasutamine, sealhulgas biomeetriliste andmete kogumine, on kooskõlas inimõiguste ja põhivabaduste kaitse konventsioonis, Euroopa Liidu põhiõiguste hartas ja ÜRO lapse õiguste konventsioonis sätestatud kaitsemeetmetega. Eelkõige seatakse lapse andmete kogumisel esikohale lapse huvid.
	Artikkel 17 (1) (c)	1. Piirivalveasutus koostab viisanõudest vabastatud kolmandate riikide kodanike isikliku toimiku, sisestades c. parema käe sõrmejälgede andmed kui need on olemas ja nende puudumisel vasaku käe vastavad sõrmejälgede andmed, sõrmejälgede andmed peavad olema piisava lahutusvõime ja kvaliteediga, et neid saaks kasutada automaatseks biomeetriliseks võrdlemiseks;
	Artikkel 18 (2)	2. Kui kolmanda riigi kodanikul keelatakse riiki siseneda põhjusel, mis vastab määruse (EL) 2016/399 V lisa B osa punktidele B, D või H ning kui asjaomase kolmanda riigi kodaniku biomeetriliste andmetega toimikut ei ole riiki sisenemise ja riigist

		lahkumise süsteemis varem salvestatud, koostab piirivalveasutus tema isikliku toimiku, millesse ta kannab käesoleva määruse artikli 16 lõike 1 või artikli 17 lõike 1 alusel nõutavad tähtnumbrilised andmed kui see on asjakohane, ja järgmised andmed: a. kolmandate riikide kodanike puhul, kelle suhtes kohaldatakse viisanõuet käesoleva määruse artikli 16 lõike 1 punktis d osutatud näokujutis; b. viisanõudest vabastatud kolmandate riikide kodanike puhul käesoleva määruse artikli 17 lõike 1 punktide b ja c alusel nõutavad biomeetrilised andmed; c. kolmandate riikide kodanike puhul, kelle suhtes kohaldatakse viisanõuet ja kes ei ole VISi registreeritud käesoleva määruse artikli 16 lõike 1 punktis d osutatud näokujutis ja käesoleva määruse artikli 17 lõike 1 punktis c osutatud sõrmejälgede andmed.
	Artikkel 40 (1) ja (2)	1. Liikmesriik võib täielikus kooskõlas liidu õigusega hoida oma riiklikus sisenemis- ja lahkumissüsteemis või samaväärsetes riiklikes toimikutes selliseid tähtnumbrilisi andmeid, mida asjaomane liikmesriik sisestas riiki sisenemise ja riigist lahkumise süsteemi kooskõlas riiki sisenemise ja riigist lahkumise süsteemi eesmärkidega. 2. Andmeid ei säilitata riiklikus sisenemis- ja lahkumissüsteemis või samaväärsetes riiklikes toimikutes kauem kui riiki sisenemise ja riigist lahkumise süsteemis.
VIS määrus	Artikkel 18 (1)	Liikmesriikide välispiiridel asuvates piiripunktides kooskõlas Schengeni piirieeskirjadega kontrolle tegevatele pädevatele asutustele võimaldatakse kooskõlas lõigetega 2 ja 3 juurdepääs otsingute tegemiseks viisakleebise numbri alusel koos viisaomaniku sõrmejälgede kontrolliga üksnes viisaomaniku isikusamasuse ja/või viisa autentsuse kontrollimiseks ja/või kontrollimaks, kas on täidetud Schengeni piirieeskirjade artikli 5 kohased liikmesriigi territooriumile sisenemise tingimused.
ETIAS määrus	Artikkel 47 (1)	Piirivalveasutused, kes on pädevad teostama vastavalt määrusele (EL) 2016/399 piirikontrolli välispiiripunktides, teevad

		reisidokumendi masinloetaval alal olevaid andmeid kasutades otsinguid ETIASe kesksüsteemis.

Kokkuvõte:

- Schengeni välispiiril põhineb isikusamasuse kontroll (sh vajadusel sõrmejälgede kontroll) Schengeni piirieeskirjal (õiguslik alus), mille täitmine on liikmesriikidele kohustuslik.
- Kuna Schengeni piiriületusel töödeldakse erinevatest andmebaasidest pärit andmeid sõltuvalt andmete töötlemise eesmärgile, on vastavate andmete muu kasutus reguleeritud spetsiifilisi andmebaase reguleerivate aktidega (nt VIS-määrus, SIS-määrus, EES, ETIAS). Üldjuhul on lubatud siseriiklikes süsteemides töödelda andmeid, mille liikmesriik on ise vastavale EL-i kesksüsteemile edastanud.

Schengeni välispiiri kontroll on üks peamisi katsemeetmeid sisepiirikontrollita alal ning aitab kaasa liidu julgeoleku tagamisele. Selleks peavad piirivalveametnikud teostama süstemaatilisi kontrolle piiri ületavate isikute osas, sh nii kolmandate riikide kodanike, kui ka liidu õiguse alusel vaba liikumist omavate isikute osas vastavalt õigusaktidele. Piiril teostatakse kontroll erinevatest EL-i kesksetest andmebaasidest (VIS-st viisakontroll, SIS II-st hoiatusteadete kontroll, EES-st kolmandate kodanike riiki sisenemise ja riigist lahkumise andmete registreeringute kontroll ning sisenemiskeeluandmete kontroll). Nendes andmebaasides tehtavate päringute sisu võib olla mõnevõrra erinev sõltuvalt konkreetse andmebaasi eesmärkidest ja ülesehitusest.

(a) Õiguslik alus

Schengeni välispiiri ületajate kontrolli reguleerib Schengeni piirieeskiri ning seda muutev määrus. Piirikontrolli teostamisel peab pädev piirivalveametnik tegema päringuid EL-i kesksetesse infosüsteemidesse, et teostada Schengeni piirieeskirjade täielik rakendamine. Muu hulgas teostatakse ka passis ja reisidokumendis kiibile salvestatud andmete autentsust – kui tekib autentsuse osas kahtlus, siis kontrollitakse vähemalt ühte biomeetrilist tunnust (näokujutis või sõrmejäljed).

(b) Tingimused

Konkreetsete päringute tegemise tingimused on reguleeritud asjaomast süsteemi või andmebaasi reguleerivates õigusaktides.

6.4. Varjupaiga ja rahvusvahelise kaitse taotluse menetlus

Õigusakt	Säte	Sõnastus
Euroopa Parlamendi ja nõukogu määrus (EL) nr 604/2013, 26. juuni 2013, millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi	Põhjenduspunkt 26	Käesoleva määruse kohaldamisel kohaldavad liikmesriigid isikuandmete töötlemisel Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivi 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta

määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku või kodakondsuseta isiku esitatud rahvusvahelise kaitse taotluse läbivaatamise eest **(Dublin III määrus)**	Artikkel 3 (1)	1. Liikmesriigid vaatavad läbi selliste kolmanda riigi kodanike või kodakondsuseta isikute rahvusvahelise kaitse taotlused, kes taotlevad rahvusvahelist kaitset mõne liikmesriigi territooriumil, sealhulgas piiril või transiidialal. Taotluse vaatab läbi üks liikmesriik, kelleks on III peatükis sätestatud kriteeriumide kohaselt vastutav liikmesriik.
	Artikkel 34 (1)	Iga liikmesriik edastab igale seda soovivale liikmesriigile sellised taotleja isikuandmed, mis on nõuetekohased, asjakohased ja hädavajalikud: a. vastutava liikmesriigi määramiseks; b. rahvusvahelise kaitse taotluse läbivaatamiseks; c. käesolevast määrusest tulenevate kohustuste täitmiseks.
	Artikkel 34 (2)	Lõikes 1 osutatud andmed võivad hõlmata üksnes: a. taotleja ja vajaduse korral tema pereliikmete, sugulaste või teiste perekonda kuuluvate isikute isikuandmeid (täielik nimi ja vajaduse korral endine nimi; hüüd- või varjunimed; praegune ja varasem kodakondsus; sünniaeg ja -koht); b. isikutunnistusi ja reisidokumente (number, kehtivusaeg, väljaandmise kuupäev, väljaandnud asutus, väljaandmise koht jne); c. muud taotleja isikusamasuse kindlakstegemiseks vajalikku teavet, sealhulgas vastavalt määrusele (EL) nr 603/2013 töödeldud sõrmejälgi; d. elukohti ja reisiteekondi; e. liikmesriigi välja antud elamislube või viisasid; f. kohta, kus taotlus on esitatud; g. võimalike varasemate rahvusvahelise kaitse taotluste esitamise kuupäevi, praeguse taotluse esitamise kuupäeva, taotluse menetlemise järku ja otsuse sisu, kui selline otsus on tehtud.
Eurodac määrus	Põhjenduspunkt 31	Selleks et tagada isikuandmete kaitse ja välistada süstemaatiline võrdlemine, mis peaks olema keelatud, tuleks Eurodac-süsteemi andmeid töödelda ainult konkreetsetel juhtudel

		ning kui see on vajalik terroriaktide või muude raskete kuritegude ennetamiseks, avastamiseks või uurimiseks. Erijuhtumiga on eelkõige tegemist siis, kui sõrmejälgede andmete võrdlemise taotluse aluseks on terroriakti või muu raske kuriteoga seotud spetsiifiline ja konkreetne olukord või spetsiifiline ja konkreetne oht või konkreetsed isikud, kelle puhul on põhjendatult alust arvata, et nad panevad toime või on toime pannud mis tahes sellise kuriteo. Erijuhtumiga on tegemist ka siis, kui sõrmejälgede andmete võrdlemise taotlus on seotud isikuga, kes on terroriakti või muu raske kuriteo ohver. Määratud asutused ja Europol peaksid seega taotlema andmete võrdlemist Eurodac-süsteemi andmetega üksnes siis, kui neil on piisavalt alust arvata, et sellise võrdluse tulemusena saadakse teavet, mis oluliselt aitab kaasa terroriakti või muu raske kuriteo ennetamisele, avastamisele või uurimisele.
	Artikkel 1 (3)	Sõrmejälgede andmeid ja muid isikuandmeid võib Eurodac-süsteemis töödelda üksnes käesolevas määruses ja määruse (EL) nr 604/2013 artikli 34 lõikes 1 sätestatud eesmärkidel, ilma et see piiraks päritoluliikmesriigi õigust töödelda Eurodac-süsteemi jaoks mõeldud andmeid oma siseriiklike õigusnormide alusel koostatud andmebaasides.
	Artikkel 25 (5)	Kui lõike 4 kohane lõplik identifitseerimine näitab, et kesksüsteemilt saadud võrdlustulemus ei lange võrdluseks saadetud sõrmejälgede andmetega kokku, kustutavad liikmesriigid viivitamata võrdlustulemused ning teavitavad sellisest asjaolust võimalikult kiiresti ja hiljemalt kolme tööpäeva jooksul komisjoni ja ametit.
	Artikkel 35 (1)	Isikuandmeid, mis liikmesriik või Europol saab kesksüsteemist käesoleva määruse kohaselt, ei edastata ega tehta kättesaadavaks ühelegi kolmandale riigile, liidus või väljaspool seda loodud rahvusvahelisele organisatsioonile ega eraõiguslikule üksusele. See keeld kehtib ka juhul, kui nimetatud andmeid töödeldakse edasi liikmesriigi või liikmesriikidevahelisel tasandil raamotsuse 2008/977/JSK artikli 2 punkti b mõistes.

Kokkuvõte:

- Õiguslik alus biomeetriliste andmete töötlemiseks varjupaiga taotlemise menetluses tuleneb Dublin III määrusest ja Eurodaci määrusest.
- Vastavate biomeetriliste andmete töötlemine ja Eurodaci edastamine on riigile kohustuslik.
- Andmete päritoluriigil on Eurodac-süsteemi jaoks mõeldud andmeid lubatud kasutada oma siseriiklike õigusnormide alusel koostatud andmebaasides.
- Kui lõplik identifitseerimine näitab, et kesksüsteemilt saadud võrdlustulemus ei lange võrdluseks saadetud sõrmejälgede andmetega kokku, kustutavad liikmesriigid viivitamata võrdlustulemused.

(a) Õiguslik alus

Dublin III määrusega kohustatakse liikmesriike kolmanda riigi kodaniku või kodakondsuseta isiku esitatud rahvusvahelise kaitse taotlust läbi vaatama. Sama määrusega on ka loodud Euroopa sõrmejälgede andmebaas ehk Eurodac-süsteem. Eurodac-süsteem võimaldab liikmesriikidel tuvastada varjupaigataotlejad ja ebaseaduslikult ühenduse välispiiri ületanud isikud. Liikmesriigid võivad sõrmejälgede võrdlemise teel kindlaks teha, kas varjupaigataotleja või ebaseaduslikult liikmesriigis viibiv isik on varem mõnes teises liikmesriigis varjupaika taotlenud. See aitab kindlaks teha, milline liikmesriik on vastutav isiku varjupaiga või rahvusvahelise kaitse taotluse menetlemise eest. Eurodacis olevaid isikuandmeid võib kasutada üksnes Dublin III määruse alusel taotluste menetlemiseks, igasugune muu kasutus on üldjuhul keelatud[88].

Sõrmejälgede andmeid ja muid isikuandmeid võib Eurodac-süsteemis töödelda üksnes Eurodac määruse ja Dublin III määruse art-s 34(1) sätestatud eesmärkidel, kuid see ei piira päritoluliikmesriigi õigust töödelda Eurodac-süsteemi jaoks mõeldud andmeid oma siseriiklike õigusnormide alusel koostatud andmebaasides. See tähendab, et kui liikmesriik töötleb samu andmeid ka oma siseriiklikus andmebaasis vastava siseriiklikult kehtestatud õiguslikul alusel, siis sellist töötlemist Eurodac määrus ei reguleeri ega piira.

Andmete edasisele töötlemisele õiguskaitse eesmärgil kohaldub õiguskaitseasutuste direktiiv, samas kui Dublin III määruse eesmärkidel andmete töötlemisele kohaldatakse isikuandmete kaitse üldmäärust.[89]

(b) Tingimused

Eurodac-süsteemis sõrmejälgede süstemaatiline võrdlemine on keelatud. Eurodac-ist võrdluste tegemine on lubatud vaid: a) rahvusvahelise kaitse taotlejate isikute kindlakstegemiseks; b) liidu välispiiride ebaseaduslikul ületamisel kinnipeetute isikute kindlakstegemiseks; c) tuvastamiseks, kas liikmesriigi territooriumil ebaseaduslikult viibiv kolmanda riigi kodanik või kodakondsuseta isik on taotlenud rahvusvahelist kaitset; d) õiguskaitse eesmärgi (kui täidetud on vastavad tingimused); e) varjupaigataotluse menetluse eest vastutava riigi määramiseks; f) rahvusvahelise kaitse taotluse läbivaatamiseks.

Sõrmejälgede võrdlemine õiguskaitse eesmärgil on lubatud üksnes konkreetsetel juhtudel ning kui see on vajalik terroriaktide või muude raskete kuritegude ennetamiseks, avastamiseks või uurimiseks. Erijuhtumiga on eelkõige tegemist siis, kui sõrmejälgede andmete võrdlemise

[88] Erand sellele on kehtestatud Dublin III määruse pp-s 31.

[89] Handbook on European Data Protection Law, lk 317

taotluse aluseks on terroriakti või muu raske kuriteoga seotud spetsiifiline ja konkreetne olukord või spetsiifiline ja konkreetne oht või konkreetsed isikud, kelle puhul on põhjendatult alust arvata, et nad panevad toime või on toime pannud mis tahes sellise kuriteo. Erijuhtumiga on tegemist ka siis, kui sõrmejälgede andmete võrdlemise taotlus on seotud isikuga, kes on terroriakti või muu raske kuriteo ohver. Liikmesriikide määratud asutused peaksid seega taotlema andmete võrdlemist Eurodac-süsteemi andmetega üksnes siis, kui neil on piisavalt alust arvata, et sellise võrdluse tulemusena saadakse teavet, mis oluliselt aitab kaasa terroriakti või muu raske kuriteo ennetamisele, avastamisele või uurimisele.[90]

Liikmesriigid peavad tagama ka andmesubjekti õigused nii isikuandmete kaitse üldmääruse kui ka Eurodaci määrusest[91] ning andmete turvalisus enne nende edastamist Eurodaci süsteemi ning edastamise ajal, võttes selleks ette nähtud meetmed[92].

6.5. Illegaalimenetlus

Õigusakt	Säte	Sõnastus
Eurodac määrus	Artikkel 14 (1)	Iga liikmesriik võtab viivitamata kõikide sõrmede sõrmejäljed kõikidelt vähemalt 14-aastastelt kolmandatest riikidest saabunud kolmandate riikide kodanikelt või kodakondsuseta isikutelt, kelle pädevad kontrolliasutused on kinni pidanud seoses kõnealuse liikmesriigi maismaa-, mere- või õhupiiri ebaseadusliku ületamisega ja keda ei ole tagasi saadetud või kes asuvad füüsiliselt liikmesriikide territooriumil ning keda ei ole kogu kinnipidamise ja tagasisaatmise otsuse alusel väljasaatmise vahelise ajavahemiku vältel hoitud vahi all, vangistuses või kes ei ole olnud eeluurimise all.
	Artikkel 17 (1)	Liikmesriik võib edastada kesksüsteemi oma viitenumbriga varustatud andmed sõrmejälgede kohta, mida liikmesriik võib olla võtnud ebaseaduslikult liikmesriigis viibimiselt tabatud vähemalt 14-aastastelt kolmandate riikide kodanikelt või kodakondsuseta isikutelt, et kontrollida, kas nad on varem esitanud rahvusvahelise kaitse taotluse teises liikmesriigis.
VIS määrus	Artikkel 20 (1)	Asutustele, kes on kooskõlas Schengeni piirieeskirjadega pädevad välispiiridel asuvates piiripunktides või liikmesriikide territooriumil kontrollima, kas liikmesriikide territooriumile sisenemise, seal viibimise või elamise tingimused on täidetud, võimaldatakse juurdepääs päringute tegemiseks isiku sõrmejälgede alusel üksnes iga sellise isiku tuvastamiseks, kes ei täida või enam

[90] Eurodac määrus pp 31

[91] *Ibid*, art 29

[92] *Ibid*, art 34

		ei täida liikmesriigi territooriumile sisenemise, seal viibimise või elamise tingimusi. Kui selle isiku sõrmejälgi ei saa kasutada või sõrmejälgede alusel ei õnnestu päringut teha, tehakse otsing artikli 9 lõike 4 punktis a ja/või c osutatud andmete alusel; sellise otsingu võib teha koos artikli 9 lõike 4 punktis b osutatud andmetega.
	Artikkel 20 (3)	Juhul kui isikul on viisa, on pädevatel asutustel juurdepääs VISile esmalt kooskõlas artikliga 18 või 19.
SIS II määrus	Artikkel 24 (3)	Hoiatusteate võib samuti sisestada, kui lõikes 1 osutatud otsus põhines asjaolul, et kolmanda riigi kodaniku suhtes on kohaldatud väljasaatmist, sisenemisest keeldumist või tagasisaatmist hõlmavat meedet, mida ei ole tühistatud või mille täitmist ei ole peatatud ja milles sisaldub või millega kaasneb sisenemiskeeld või vajaduse korral riigis elamise keeld ning mis põhineb kolmandate riikide kodanike sisenemise või riigis elamisega seotud siseriiklike eeskirjade eiramisel.
	Artikkel 27 (1)	SIS II-te sisestatud andmetele on juurdepääs ja neid andmeid on õigus otsida vahetult või SIS II andmete koopias ainult kolmandate riikide kodanike tuvastamise eest vastutavatel asutustel, kelle ülesandeks on: a) piirivalve; vastavalt Euroopa Parlamendi ja nõukogu 15. märtsi 2006. aasta määrusele (EÜ) nr 562/2006, millega kehtestatakse isikute üle piiri liikumist reguleerivad ühenduse eeskirjad (Schengeni piirieeskirjad); b) muud kõnealuses liikmesriigis teostatavad politsei- ja tollikontrollid, nende kontrollide kooskõlastamine määratud asutuste poolt.
	Artikkel 27 (2)	Siseriiklikud õigusasutused, muu hulgas need, kes vastutavad riiklike süüdistuste algatamise eest kriminaalmenetluses ja kohtuliku uurimise eest enne süüdistuse esitamist, ning nende kooskõlastusasutused võivad oma siseriiklike õigusaktidega sätestatud ülesannete täitmiseks aga samuti omada juurdepääsu SIS II-te sisestatud andmetele ning kasutada õigust vahetult sellist teavet otsida.
	Artikkel 27 (3)	Peale selle võivad vastavalt SIS II-te sisestatud andmetele ja kooskõlas otsuse 2006/000/JSK artikli 38 lõike 2 punktidega d ja e sisestatud ning

		isikutega seotud dokumente käsitlevatele andmetele juurdepääsu õigust ja nende andmete vahetu otsimise õigust kasutada viisade andmise eest vastutavad asutused, viisataotluste läbivaatamise eest vastutavad keskasutused ja asutused, kes vastutavad elamislubade andmise ja kolmandate riikide kodanikke käsitlevate õigusnormide kohaldamise eest seoses isikute liikumise alaste ühenduse õigusaktide kohaldamisega. Nende asutuste juurdepääsu andmetele reguleerib liikmesriigi õigus.
EES määrus	Artikkel 27 (1)	Piirivalveasutustele või immigratsiooniasutustele antakse juurdepääs otsingute tegemiseks sõrmejälgede andmete või sõrmejälgede andmete ja näokujutise alusel üksnes selliste kolmandate riikide kodanike tuvastamiseks, kes võivad olla riiki sisenemise ja riigist lahkumise süsteemis varem registreeritud teistsuguste isikuandmetega või kes ei täida või enam ei täida liikmesriikide territooriumile sisenemise või seal viibimise tingimusi.
Euroopa Parlamendi ja nõukogu määrus (EL) 2018/1240, 12. september 2018, millega luuakse Euroopa reisiinfo ja -lubade süsteem (ETIAS) ning muudetakse määrusi (EL) nr 1077/2011, (EL) nr 515/2014, (EL) 2016/399, (EL) 2016/1624 ja (EL) 2017/2226 **(ETIAS määrus)**	Artikkel 13 (1) ja 13 (4)	1. Juurdepääs ETIASe infosüsteemile on ainult ETIASe kesküksuse ja ETIASe riiklike üksuste nõuetekohaselt volitatud töötajatel. 4. Immigratsiooniasutustel on kooskõlas artikliga 49 juurdepääs ETIASe kesksüsteemile üksnes selleks, et saada teavet liikmesriigi territooriumil viibiva reisija reisiloa oleku kohta, ning juurdepääs nimetatud artiklis osutatud teatavatele andmetele. Immigratsiooniasutustel on kooskõlas artikli 65 lõikega 3 juurdepääs ETIASe kesksüsteemile üksnes nimetatud artiklis osutatud andmete saamiseks.
	Artikkel 49 (1)	Selleks et kontrollida, kas liikmesriikide territooriumile sisenemise või seal viibimise tingimused on täidetud, ning et võtta sellega seoses asjakohaseid meetmeid, on liikmesriikide immigratsiooniasutustel juurdepääs otsingute tegemiseks ETIASe kesksüsteemis, kasutades andmeid, millele on osutatud artikli 17 lõike 2 punktides a–e.
Euroopa Parlamendi ja nõukogu direktiiv 2008/115/EÜ, 16. detsember 2008 , ühiste nõuete ja korra kohta liikmesriikides ebaseaduslikult viibivate kolmandate riikide kodanike tagasisaatmisel	Põhjenduspunkt 18	Liikmesriikidel peaks olema kiire juurdepääs teiste liikmesriikide väljastatud sisenemiskeelde käsitlevale teabele. Selline teabevahetus peaks toimuma vastavalt Euroopa Parlamendi ja nõukogu 20. detsembri 2006. aasta määrusele (EÜ) nr 1987/2006 (mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist)

(Naasmisdirektiiv)		

Kokkuvõte:

- Õiguslik alus biomeetriliste andmete töötlemiseks illgaalimenetluses tuleneb EL-i õigusaktidest (Eurodac määrus, VIS määrus, EES määrus), mis käsitlevad liidu välispiiri ebaseaduslikku ületamist ning liikmesriikides ebaseaduslikku viibimist.
- Ebaseadusliku riigipiiri ületamisel kinni peetud kolmandate riikide kodanike või kodakondsuseta isikute andmete (sh sõrmejälgede andmete) edastamine Eurodaci süsteemi on riigile kohustuslik.
- Kui riik tabab riigis ebaseaduslikult viibivad kolmandate riikide kodanikud või kodakondsuseta isiku, võid ta edastada andmed Eurodaci süsteemi võrdluseks, et kontrollida, kas isik on esitanud rahvusvahelise kaitse taotluse teises liikmesriigis. Neid sõrmejälgede andmeid ei salvestata Eurodaci kesksüsteemis.
- VIS-süsteemi kasutatakse sõrmejälgede alusel isiku tuvastamiseks, kes ei täida liikmesriikidesse sisenemise, seal viibimise või elamise tingimusi. Liikmesriigi pädevale asutusele luuakse võimalus sellise päringu teostamiseks, kuid see ei ole kohustuslik.
- Liikmesriigid võivad sisestada sissesõidukeelu andmed SIS II süsteemi hoiatusteate raames, kuid hetkel ei ole see riikidele kohustuslik.
- Liidus ebaseaduslikult viibivate isikute tuvastamiseks on pädevatel asutustel võimalik teha päringuid erinevates EL-i andmebaasides. Vastavad õigused on sätestatud konkreetset andmebaasi reguleerivas õigusaktis.

Illegaalimenetluse all mõeldakse käesoleva analüüsi raames menetlust, mis viiakse läbi kolmanda riigi kodaniku või kodakondsuseta isiku tabamisel Schengeni välispiiril või liikmesriigi territooriumil, kui vastaval isikul puudub õigus Schengeni välispiiri ületada või liikmesriigis viibida, või kui on kahtlus, et isikul puudub vastav õigus.

Käesolevast analüüsist on välja jäetud välispiiri ületamise või liikmesriigis viibimise õigust andvate dokumentide (viisad, elamisload) tühistamise või kehtetuks tunnistamise menetlus, sest eelduslikult ei töödelda ega koguta selle menetluse käigus täiendavalt biomeetrilise andmeid võrreldes vastava loa andmise menetluses (nt viisamenetluses juba kogutakse 10 sõrmejälge ja foto). Erandiks võib olla olukord, kui isiku kohta ei ole selliseid andmeid kogutud, kuid nüüd lisatakse hoiatusteade SIS II süsteemi. Sellisel juhul lähtutakse SIS II määruses sätestatud hoiatusteate edastamise regulatsioonist.

(a) Õiguslik alus

<u>Eurodac</u>

Ebaseadusliku piiriületuse ning ebaseadusliku viibimise korral liikmesriigis toimuvad Eurodaci süsteemis erinevad andmetöötluse tegevused: esimesel juhul liikmesriik kohustub edastama andmed Eurodaci ning teisel juhul võib teostada andmete võrdluse süsteemis olevate andmetega.

Võrdluse teostamise korral annab süsteem teate andmete kokkulangevuse või negatiivse võrdlustulemuse kohta. Andmete kokkulangevuse korral edastatakse päringu teinud riigile

süsteemis olevad täiendavad andmed (sh sõrmejäljeandmed, mille osas teeb lõpliku identifitseerimise sõrmejäljeekspert). Kui lõplik identifitseerimine näitab, et Eurodac-ist saadud võrdlustulemus ei lange võrdluseks saadetud sõrmejälgede andmetega kokku, kustutavad liikmesriigid viivitamata võrdlustulemused ning teavitavad sellisest asjaolust võimalikult kiiresti ja hiljemalt kolme tööpäeva jooksul komisjoni ja ametit.

VIS

Lisaks Eurodac-süsteemile teostatakse võrdlus ka VIS-süsteemiga. VIS-süsteemi kasutatakse sõrmejälgede alusel isiku tuvastamiseks, kes ei täida liikmesriikidesse sisenemise, seal viibimise või elamise tingimusi. Kui isikul on viisa, siis on pädevatel asutustel juurdepääs VIS-ile vastavalt VIS määruse sätetele, mis reguleerivad andmetele juurdepääsu viisakleebise numbri ja sõrmejälgede alusel. Liikmesriigi pädevale asutusele luuakse võimalus sellise päringu teostamiseks, kuid see ei ole kohustuslik.

SIS II

SIS II süsteemi lisatav hoiatusteade võib sisaldada isiku biomeetrilisi andmeid, sõrmejälgi ja fotot. Hoiatusteate võib vastavalt SIS II määrusele sisestada süsteemi mh ka juhul kui isiku suhtes on kohaldatud väljasaatmist, riiki sisenemisest keeldumist või tagasisaatmist hõlmavat meedet, mida ei ole tühistatud või mille täitmist ei ole peatatud ja milles sisaldub või millega kaasneb sisenemiskeeld või vajaduse korral riigis elamise keeld ning mis põhineb kolmandate riikide kodanike sisenemise või riigis elamisega seotud siseriiklike eeskirjade eiramisel. Seega on hoiatusteate lisamine SIS II süsteemi hetkel vabatahtlik.

Naasmisdirektiiv viitab, et liikmesriikidel peab olema sisenemiskeelde käsitlevale teabele juurdepääs vastavalt SIS II määrusele ehk läbi SIS II süsteemi. Seega lähtutakse biomeetriliste andmete töötlemisel SIS II määrusest. Samas ei ole pruugi päringud sisenemiskeeldude osas käesoleval hetkel anda täielikku pilti, sest riikidel puudub kohustus sisenemiskeeldude andmeid SIS II süsteemi lisada. Käesoleval hetkel on SIS II regulatsiooni puudutava reformiga arutlusel ka sissesõidukeelu teavet puudutava info sisestamise kohustuse kehtestamine liikmesriikidele.

SIS II süsteemis päringute tegemise õigused on määratud asutustele ette nähtud SIS II määruse art-s 27.

EES

Piirivalve ja immigratsiooniasutustele on lisaks juurdepääs ka EES süsteemile kas sõrmejälgede andmete või sõrmejälgede ja näokujutise alusel tuvastamaks kolmandate riikide kodanikke, kes võivad olla EES süsteemis varem registreeritud teistsuguste isikuandmetega või kes ei täida liikmesriikide territooriumile sisenemise või seal viibimise tingimusi.

Kui päring tehakse muul eesmärgil (nt isikusamasuse kontrollimiseks piiril või liikmesriigi territooriumil, mille puhul sisendandmed ei ole biomeetrilised andmed), kuid otsingust selgub, et isiku andmed ei ole EES süsteemis registreeritud, isiku tuvastamine ebaõnnestub või isikusamasuses on kahtlusi, antakse juurdepääs EES-s olevatele andmetele vastavalt EES määruse art-le 27 ehk biomeetriliste tunnuste alusel.

ETIAS

Immigratsiooniasutustel on õigus teha päringuid ETIAS süsteemi kontrollimaks, kas isikul on liikmesriikide territooriumile sisenemise või seal viibimise tingimused täidetud. Erinevalt teistest käesolevas peatükis analüüsitud infosüsteemidest ei ole ETIASe süsteemis biomeetrilisi andmeid.

(b) Tingimused

Eurodac

Sõrmejälgede andmeid ja muid isikuandmeid võib Eurodac-süsteemis töödelda üksnes VIS määruses ja Dublin III määruses sätestatud eesmärkidel. See ei piira päritoluliikmesriigi õigust töödelda Eurodac-süsteemi jaoks mõeldud andmeid oma siseriiklike õigusnormide alusel koostatud andmebaasides[93].

Kui lõplik identifitseerimine näitab, et kesksüsteemilt saadud võrdlustulemus ei lange võrdluseks saadetud sõrmejälgede andmetega kokku, kustutavad liikmesriigid viivitamata võrdlustulemused ning teavitavad sellisest asjaolust võimalikult kiiresti ja hiljemalt kolme tööpäeva jooksul komisjoni ja ametit[94].

VIS

VIS-st tehakse päring isiku sõrmejälgede alusel või kui sõrmejälgi ei saa kasutada või nende alusel ei õnnestu päringut teha, siis isiku nime (perekonnanimi, sünnijärgne perekonnanimi, varasemad perekonnanimed, eesnimi), soo, sünniaja, -koha, -riigi ja /või reisidokumendi liigi ja numbri, väljastanud asutuse ning väljaandmise kuupäeva ja kehtivusaja lõpu järgi, samuti võib päringu teha koos praeguse kodakondsuse ja sünnijärgse kodakondsuse andmetega. Kui selgib, et isiku andmed on VIS-is registreeritud, saab päringu teinud liikmesriik tutvuda isiku tehtud taotluse andmetega, fotoga, väljastatud viisadega.

VIS-ist saadud andmeid võib hoida riiklikes toimikutes üksnes juhul, kui see on üksikjuhtumil vajalik, kooskõlas VIS-i eesmärgi ja asjakohaste, sh andmekaitset käsitletavate seadusesätetega, ning mitte kauem kui üksikjuhtumil vajalik[95]. See ei piira aga liikmesriigi õigust hoida riiklikes toimikutes selle liikmesriigi poolt VIS-i sisestatud andmeid.

SIS II

Piirivalvel, politsei- ja tollikontrollil on õigus SIS II süsteemis andmetele juurde pääseda SIS II määruse art-s 27 toodud eesmärkidel (nt kolmandate riikide kodanike tuvastamiseks). Liikmesriigid võivad töödelda andmeid riiki sisenemise või oma territooriumil viibimise keelamiseks[96]. SIS II andmete edasine töötlemine on üldjuhul keelatud, mh ei tohi ühe liikmesriigi sisestatud hoiatusteateid ei tohi kopeerida N.SIS II-st teistesse siseriiklikesse andmefailidesse.[97]

EES

EES süsteemis võib illegaalimenetluse raames sõrmejälgede ja näokujutise alusel andmetele juurdepääsu saada vaid EES määruses toodud eesmärkidel. Juurdepääs võimaldatakse sel eesmärgil piirivalveasutustele või immigratsiooniasutustele. Riiklikes toimikutes võib neid andmeid hoida vaid juhul, kui see on üksikjuhtumil vajalik, kooskõlas andmete saamise eesmärgiga (st muul eesmärgil töödelda ei tohi) ning asjakohaste õigusaktidega ning vaid nii kaua, kui see vastava üksikjuhtumi puhul on vajalik.[98]

ETIAS

Immigratsiooniasutused saavad juurdepääsu ETIASe süsteemi andmetele üksnes juhul kui eelnevalt on tehtud otsing EES-st EES määruse art 26 alusel ning kui sellest otsingu tulemustest

[93] Eurodac määrus art 1(3)

[94] *Ibid*, art 25

[95] VIS määrus art 30(1)

[96] SIS II määrus art 31(1)

[97] *Ibid*, art 31(2)

[98] EES määrus art 28

ilmneb, et EES süsteemis ei ole riiki sisenemise andmeid, mis vastavad asjaomase kolmanda riigi kodaniku viibimisele liikmesriikide territooriumil.

6.6. Süütegudega seotud menetlused

Õigusakt	Säte	Sõnastus
Austria Vabariigi, Belgia Kuningriigi, Hispaania Kuningriigi, Luksemburgi Suurhertsogiriigi, Madalmaade Kuningriigi, Prantsuse Vabariigi ja Saksamaa Liitvabariigi vahelise eelkõige terrorismi-, piiriülese kuritegevuse ja ebaseadusliku rände vastases võitluses piiriülese koostöö tõhustamise leping **(Prümi leping)**	Artikkel 9 (1)	1. Kuritegude ennetamiseks ja uurimiseks võimaldavad lepinguosalised teiste lepinguosaliste riiklikele kontaktpunktidele, keda on nimetatud artiklis 11, juurdepääsu selleks otstarbeks loodud sõrmejälgede automatiseeritud identifitseerimise süsteemides olevatele viiteandmetele koos õigusega teha sõrmejälgede andmeid võrreldes automatiseeritud otsinguid. Õigust teha otsingut võib kasutada ainult üksikjuhtudel ja kooskõlas otsingut tegeva lepinguosalise õigusega.
Nõukogu otsus 2008/615/JSK, 23. juuni 2008, piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega	Artikkel 26 (1)	1. Isikuandmete töötlemine andmeid saava liikmesriigi poolt on lubatud üksnes eesmärkidel, milleks andmed on otsuse kohaselt edastatud. Teabe kasutamine teistel eesmärkidel on lubatud ainult registrit haldava liikmesriigi eelneval loal ja üksnes andmeid saava liikmesriigi siseriikliku õiguse kohaselt. Sellise loa võib anda tingimusel, et kõnealune muudel eesmärkidel töötlemine on lubatud registrit haldava liikmesriigi siseriikliku õigusega.
	Artikkel 26 (2)	2. Otsingut sooritavatel või andmeid võrdlevatel liikmesriikidel lubatakse artiklite 3, 4 ja 9 kohaselt edastatud andmeid töödelda üksnes selleks, et: a. kindlaks teha, kas võrreldavad DNA-profiilid või sõrmejälgede andmed omavahel kokku langevad; b. nende andmete omavahelise kokkulangevuse korral koostada ja esitada kooskõlas siseriikliku õigusega politsei- või õigusasutuse õigusabitaotlus; c. andmeid artikli 30 tähenduses salvestada. Registrit haldav liikmesriik võib talle edastatud andmeid töödelda kooskõlas artiklitega 3, 4 ja 9 üksnes juhul, kui see on vajalik võrdlemiseks, otsingutele automaatvastuste saamiseks või artikli 30 kohaseks salvestamiseks.

		Edastatud andmed kustutatakse viivitamata pärast andmete võrdlemist või otsingutele automaatvastuste saamist, kui ei ole vajalik edasine töötlemine esimese lõigu punktides b ja c nimetatud eesmärkidel.
Nõukogu otsus 2008/616/JSK, 23. juuni 2008, millega rakendatakse otsust 2008/615/JSK piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega	Sisaldab haldus- ja tehnilisi sätteid sõrmejälgede andmete automatiseeritud andmevahetuseks, mis on vajalikud otsuse 2008/615/JSK rakendamiseks.	
Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK **(õiguskaitseasutuste direktiiv)**	Artikkel 4	1. Liikmesriigid näevad ette järgmist: a. isikuandmeid töödeldakse seaduslikult ja õiglaselt; b. isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei töödelda viisil, mis on nende eesmärkidega vastuolus; c. isikuandmed on piisavad ja asjakohased ega ole liiased nende töötlemise eesmärkide suhtes; d. isikuandmed on õiged ja vajaduse korral ajakohastatud; võetakse kõik mõistlikud meetmed tagamaks, et töötlemise eesmärgi seisukohast ebaõiged isikuandmed kustutatakse või parandatakse viivitamata; e. isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada üksnes seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse; f. isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kadumise, hävimise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid.
	Artikkel 10	1. Selliste isikuandmete töötlemine, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, ning geneetiliste andmete, füüsilise isiku kordumatuks tuvastamiseks kasutatavate biomeetriliste andmete, tervist või

		seksuaalelu või seksuaalset sättumust käsitlevate andmete töötlemine on lubatud üksnes siis, kui see on rangelt vajalik, sellele kohaldatakse andmesubjekti õiguste ja vabaduste kaitsmiseks asjakohaseid kaitsemeetmeid ning üksnes järgmistel juhtudel: a. see on lubatud liidu või liikmesriigi õigusega; b. et kaitsta andmesubjekti või teise füüsilise isiku elulisi huve või 2. selliselt töödeldakse isikuandmeid, mille andmesubjekt on ilmselgelt avalikustanud.
Ettepanek: ***Euroopa Parlamendi ja nõukogu määrus, millega luuakse kesksüsteem nende liikmesriikide väljaselgitamiseks, kellel on teavet kolmandate riikide kodanike ja kodakondsuseta isikute suhtes tehtud süüdimõistvate kohtuotsuste kohta, et täiendada ja toetada Euroopa karistusregistrite infosüsteemi (ECRIS-TCN-süsteem), ning muudetakse määrust (EL) nr 1077/2011***	Artikkel 5 (1) (b)	1. Iga kolmanda riigi kodaniku kohta, kelle suhtes on tehtud süüdimõistev kohtuotsus, teeb süüdimõistva kohtuotsuse teinud liikmesriigi ametiasutus kesksüsteemis registrikande. Registrikanne sisaldab järgmisi andmeid: b. sõrmejälgede andmed vastavalt raamotsusele 2009/315/JHA koos artikli 10 lõike 1 punktis b osutatud sõrmejälgede eraldusvõime ja kasutamise tehnilisele kirjeldusega; süüdimõistetud isiku sõrmejälgede andmete viitenumber, sh süüdimõistva kohtuotsuse teinud liikmesriigi kood;
	Artikkel 5 (2)	2. Registrikanne võib sisaldada ka kolmanda riigi kodaniku, kelle suhtes on tehtud süüdimõistev kohtuotsus, näokujutist.
	Artikkel 6	1. Artikli 5 lõikes 2 osutatud näokujutist kasutatakse üksnes tähtnumbrilise päringu tulemusel või sõrmejälgede alusel tuvastatud kolmanda riigi kodaniku isikusamasuse kontrollimiseks. 2. Niipea kui tehnika seda võimaldab, võib ka näokujutist kasutada kolmanda riigi kodaniku isiku tuvastamiseks selle biomeetrilise tunnuse alusel. Enne nimetatud funktsiooni rakendamist ECRIS-TCN-süsteemis esitab komisjon aruande nõutava tehnoloogia kättesaadavuse ja töövalmiduse kohta, mille osas konsulteeritakse Euroopa Parlamendiga.
	Artikkel 22 (1)	1. Kesksüsteemi sisestatud andmeid töödeldakse üksnes selle liikmesriigi (nende liikmesriikide) väljaselgitamiseks,

		kellel on kolmandate riikide kodanike kohta karistusregistriandmeid.
Eurodac määrus	Põhjenduspunkt 8	Võitluses terroriaktide ja muude raskete kuritegude vastu on oluline, et õiguskaitseasutustel oleks oma ülesannete täitmiseks täielik ja kõige ajakohasem teave. Eurodac-süsteemis sisalduv teave on vajalik terroriaktide või muude raskete kuritegude ennetamiseks, avastamiseks või uurimiseks nagu on osutatud vastavalt nõukogu 13. juuni 2002. aasta raamotsuses 2002/475/JSK terrorismivastase võitluse kohta ja nõukogu 13. juuni 2002. aasta raamotsuses 2002/584/JSK Euroopa vahistamismääruse ja liikmesriikidevahelise üleandmiskorra kohta. Seepärast peaks Eurodac-süsteemi andmed olema kättesaadavad käesolevas määruses sätestatud tingimustel, et neid oleks võimalik võrrelda liikmesriikide määratud asutuste ja Euroopa Politseiameti (Europol) andmetega.
	Põhjenduspunkt 13	Kuna Eurodac-süsteem loodi esialgselt Dublini konventsiooni kohaldamise hõlbustamiseks, tähendab terroriaktide või muude raskete kuritegude ennetamiseks, avastamiseks või uurimiseks antav juurdepääs Eurodac-süsteemile kõnealuse süsteemi algse eesmärgi muutmist, mis piirab nende isikute põhiõigust eraelu puutumatusele, kelle andmeid Eurodac-süsteemis töödeldakse. Kõik sellised piirangud peavad olema kooskõlas õigusnormidega, mis tuleb sõnastada piisavalt täpselt, et isikud saaksid kohandada oma käitumist, ning need normid peavad kaitsma isikuid omavoli eest ja määrama piisavalt täpselt kindlaks pädevatele asutustele antava kaalutlusõiguse ulatuse ja selle kasutamise korra. Demokraatlikus ühiskonnas peavad kõik sellised piirangud olema vajalikud õigustatud ja proportsionaalse huvi kaitsmiseks ning proportsionaalsed õiguspärase eesmärgiga, mida nendega tahetakse saavutada.
	Põhjenduspunkt 14	Kuigi Eurodac-süsteemi esialgne eesmärk ei hõlmanud võimalust taotleda andmete võrdlemist andmebaasis olevate andmetega latentsete sõrmejälgede ehk kuriteopaigalt leitavate daktüloskoopiliste andmete alusel, on kõnealune võimalus politseikoostöö valdkonnas keskse tähtsusega. Võimalus võrrelda latentseid sõrmejälgi Eurodac-süsteemis salvestatud sõrmejälgede andmetega juhtudel, kui on piisavalt alust arvata, et kuriteo toimepanija või ohver kuulub mõnda käesoleva määrusega hõlmatud kategooriasse, annab liikmesriikide määratud

		asutustele väga väärtusliku vahendi terroriaktide või muude raskete kuritegude ennetamiseks, avastamiseks või uurimiseks näiteks juhul, kui kuriteopaigalt leitavad ainsad tõendid on latentsed sõrmejäljed.
	Põhjenduspunkt 15	Käesolevas määruses sätestatakse ka tingimused, mille kohaselt tuleks lubada esitada taotlus sõrmejälgede andmete võrdlemiseks Eurodac-süsteemi andmetega terroriaktide või muude raskete kuritegude ennetamiseks, avastamiseks või uurimiseks, ning vajalikud kaitsemeetmed, et tagada nende isikute põhiõigus eraelu puutumatusele, kelle andmeid Eurodac-süsteemis töödeldakse. Kõnealuste tingimuste rangus tuleneb asjaolust, et Eurodac-süsteemi andmebaasis registreeritakse selliste isikute sõrmejälgede andmed, keda ei kahtlustata terroriaktide või teiste tõsiste kuritegude toimepanemises
	Põhjenduspunkt 31	Selleks et tagada isikuandmete kaitse ja välistada süstemaatiline võrdlemine, mis peaks olema keelatud, tuleks Eurodac-süsteemi andmeid töödelda ainult konkreetsetel juhtudel ning kui see on vajalik terroriaktide või muude raskete kuritegude ennetamiseks, avastamiseks või uurimiseks. Erijuhtumiga on eelkõige tegemist siis, kui sõrmejälgede andmete võrdlemise taotluse aluseks on terroriakti või muu raske kuriteoga seotud spetsiifiline ja konkreetne olukord või spetsiifiline ja konkreetne oht või konkreetsed isikud, kelle puhul on põhjendatult alust arvata, et nad panevad toime või on toime pannud mis tahes sellise kuriteo. Erijuhtumiga on tegemist ka siis, kui sõrmejälgede andmete võrdlemise taotlus on seotud isikuga, kes on terroriakti või muu raske kuriteo ohver. Määratud asutused ja Europol peaksid seega taotlema andmete võrdlemist Eurodac-süsteemi andmetega üksnes siis, kui neil on piisavalt alust arvata, et sellise võrdluse tulemusena saadakse teavet, mis oluliselt aitab kaasa terroriakti või muu raske kuriteo ennetamisele, avastamisele või uurimisele.
	Põhjenduspunkt 33	Määratud asutused peaksid selliseks võrdlemiseks vajalike tingimuste täidetuse korral enne Eurodac-süsteemist otsimist kasutama ka viisainfosüsteemi vastavalt nõukogu 23. juuni 2008. aasta otsusele 2008/633/JSK (mis käsitleb liikmesriikide määratud asutuste ja Europoli juurdepääsu viisainfosüsteemile (VIS) terroriaktide ja muude raskete kuritegude ennetamise, avastamise ja uurimise eesmärkidel)

	Artikkel 20	1. Määratud asutused võivad oma volituste piires ja artikli 1 lõikes 2 sätestatud eesmärgil esitada põhjendatud elektroonilise taotluse sõrmejälgede andmete võrdlemiseks kesksüsteemis säilitatavate andmetega ainult siis, kui andmesubjekti ei õnnestunud tuvastada võrdlemisel järgmistes andmebaasides olevate andmetega: — siseriiklikud sõrmejälgede andmebaasid; — otsusel 2008/615/JSK põhinevad teiste liikmesriikide sõrmejälgede automatiseeritud identifitseerimise süsteemid, mille andmetega võrdlemine on tehniliselt võimalik, välja arvatud juhul, kui võib põhjendatult eeldada, et nende süsteemide andmetega võrdlemine ei aita andmesubjekti tuvastada. Vastavad põhjendatud eeldused lisatakse elektroonilisse põhjendatud taotlusesse Eurodac-süsteemi andmetega võrdlemiseks, mille määratud asutus esitab kontrolliasutusele ning — viisainfosüsteem, eeldusel et on täidetud otsuses 2008/633/JSK sellise võrdluse teostamiseks määratud tingimused ning täidetud on kõik alljärgnevad tingimused: a. võrdlemine on vajalik terroriaktide või muude raskete kuritegude ennetamiseks, avastamiseks või uurimiseks, st et esineb ülekaalukas avaliku julgeoleku huvi, mis muudab andmebaasi päringu proportsionaalseks meetmeks; b. võrdlemine on vajalik konkreetse juhtumi korral (s.t et süstemaatilisi võrdlusi ei teostata) ning c. on põhjendatult alust arvata, et võrdlemine aitab oluliselt kaasa asjaomase kuriteo ennetamisele, avastamisele või uurimisele. Selline põhjendatud alus esineb eeskätt põhjendatud kahtluse korral, et terroriaktis või muus tõsises kuriteos kahtlustatav isik või selle toimepanija või ohver kuulub käesoleva määrusega hõlmatud isikute kategooriasse. 2. Taotlus andmete võrdlemiseks Eurodac-süsteemi andmetega piirdub sõrmejälgede andmete otsinguga.

VIS määrus	Artikkel 3	1. Liikmesriikide määratud asutustel on õigus erandjuhtudel ja pärast põhjendatud kirjaliku või elektroonilise taotluse esitamist tutvuda artiklites 9–14 osutatud VISi teabega, kui on piisavalt alust uskuda, et VISis sisalduvate andmetega tutvumine aitab oluliselt kaasa terroriaktide ja teiste raskete kuritegude ärahoidmisele, avastamisele või uurimisele. Europolil on võimalik tutvuda VISiga oma volituste raames ja kui see on vajalik tema kohustuste täitmiseks. 2. Lõikes 1 osutatud tutvumine toimub keskse(te) juurdepääsupunkti(de) kaudu, kes vastutab/vastutavad range kooskõla tagamise eest seoses juurdepääsu tingimuste ja korraga, mis on kehtestatud nõukogu 23. juuni 2008. aasta otsusega 2008/633/JSK, mis käsitleb liikmesriikide määratud asutuste ja Europoli juurdepääsu viisainfosüsteemile (VIS) terroriaktide ja teiste raskete kuritegude ärahoidmise, avastamise ja uurimise eesmärgil (18). Liikmesriigid võivad määrata põhiseaduslike või seaduslike nõuete täitmiseks kooskõlas oma korraldusliku ja haldusstruktuuriga vähemalt ühe keskse juurdepääsupunkti. Kiireloomulisel erandjuhul võivad kesksed juurdepääsupunktid vastu võtta kirjalikke, elektroonilisi või suulisi taotlusi ja kontrollida alles tagantjärele, kas kõik juurdepääsutingimused, kaasa arvatud kiireloomulise erandjuhtumi esinemine, on täidetud. Tagantjärele kontrollimine tehakse pärast taotluse töötlemist tarbetu viivituseta. 3. Lõikes 2 osutatud otsuse kohaselt VISist saadud andmeid ei edastata ega tehta kättesaadavaks kolmandale riigile või rahvusvahelisele organisatsioonile. Kiireloomulisel erandjuhul võib siiski kõnealuseid andmeid edastada või teha kättesaadavaks kolmandale riigile või rahvusvahelisele organisatsioonile eranditult terroriaktide ja teiste raskete kuritegude ärahoidmise ja avastamise eesmärgil ning nimetatud otsuses sätestatud tingimustel. Kooskõlas siseriikliku õigusega tagavad liikmesriigid registri pidamise kõnealuste andmeedastuste kohta ja taotluse alusel sellega tutvumise liikmesriikide

		andmekaitseasutuste poolt. Andmete edastamisele VISi andmed sisestanud liikmesriigi poolt kohaldatakse selle liikmesriigi õigust. 4. Käesolev määrus ei piira artiklis 6 osutatud asutuste poolt siseriikliku õiguse kohaselt ametikohustuste täitmisel avastatud mis tahes kriminaalset tegevust käsitleva teabe edastamist vastutavatele asutustele seonduvate kuritegude ärahoidmise, uurimise ja nende eest süüdimõistmise eesmärgil.

Kokkuvõte:

- Isikuandmete töötlemise üldnõuded süütegude tõkestamisel, uurimisel, avastamisel ja nende eest vastutusele võtmisel reguleerib EL-s õiguskaitseasutuste direktiiv. Direktiiv ei ole otsekohalduv ja selle sätted tuleb üle võtta siseriiklikusse õigusesse.
- Direktiiv lubab süütegude tõkestamisel, uurimisel, avastamisel ja nende eest vastutusele võtmisel biomeetriliste andmete töötlemist, kui täidetud on direktiivis sätestatud tingimused. Konkreetne õiguslik alus biomeetriliste andmete töötlemiseks tuleks sätestada EL-i või liikmesriigi õiguses.
- Liikmesriikide õigusalase koostöö ja teabevahetuse tõhustamine on EL-i pädevuses ning selle raames on EL-i õigusesse üle võetud teatud Prümi lepingu sätted, mis kohustavad riiki tegema kättesaadavaks teatud biomeetrilisi andmeid (sh sõrmejäljed) päringute tegemiseks teistele liikmesriikidele. Andmete kokkulangevuse korral menetlevad riigid andmeid edasi õigusabitaotluse korras.
- Menetluses oleva ECRIS-TCN süsteemi määrus võimaldaks teha päringuid kolmandate riikide kodanike ja kodakondsuseta isikute süüdimõistvate kohtuotsuste kohta EL-i liikmesriikides. Sarnaselt Prümi süsteemile põhineks andmete kokkulangevuse (vastava kohtuotsuse teinud liikmesriigi tuvastamisel) korral riikide vaheline edasine koostöö ECRIS-e raamistikul, s.t. süsteem üksnes võimaldab tuvastada riigi, kellega teha edasist koostööd karistusregistri andmete väljastamiseks.
- Erandlikel juhtudel on liikmesriikidel õigus saada EL-i kesksetest andmebaasidest ja süsteemidest andmeid kui see on vajalik terroriaktide või raskete kuritegude menetlemiseks. Konkreetne õiguslik alus ja tingimused selliste andmete saamiseks ja töötlemiseks on toodud vastavat andmebaasi reguleerivas EL-i õigusaktis.

Õiguskaitseasutuste direktiivi, Prümi lepinguga, seda inkorporeerivate jt EL-i õigusaktidega on sätestatud, millal liikmesriigid võivad ja peavad biomeetrilisi andmeid töötlema terrorismi ja kuritegude uurimiseks, avastamiseks ja ennetamiseks.

6.6.1. Õiguskaitseasutuste direktiiv

Õiguskaitseasutuste direktiiv sätestab reeglid füüsiliste isikute kaitset isikuandmete töötlemisel pädevate asutuste poolt süütegude tõkestamiseks, uurimiseks, avastamiseks, nende eest vastutusele võtmiseks või kriminaalkaristuste täitmisele pööramiseks, sealhulgas avalikku

julgeolekut ähvardavate ohtude eest kaitsmiseks ja nende ennetamiseks[99]. Nimetatud direktiiv ja selle sätted tuleb liikmesriigil üle võtta siseriiklikkusse õigusesse. Direktiivi ei kohaldata valdkondades, mis ei kuulu EL-i pädevusse (nt riiklik julgeolek).

(a) Õiguslik alus

Õiguslik alus isikuandmete töötlemiseks sätestatakse liikmesriigi siseriiklikus õiguses. Kuna nõusolek ei pruugi sellises andmetöötluse kontekstis olla sobiv õiguslik alus (vt lk 24), tuleks õiguslik alus luua seadusega. Kooskõlas direktiiviga peaks isikuandmete töötlemine olema lubatud seaduse alusel, kui nende töötlemine on vajalik süütegude tõkestamise, avastamise, menetlemise või karistuste täideviimise eesmärgist tuleneva ülesande täitmiseks.

Kui isikuandmete kaitse üldmäärusega peaks eriliigiliste andmete (sh biomeetriliste andmete) töötlemine üldjuhul olema keelatud, siis õiguskaitseasutuste tegevuse konteksti arvestades ei ole sellist keeldu praktikas võimalik rakendada. Seetõttu sätestab õiguskaitseasutuste direktiiv, et eriliigiliste andmete töötlemine on lubatud, kuid üksnes siis, kui see on rangelt vajalik, sellele kohaldatakse andmesubjekti õiguste ja vabaduste kaitsmiseks asjakohaseid kaitsemeetmeid ning üksnes järgmistel juhtudel:

a. see on lubatud liidu või liikmesriigi õigusega;

b. et kaitsta andmesubjekti või teise füüsilise isiku elulisi huve või

c. selliselt töödeldakse isikuandmeid, mille andmesubjekt on ilmselgelt avalikustanud.

Kuna eriliigiliste andmete töötlemiseks on siiski vaja selget õiguslikku alust, peab selline õiguslik alus olema kehtestatud EL-i või liikmesriigi õiguses. Näiteks EL-i õigusaktides on sätestatud VIS-süsteemist saadud andmete töötlemise õiguslik alus olukorras, kus esineb kiireloomuline erandjuht terroriaktide ja muude raskete kuritegude vältimise, avastamise ja uurimise eesmärkidel (ning täidetud on muud õigusaktis toodud eeldused)[100].

(b) Tingimused

Direktiivis toodud tingimused isikuandmete töötlemisele on analoogsed isikuandmete üldmääruses toodud tingimustega (nt seaduslikkuse, eesmärgipärasuse, õigusliku aluse, säilitamise jms põhimõtted).[101] Õiguskaitseasutuste direktiivi eesmärkidel pädevate asutuste poolt kogutavaid isikuandmeid ei tohi töödelda muudel kui ainult nendel eesmärkidel, välja arvatud juhul, kui selline töötlemine on lubatud liidu või liikmesriigi õigusega. Kui isikuandmeid töödeldakse sellistel muudel eesmärkidel, kohaldatakse isikuandmete kaitse üldmäärust, välja arvatud juhul, kui isikuandmeid töödeldakse tegevuse käigus, mis ei kuulu liidu õiguse kohaldamisalasse.

Kui liikmesriigi õigusega on pädevatele asutustele antud muud ülesanded kui need, mida täidetakse süütegude tõkestamise, uurimise, avastamise, nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärkidel, kohaldatakse sellistel eesmärkidel isikuandmete töötlemisele (sealhulgas avalikes huvides arhiveerimise, teadusliku või ajaloolise uurimistöö või statistika tarvis) isikuandmete kaitse üldmäärust, välja arvatud juhul, kui isikuandmeid töödeldakse tegevuse käigus, mis ei kuulu EL õiguse kohaldamisalasse.

6.6.2. Prümi leping

[99] Õiguskaitseasutuste direktiiv art 1(1)

[100] Nõukogu otsus 2008/633/JSK

[101] *Ibid*, art 4

Prümi lepingu eesmärk on tõhustada piiriülest koostööd terrorismi-, piiriülese kuritegevuse ja ebaseadusliku rände vastases võitluses. Lepingu osapooled on Austria, Belgia, Bulgaaria, Eesti, Soome, Prantsusmaa, Saksamaa, Ungari, Luksemburg, Holland, Rumeenia, Slovakkia, Sloveenia ja Hispaania. Prümi lepingu sätete sisu on inkorporeeritud EL-i õigusraamistikku läbi nõukogu otsuse 2008/615/JSK, mis kohaldub kõikidele EL-i liikmesriikidele. Nende eesmärgiks on eelkõige piiriülese koostöö tõhustamine, sh teabevahetus kuritegude ärahoidmise ja uurimise eest vastutavate asutuste vahel.

(a) Õiguslik alus

Riigil on kohustus tagada automatiseeritud identifitseerimise registris viiteandmete olemasolu (sh biomeetrilised andmed)[102]. Samuti peavad riigid tagama teistele riikidele juurdepääsu viiteandmetele koos õigusega teha sõrmejälgede andmeid võrreldes automatiseeritud otsinguid[103]. Seega on selles ulatuses biomeetriliste andmete töötlemine riigile kohustuslik ning õiguslik alus selleks töötlemiseks tuleneb Eestile Prümi lepingut inkorporeerivast otsusest.

(b) Tingimused

Riikide kohustused isikuandmete kaitse tagamisel on järgmised:

a. tuleb tagada isikuandmete õigsus ja asjakohasus[104];
b. tuleb kasutusele võtta asjakohased tehnilised ja korralduslikud meetmed[105];
c. registrit haldav asutuse ja otsingut tegev asutuse kohustus logida kõik isikuandmete edastused ja kättesaamised[106].

Otsus sätestab eeskirjad mh sõrmejälgede andmete automatiseeritud edastamiseks. Selleks peavad liikmesriigid tagama, et siseriiklikus sõrmejälgede automatiseeritud identifitseerimise süsteemi registris on saadaval viiteandmed, mille hulka kuuluvad sõrmejälgede andmed ja viitenumber (s.t. need ei sisalda andmeid, mille abil saab andmesubjekti otseselt kindlaks teha). Kui tehtud päringu pinnalt esineb sõrmejälgede kokkulangevus, koostab päringut tegev riik õigusabitaotluse, mille suhtes kohaldatakse taotluse saanud riigi siseriiklikku õigust.

Üldjuhul lubatakse *otsingut sooritavatel või andmeid võrdlevatel* liikmesriikidel töödelda sõrmejälje andmeid üksnes selleks, et:

1. kindlaks teha, kas võrreldavad sõrmejälje andmed on omavahel kokkulangevad;
2. nende andmete omavahelise kokkulangevuse korral koostada ja esitada kooskõlas siseriikliku õigusega politsei- või õigusasutuste õigusabitaotlus;
3. salvestada edastatavad andmed; andmeedastuse kuupäev ja täpne aeg ning otsingut sooritava organi ja registrit haldava organi nimi või viitekood.

Registrit haldav liikmesriik võib talle edastatud andmeid (s.t. päringu tegemiseks saadetud andmeid) töödelda vaid juhul, kui see on vajalik võrdlemiseks, otsingutele automaatvastuse saatmiseks või salvestamiseks vastavalt otsusele 2005/615/JSK.

Andmete edasine töötlemine ei ole üldjuhul lubatud ning andmed tuleb koheselt pärast võrdlemist või otsingule vastuse saamist kustutada, v.a. juhul kui see on vajalik õigusabitaotluse esitamiseks või nõutud logimiseks/salvestamiseks.

[102] Prümi lepingu art 8

[103] *Ibid*, art 9

[104] *Ibid*, art 37

[105] *Ibid*, art 38

[106] *Ibid*, art 39

Lisaks eelnevale täpsustab nõukogu otsus 2008/616/JSK Prümi lepingu kontekstis piiriülese koostöö toimimist halduslikest ja tehnilistest aspektidest.

6.6.3. EL-i kesksetest andmebaasidest saadud andmete töötlemine süütegude menetlustes

Lisaks eeltoodud mehhanismidele on liikmesriikidel võimalik õiguskaitse eesmärkidel töödelda EL-i kesksetest andmebaasidest saada teatud andmeid (sh nendes andmebaasides salvestatud biomeetrilisi andmeid). Sellise töötlemise õiguslik alus ja tingimused tulenevad konkreetset andmebaasi reguleerivast määrusest või muudest õigusaktidest (nt nõukogu otsus 2008/633/JSK, mis käsitleb juurdepääsu VIS-süsteemile terroriaktide ja muude raskete kuritegude vältimise, avastamise ja uurimise eesmärkidel; Eurodac määrus).

6.6.4. ECRIS-TCN kesksüsteem nende liikmesriikide väljaselgitamiseks, kellel on teavet kolmandate riikide kodanike ja kodakondsuseta isikute suhtes tehtud süüdimõistvate kohtuotsuste kohta (ettepanek)

Hetkel on menetluses Euroopa Parlamendi ja nõukogu määrus, mis looks EL-i tasandil kesksüsteemi, kus talletatakse kolmandate riikide kodanike ja kodakondsuseta isikute isikuandmed, kelle suhtes on EL-i territooriumil asuv kriminaalkohus teinud süüdimõistva kohtuotsuse.[107] Need isikuandmed sisaldaksid tähtnumbrilisi andmeid, isiku sõrmejälgede andmeid ja näokujutist (kui see on liikmesriigi karistusregistris talletatud).

(a) Õiguslik alus

Vastavalt määruse ettepanekule oleks liikmesriikidel kohustus tagada riikliku karistusregistri ja sõrmejäljeandmebaasi vaheline ühendus[108]. Samuti on kohustus saadud teabepäringute puhul kasutada ECRIS-TCN süsteemi ning võtta päringutabamuse osas meetmeid selle süsteemi kaudu välja selgitatud liikmesriikidega.[109] Seega oleks määruse vastuvõtmisel nimetatud süsteemis andmete töötlemine liikmesriigile kohustuslik.

(b) Tingimused

Andmeid töödeldakse süsteemis selleks, et teada saada, millises liikmesriigis süüdimõistev kohtuotsus on tehtud. Päringutabamuse korral teatab kesksüsteem automaatselt, millisel liikmesriigil või liikmesriikidel on isiku kohta karistusregistriandmeid, lisades ka seotud viitenumbri ja mis tahes vastavad isikuandmed. Neid isikuandmeid võib kasutada üksnes selle isiku isikusamasuse kontrollimiseks. Kui päringutabamus on kinnitatud, kasutatakse olemasolevat ECRIS-e raamistikku, et taotleda vastavalt liikmesriigilt karistusregistriandmeid vastavalt raamotsusele 2009/315/JSK, mis käsitleb karistusregistrite andmete vahetamise liikmesriikidevahelist korraldust ja andmete sisu [110].

6.7. SIS II-ga, VIS-iga ja koostalitusvõimega seotud algatused

Hetkel on EL-i tasandil menetluses ka algatused, mis peaksid muutma olemasolevad EL-i infosüsteemid tõhusamaks läbi olemasolevate lünkade ületamise ning koostalitlusvõime loomise. Antud algatusi oleme võimalike muudatuste valguses käesoleva analüüsi raames

[107] 2017/0144(COD) pp 11

[108] *Ibid*, art 12

[109] *Ibid*, pp 18

[110] *Ibid*, pp 7

käsitlenud üldiselt, sest analüüsi valmimise hetkeks ei ole need dokumendid veel vastu võetud ning nendes sätestatud tingimused ei loo riigile õiguslikke kohustusi.

Koostalitusvõime loob seejuures võimaluse pärida andmeid EL-i süsteemidest mis tahes menetluste raames (sh viisamenetlus, varjupaigamenetlus jms). Ettepaneku kohaldamisala hõlmab SIS, Eurodac, VIS, EES, ETIAS ja ECRIS-TCN süsteemi. See aga ei tähenda, et liikmesriigi asutused saavad valimatult ligi kõigile koostalitusvõime raamistikku hõlmatud andmebaasidele. Ligipääsuõiguste juures jäävad kehtima hetkel juurutatud põhimõtted – kasutaja pääseb juurde süsteemide nendele andmetele, millele tal on seadusest tulenev juurdepääs.

Lisaks on andmebaasidega seotud reform puudutamas ka andmebaase individuaalselt – nt on SIS II puudutava algatuse eesmärk tagada mh võitlus terrorismi ja piiriülese kuritegevusega. Ühelt poolt olemasolevate süsteemide tõhusam kasutamine, kuid samal ajal rõhutatakse vajadust järgida andmete kogumise ja töötlemise osas EL-i ja siseriiklikke isikuandmete kaitset reguleerivaid õigusakte. SIS II osas on hetkel menetluses vastavalt valdkonnale kolm algatust: riigipiiri ületamise kontrolli valdkonda käsitleva SIS-i määrus[111], õiguskaitse valdkonda käsitleva SIS-i määrus[112] ja ebaseaduslikku tagasipöördumist käsitleva SIS-i määrus[113].

Lisaks on menetluses ka VIS-süsteemiga seotud muudatused[114], millega nähakse ette menetlused teabevahetuseks liikmesriikide vahel seoses pikaajaliste viisade ja elamislubadega, mh hõlbustatakse viisamenetlust, piirikontrolli, tagatakse isikute õige tuvastamine jms. Näiteks alandatakse lastelt sõrmejälgede võtmise alampiiri 6-aastale, sätestatakse reisidokumendi biograafilise andmetega lehekülje koopia salvestamine VIS-s, võimaluse võrrelda latentseid sõrmejälgi VISis salvestatud sõrmejälgedega juhtudel, kui on piisavalt alust arvata, et kuriteo toimepanija või ohver võib olla VISis registreeritud.

Samuti on esitatud algatus EL-i infosüsteemide koostalitlusvõimet reguleeriva raamistiku kehtestamiseks ning Euroopa otsinguportaali loomiseks.[115] Koostalituse üheks komponendiks on ka ühine biomeetriline võrdlemise teenus ning mitme identiteedi detektor. Ühine biomeetrilise võrdlemise teenus võimaldab leida seoseid sama isiku kohta eri süsteemidesse salvestatud andmekogumite ja eri identiteetide vahel. Euroopa otsinguportaal võimaldaks samaaegselt teha päringuid mitmes EL-i süsteemis kasutades selleks identiteediandmeid (sh biomeetrilisi andmeid).

[111] RAPORT ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse Schengeni infosüsteemi (SIS) loomist, toimimist ja kasutamist riigipiiri ületamise kontrolli valdkonnas ning millega muudetakse määrust (EL) nr 515/2014 ja tunnistatakse kehtetuks määrus (EÜ) nr 1987/2006 (COM(2016)0882 – C8-0533/2017 – 2016/0408(COD))

[112] RAPORT ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse Schengeni infosüsteemi (SIS) loomist, toimimist ja kasutamist politseikoostöös ja kriminaalasjades tehtavas õigusalases koostöös ning millega muudetakse määrust (EL) nr 515/2014 ja tunnistatakse kehtetuks määrus (EÜ) nr 1986/2006, nõukogu otsus 2007/533/JSK ja komisjoni otsus 2010/261/EL (COM(2016)0883 – C8-0530/2016 – 2016/0409(COD))

[113] RAPORT ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus Schengeni infosüsteemi kasutamise kohta ebaseaduslikult riigis viibivate kolmandate riikide kodanike tagasisaatmiseks (COM(2016)0881 – C8-0532/2016 – 2016/0407(COD))

[114] Ettepanek 2018/0152 (COD)

[115] Ettepanek 2017/0352(COD)

7. BIOMEETRILISTE ANDMETE RISTKASUTUS

7.1. Ristkasutusest üldiselt

Andmete ristkasutuse mõistel puudub legaaldefinitsioon. Sisuliselt on tegemist andmete edasise töötlemisega, mille eesmärk võib erineda andmete kogumise algsest eesmärgist. Teisisõnu tähistab see olukorda, kus isikuandmeid kogutakse ühel eesmärgil, kuid hiljem kasutatakse ka teistel eesmärkidel, sh võidakse edastada kolmandatele isikutele, kes algses andmetöötluse protsessis ei osalenud. Andmete ristkasutus on atraktiivne kontseptsioon, sest võimaldab ära kasutada ära juba olemasolevaid ressursse (andmeid) ning vältida andmete dubleerimist.

Siiski eeldab ka andmete edasine kasutamine õigusliku aluse olemasolu konkreetse töötlemistegevuse ehk edasise töötlemise jaoks. Tulenevalt eesmärgipärasuse printsiibist ei saa andmeid kasutada viisil, mis ei vasta andmete kogumisele algsele eesmärgile. Seega peavad andmete töötlemise eesmärgid olema selgelt sõnastatud ning töötlemistegevused, mis sellele eesmärgile ei vasta, vajavad omaette õiguslikku alust.

Eesti e-riigi lahenduses, kus erinevad andmed kogutakse erinevates andmekogudesse, on andmete ristkasutus oluline teema, sest võimaldab vältida andmete dubleerimist. ABIS-e süsteemi kontekstis on oluline küsimus, kas ja millisel viisil saab erinevatest andmebaasidest ja andmekogudest pärinevaid andmeid kasutada. Käesolevas peatükis oleme analüüsinud andmete ristkasutamise lubatavust erinevatest aspektidest vastavalt tellija sõnastatud eesmärkidele. Peatükk analüüsib ristkasutatavuse võimalikkust üldiselt, samuti konkreetsete avalik-õiguslike menetluste vahel (tulenevalt EL-i õigusest) ning eraõiguslikes suhetes.

7.1.1. Rahvusvaheline õigus

Õigusakt	**Säte**	**Sisu**
Konventsioon 108+	Artikkel 5 (4) (b)	4. Töödeldavad isikuandmed peavad olema: b. kogutud selgesõnalisel, konkreetsel ja õigustatud eesmärgil ning mitte olla töödeldud nende eesmärkidega mittesobival eesmärgil; edasine töötlemine arhiveerimise eesmärgil avalikes huvides, teadusliku või ajaloolise uurimuse eesmärgil või statistilisel eesmärgil peab olema teostatud asjakohaste kaitsemeetmete abil, mis vastavad nendele eesmärkidele.

Kokkuvõte:

- Rahvusvaheline õigus ei keela andmete edasist kasutamist (sh ristkasutamist). Andmete edasise kasutamise olulisim nõue on eesmärgipärasus, s.t. andmeid tohib töödelda selle algselt sõnastatud eesmärgil või, kui töötlemine ei vasta sellele eesmärgile, peab edasiseks töötlemiseks olema iseseisev õiguslik alus.
- Andmete kasutamine avalikes huvides teaduse, ajaloo või statistika eesmärkidel on kooskõlas andmete esialgse töötlemise eesmärgiga kui rakendatakse asjakohaseid

	kaitsemeetmeid (nt anonüümiseerimine), s.t. sellel eesmärgil andmete edasine töötlemine ei vaja täiendavat õiguslikku alust.

Rahvusvahelise õiguse õigusaktid ei ole üldjuhul reguleerinud spetsiifiliselt andmete ristkasutuse küsimust. Konventsiooni 108+ sõnastuses on andmete ristkasutusest konkreetsemalt räägitud. Nimelt lubab Konventsioon 108+ andmete edasist töötlemist konkreetsetel eesmärkidel ning eeldusel, et rakendatakse asjakohaseid kaitsemeetmeid. Näiteks lubab Konventsioon 108+ andmete edasist kasutamist avalikes huvides teaduse, ajaloo või statistika eesmärkidel isegi juhul kui see ei lange selgelt kokku andmete algse kogumise eesmärgiga (töötlemine algse eesmärgiga erineval eesmärgil on piiratud nimetatud teaduse, ajaloo või statistika eesmärkidega). Artiklis 5(4)(b) loetletud edasist töötlemist peetakse *a priori* kooskõlas algse eesmärgiga kui kohaldatakse vastavaid kaitsemeetmeid (nt andmete anonüümseks muutmine).[116]

Kooskõla algse eesmärgiga ei tohi mõjutada andmete töötlemise läbipaistvust, õiguskindlust, ettenähtavust ega ausust. Andmeid ei või töödelda viisil, mida andmesubjekt võiks pidada ootamatuks, sobimatuks või muul viisil vastuvõetamatuks. Statistilistel eesmärkidel töötlemisel võivad andmesubjekti õigused olla piiratud, eeldusel, et andmesubjekti õigustele ja vabadustele ei ole märgatavat riski.

Niisiis ei keela rahvusvaheline õigus printsiibis isikuandmete ristkasutamist. Ristkasutuse eesmärk peaks seejuures olema selgelt määratud, s.t. eesmärk ei tohiks olla defineerimata, ebatäpne või liiga üldsõnaline[117].

7.1.2. Euroopa Liidu õigus

Õigusakt	Säte	Sõnastus
Isikuandmete kaitse üldmäärus	Põhjenduspunkt 50	Isikuandmete töötlemine muudel eesmärgil kui need, milleks isikuandmed algselt koguti, peaks olema lubatud üksnes juhul, kui töötlemine on kooskõlas eesmärkidega, mille jaoks isikuandmed algselt koguti. Sellisel juhul ei ole nõutav, et õiguslik alus oleks erinev õiguslikust alusest, mis võimaldas isikuandmete kogumist. Kui töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks, võib liidu või liikmesriigi õiguses kindlaks määrata ja täpsustada need ülesanded ja eesmärgid, mille puhul tuleks pidada edasist töötlemist eesmärkidele vastavaks ja seaduslikuks. Edasist töötlemist avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgil tuleks käsitada eesmärkidele vastavate seaduslike isikuandmete töötlemise toimingutena. Liidu või liikmesriigi

[116] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. pp 50

[117] *Ibid*, pp 48

		õiguses sätestatud õiguslik alus isikuandmete töötlemiseks võib olla ka edasise töötlemise õiguslikuks aluseks. Selleks et teha kindlaks, kas edasise töötlemise eesmärk vastab eesmärgile, mille jaoks isikuandmed algselt koguti, peaks vastutav töötleja võtma pärast kõikide esialgse töötlemise seaduslikkuse seisukohast vajalike nõuete täitmist muu hulgas arvesse mis tahes seoseid sellise eesmärgi ja kavandatava edasise töötlemise eesmärgi vahel, isikuandmete kogumise konteksti, eelkõige andmesubjekti ja vastutava töötleja vahelisel suhtel põhinevaid andmesubjekti mõistlikke ootusi andmete edasise kasutamise suhtes, isikuandmete laadi, kavandatava edasise töötlemise tagajärgi andmesubjekti jaoks ning asjakohaste kaitsemeetmete olemasolu nii esialgsetes kui ka kavandatavates edasistes isikuandmete töötlemise toimingutes. Kui andmesubjekt on andnud nõusoleku või kui töötlemine põhineb liidu või liikmesriigi õigusel, mis on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede, millega kaitsta eelkõige üldist avalikku huvi pakkuvaid olulisi eesmärke, peaks vastutaval töötlejal olema lubatud isikuandmeid edasi töödelda, olenemata eesmärkidele vastavusest. Igal juhul tuleks tagada käesolevas määruses sätestatud põhimõtete kohaldamine ja eelkõige andmesubjekti teavitamine kõnealustest muudest eesmärkidest ja tema õigustest, sealhulgas õigusest esitada vastuväiteid. Seda, et vastutav töötleja teatab võimalikest süütegudest või avalikku julgeolekut ähvardavatest ohtudest ning edastab sama kuriteoga või avalikku julgeolekut ähvardavate ohtudega seotud üksikjuhtumi või mitme juhtumi korral asjakohased isikuandmed pädevale asutusele, tuleks pidada vastutava töötleja õigustatud huvides olevaks. Selline edastamine vastutava töötleja õigustatud huvides või isikuandmete edasine töötlemine peaks aga olema keelatud, kui töötlemine ei ühildu õigusliku, kutsealase või muu siduva saladuste hoidmise kohustusega.
	Artikkel 6 (3)	Lõike 1 punktides c ja e osutatud isikuandmete töötlemise alus kehtestatakse: a) liidu õigusega või b) vastutava töötleja suhtes kohaldatava liikmesriigi õigusega. Isikuandmete töötlemise eesmärk määratakse kindlaks selles õiguslikus aluses või see on lõike

		1 punktis e osutatud isikuandmete töötlemise osas vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks. See õiguslik alus võib sisaldada erisätteid, et kohandada käesoleva määruse sätete kohaldamist, sealhulgas üldtingimusi, mis reguleerivad vastutava töötleja poolt isikuandmete töötlemise seaduslikkust, töötlemisele kuuluvate andmete liiki, asjaomaseid andmesubjekte, üksuseid, kellele võib isikuandmeid avaldada, ja avaldamise põhjuseid, eesmärgi piirangut, säilitamise aega ning isikuandmete töötlemise toiminguid ja -menetlusi, sealhulgas meetmeid seadusliku ja õiglase töötlemise tagamiseks, nagu näiteks meetmed teiste andmetöötluse eriolukordade jaoks, nagu need on sätestatud IX peatükis. Liidu või liikmesriigi õigus vastab avaliku huvi eesmärgile ning on proportsionaalne taotletava õiguspärase eesmärgiga.
	Artikkel 6 (4)	Kui isikuandmete töötlemine muul eesmärgil kui see, milleks isikuandmeid koguti, ei põhine andmesubjekti nõusolekul või liidu või liikmesriigi õigusel, mis on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede, et tagada artikli 23 lõikes 1 osutatud eesmärkide täitmine, võtab vastutav töötleja selle kindlakstegemiseks, kas muul eesmärgil töötlemine on kooskõlas eesmärgiga, mille jaoks isikuandmeid algselt koguti, muu hulgas arvesse a. seost nende eesmärkide, mille jaoks isikuandmeid koguti, ja kavandatava edasise töötlemise eesmärkide vahel; b. isikuandmete kogumise konteksti, eelkõige andmesubjektide ja vastutava töötleja vahelist seost; c. isikuandmete laadi, eelkõige seda, kas töödeldakse isikuandmete eriliike vastavalt artiklile 9 või süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmeid vastavalt artiklile 10; d. kavandatava edasise töötlemise võimalikke tagajärgi andmesubjektide jaoks; e. asjakohaste kaitsemeetmete olemasolu, milleks võivad olla näiteks krüpteerimine ja pseudonümiseerimine.

	Artikkel 9(4)	Liikmesriigid võivad säilitada või kehtestada täiendavad tingimused, sealhulgas piirangud seoses geneetiliste, biomeetriliste või terviseandmete töötlemisega.
Õiguskaitseasutuste direktiiv	Artikkel 9 (1)	1. Artikli 1 lõikes 1 sätestatud eesmärkidel pädevate asutuste poolt kogutavaid isikuandmeid ei tohi töödelda muudel kui artikli 1 lõikes 1 sätestatud eesmärkidel, välja arvatud juhul, kui selline töötlemine on lubatud liidu või liikmesriigi õigusega. Kui isikuandmeid töödeldakse sellistel muudel eesmärkidel, kohaldatakse määrust (EL) 2016/679, välja arvatud juhul, kui isikuandmeid töödeldakse tegevuse käigus, mis ei kuulu liidu õiguse kohaldamisalasse.
	Artikkel 9 (2)	2. Kui liikmesriigi õigusega on pädevatele asutustele antud muud ülesanded kui need, mida täidetakse artikli 1 lõikes 1 sätestatud eesmärkidel, kohaldatakse sellistel eesmärkidel isikuandmete töötlemisele (sealhulgas avalikes huvides arhiveerimise, teadusliku või ajaloolise uurimistöö või statistika tarvis) määrust (EL) 2016/679, välja arvatud juhul, kui isikuandmeid töödeldakse tegevuse käigus, mis ei kuulu liidu õiguse kohaldamisalasse.
	Artikkel 10	Selliste isikuandmete töötlemine, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, ning geneetiliste andmete, füüsilise isiku kordumatuks tuvastamiseks kasutatavate biomeetriliste andmete, tervist või seksuaalelu või seksuaalset sättumust käsitlevate andmete töötlemine on lubatud üksnes siis, kui see on rangelt vajalik, sellele kohaldatakse andmesubjekti õiguste ja vabaduste kaitsmiseks asjakohaseid kaitsemeetmeid ning üksnes järgmistel juhtudel: a. see on lubatud liidu või liikmesriigi õigusega; b. et kaitsta andmesubjekti või teise füüsilise isiku elulisi huve või c. selliselt töödeldakse isikuandmeid, mille andmesubjekt on ilmselgelt avalikustanud.

Kokkuvõte:

- Isikuandmete edasine töötlemine (sh ristkasutus) on lubatud kui töötlemine on kooskõlas eesmärkidega, mille jaoks isikuandmed algselt koguti.
- Kui isikuandmeid töödeldakse eesmärgil ja viisil, mis pole kooskõlas andmete kogumise algse eesmärgiga, peab selliseks edasiseks töötlemiseks olema iseseisev õiguslik alus.
- Pädevate asutuste poolt süütegude tõkestamiseks, uurimiseks, avastamiseks, nende eest vastutusele võtmiseks või kriminaalkaristuste täitmisele pööramiseks kogutud andmeid ei või üldjuhul edasi töödelda. Erandiks on olukord, kus EL-i või liikmesriigi õigus lubab edasist töötlemist. Sel juhul kohaldatakse edasisele töötlemisele isikuandmete kaitse üldmäärust (art 6(4)). Isikuandmete kaitse üldmäärust ei kohaldata, kui isikuandmete töötlemine toimub tegevuse käigus, mis ei ole EL-i õiguse kohaldamisalas (nt riigikaitse, julgeolek).

Ristkasutuse temaatika seondub tihedalt töötlemise seaduslikkuse (ehk õigusliku aluse olemasolu) ning eesmärgi piirangu printsiipidega. EL-i õigusaktid lubavad teatud juhtudel biomeetriliste andmete ristkasutust. Isikuandmete ristkasutuseks peab olema õiguslik alus, kuid kõigi töötlemiseks sobivate õiguslike aluste puhul on oluline analüüsida, kas ristkasutus on *vajalik* eesmärgi saavutamiseks ja kas see on eesmärgiga proportsionaalne. Muuhulgas tuleb silmas pidada, et kui eesmärk on saavutatav vähem riivavate meetmetega, näiteks isikuandmete eriliikide asemel „tavaliste" isikuandmete töötlemisega või isikuandmete töötlemisega vähemal määral (nt 10 sõrmejälje asemel 1-2 sõrmejälge), siis ei ole töötlemine tõenäoliselt vajalik eesmärgi saavutamiseks.

(a) Isikuandmete kaitse üldmäärus

Isikuandmete kaitse üldmäärus näeb ette, et töötlemiseks peab olema õiguslik alus ning et isikuandmeid kogutakse üksnes täpselt ja selgelt kindlaksmääratud õiguspärastel eesmärkidel ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus.[118] Isikuandmete töötlemine muudel eesmärkidel kui need, milleks isikuandmed algselt koguti, peaks olema lubatud üksnes juhul, kui töötlemine on *kooskõlas* eesmärkidega, mille jaoks isikuandmed algselt koguti. Sellisel juhul ei ole nõutav, et õiguslik alus oleks erinev õiguslikust alusest, mis võimaldas isikuandmete kogumist.

Kui töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks, võib liikmesriigi õiguses kindlaks määrata ja täpsustada need ülesanded ja eesmärgid, mille puhul tuleks pidada edasist töötlemist eesmärkidele vastavaks ja seaduslikuks. Liikmesriigi õiguses sätestatud õiguslik alus võib olla ka edasise töötlemise õiguslikuks aluseks.[119] Seejuures on oluline märkida, et lisaks isikuandmete kaitse üldmääruse artiklis 9(2) nimetatud õiguslikele alustele võib liikmesriik kehtestada täiendavaid tingimusi geneetiliste, biomeetriliste või terviseandmete töötlemiseks.[120]

Selleks et teha kindlaks, kas edasise töötlemise eesmärk vastab eesmärgile, mille jaoks isikuandmed algselt koguti, peaks vastutav töötleja võtma pärast kõikide esialgse töötlemise seaduslikkuse seisukohast vajalike nõuete täitmist muu hulgas arvesse mis tahes seoseid sellise

[118] Isikuandmete kaitse üldmäärus, art 5(1)(d), (a), (b).

[119] *Ibid*, pp 50.

[120] *Ibid*, art 9(4)

eesmärgi ja kavandatava edasise töötlemise eesmärgi vahel, isikuandmete kogumise konteksti, eelkõige andmesubjekti ja vastutava töötleja vahelisel suhtel põhinevaid andmesubjekti mõistlikke ootusi andmete edasise kasutamise suhtes, isikuandmete laadi, kavandatava edasise töötlemise tagajärgi andmesubjekti jaoks ning asjakohaste kaitsemeetmete olemasolu nii esialgsetes kui ka kavandatavates edasistes isikuandmete töötlemise toimingutes.[121]

Kui aga andmesubjekt on andnud nõusoleku[122] või kui töötlemine põhineb liidu või liikmesriigi õigusel, mis on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede, millega kaitsta eelkõige üldist avalikku huvi pakkuvaid olulisi eesmärke, peaks vastutaval töötlejal olema lubatud isikuandmeid edasi töödelda, olenemata esialgsele isikuandmete töötlemise eesmärgile vastavusest. Igal juhul tuleks tagada isikuandmete kaitse üldmääruses sätestatud põhimõtete kohaldamine ja eelkõige andmesubjekti teavitamine kõnealustest muudest eesmärkidest ja tema õigustest, sealhulgas õigusest esitada vastuväiteid. Seda, et vastutav töötleja teatab võimalikest süütegudest või avalikku julgeolekut ähvardavatest ohtudest ning edastab sama kuriteoga või avalikku julgeolekut ähvardavate ohtudega seotud üksikjuhtumi või mitme juhtumi korral asjakohased isikuandmed pädevale asutusele, tuleks pidada vastutava töötleja õigustatud huvides olevaks. Selline edastamine vastutava töötleja õigustatud huvides või isikuandmete edasine töötlemine peaks aga olema keelatud, kui töötlemine ei ühildu õigusliku, kutsealase või muu siduva saladuste hoidmise kohustusega.[123]

Kui EL või liikmesriik annab ristkasutuseks õigusliku aluse, peaks see õiguslik alus kindlaks määrama isikuandmete töötlemise eesmärgi, vastama avaliku huvi eesmärgile (nimetatud isikuandmete kaitse üldmääruse art 23(1)) ning olema proportsionaalne taotletava õiguspärase eesmärgiga. See õiguslik alus võib sisaldada erisätteid, et kohandada üldmääruse sätete kohaldamist, sealhulgas üldtingimusi, mis reguleerivad vastutava töötleja poolt isikuandmete töötlemise seaduslikkust, töötlemisele kuuluvate andmete liiki, asjaomaseid andmesubjekte, üksuseid, kellele võib isikuandmeid avaldada, ja avaldamise põhjuseid, eesmärgi piirangut, säilitamise aega ning isikuandmete töötlemise toiminguid ja -menetlusi, sealhulgas meetmeid seadusliku ja õiglase töötlemise tagamiseks.[124]

(b) Õiguskaitseasutuste direktiiv

Ristkasutus on õiguskaitseasutuste direktiivi alusel lubatud, kui:

a. Selline töötlemine on kooskõlas eesmärkidega, mille jaoks isikuandmed algselt koguti (s.t. vastavalt art 1(1) pädevate asutuste poolt süütegude tõkestamiseks, uurimiseks, avastamiseks, nende eest vastutusele võtmiseks või kriminaalkaristuste täitmisele pööramiseks, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmiseks ja nende ennetamiseks);

b. Töötlemine toimub muul õiguskaitseasutuste direktiivi art 1(1) nimetatud eesmärgil kui eesmärk, milleks isikuandmed algselt koguti ja vastutav töötleja on volitatud töötlema selliseid isikuandmeid kooskõlas liidu või liikmesriigi õigusega ja töötlemine on vajalik ja proportsionaalne kõnealuse muu eesmärgiga;

c. Töötlemine toimub muul (õiguskaitseasutuste direktiivi art 1(1) nimetamata) eesmärgil kui eesmärk, milleks isikuandmeid algselt koguti, kui töötlemine on lubatud liidu või

[121] Isikuandmete kaitse üldmäärus art 6(4), pp 50.

[122] Nõusolek ABIS-e süsteemi kontekstis on problemaatiline, vt lk 23

[123] Isikuandmete kaitse üldmäärus pp 50.

[124] *Ibid*, art 6(4), pp 45.

liikmesriigi õigusega ja on kooskõlas isikuandmete kaitse üldmäärusega (v.a. juhul, kui töödeldakse tegevuse käigus, mis ei kuulu EL-i õiguse kohaldamisalasse).

Isikuandmete töötlemine muul süütegude tõkestamise, uurimise, avastamise, nende eest vastutusele võtmise või kriminaalkaristuse täitmisele pööramise, sh avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamisega seotud eesmärgil kui eesmärk, milleks isikuandmeid kogutakse, on lubatud niivõrd, kuivõrd vastutav töötleja on volitatud töötlema selliseid isikuandmeid sellisel eesmärgil kooskõlas liidu või liikmesriigi õigusega ning isikuandmete töötlemine on vajalik ja proportsionaalne kõnealuse muu eesmärgiga.[125] Eelnimetatud eesmärkidel kogutavaid isikuandmeid ei tohi töödelda muudel kui eelnimetatud eesmärkidel, v.a. juhul, kui töötlemine on lubatud liidu või liikmesriigi õigusega. Kui isikuandmeid töödeldakse sellistel muudel eesmärkidel, kohaldatakse isikuandmete kaitse üldmäärust, v.a. juhul, kui isikuandmeid töödeldakse tegevuste käigus, mis ei kuulu liidu õiguse kohaldamisalasse.[126] Nimetatud põhimõtted võetakse Eesti õigusesse eelduslikult üle isikuandmete kaitse seadusega (§ 15), mille eelnõu on käesoleva analüüsi esitamise hetkel Riigikogu menetluses.[127]

Selline liikmesriigi õigus ei pea õiguskaitseasutuste direktiivi kohaselt tingimata olema parlamendi poolt vastu võetud seadusandlik akt. Küll aga on Eesti siseriiklik õigus (isikuandmete kaitse seaduse praegune versioon kui ka menetluses olev eelnõu) täpsustanud, et selline õiguslik alus saab tulla seadusest (s.t. nt ministri määrus ei ole piisav). Liikmesriigi õigus, õiguslik alus või seadusandlik meede peaks siiski olema selge ja täpne ning selle kohaldamine ettenähtav nendele, kelle suhtes seda kohaldatakse. Õiguskaitseasutuste direktiivi kohaldamisalasse kuuluvat isikuandmete töötlemist reguleerivas liikmesriigi õiguses tuleks kindlaks määrata vähemalt isikuandmete töötlemise üldeesmärgid, töödeldavad isikuandmed, töötlemise konkreetsed eesmärgid ning isikuandmete tervikluse ja konfidentsiaalsuse tagamise menetluses ja isikuandmete hävitamist käsitlevad menetlused, mis annaksid piisava tagatise ohu vastu, et isikuandmeid võidakse kuritarvitada või meelevaldselt kasutada.[128]

(c) Kohtupraktika

Kohtupraktikas on isikuandmete ristkasutamise seaduslikkust analüüsitud nt Soomes. Soome halduskohus arutas 2017. aastal kohtuasja, kus kaebaja polnud nõustunud sellega, et tema sõrmejälgi ei hoita mitte üksnes passi kiibis, vaid ka passide registris. Sellest registrist võimaldavad Soome seadused saada politseil informatsiooni selleks, et identifitseerida kuriteo või loodus- vm õnnetuse ohver, kui ohvrit pole võimalik kindlaks teha muul moel. Passide registrist saadud sõrmejälje koopia tuleb kustutada kohe kui võrdlus on tehtud. Sellises olukorras leidis Soome halduskohus, et piirangud isikuandmete kaitse õigusele on sellisel juhul piisavalt täpselt määratletud ja kirjeldatud ning need on kooskõlas Euroopa Liidu põhiõiguste hartaga, EIÕK-ga ning Soome konstitutsiooniga.[129] Seega jaatas halduskohus õigust hoida sõrmejälgi lisaks passile ka passide registris ja töödelda neid muul eesmärgil kui üksnes dokumendi väljaandmine.

---

[125] Õiguskaitseasutuste direktiivi art 4(2)

[126] Õiguskaitseasutuste direktiivi art 9(1) ja 9(2).

[127] Eelnõu on kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/5c9f8086-b465-4067-841e-41e7df3b95af/Isikuandmete%20kaitse%20seadus (19.11.2018)

[128] Õiguskaitseasutuste direktiiv, pp33.

[129] Kokkuvõte kohtuasjast kättesaadav: http://fra.europa.eu/en/caselaw-reference/finland-supreme-administrative-court-38722017-3736315 (19.11.2018)

Ka Euroopa kohus on jaatanud teatud tingimustel ristkasutuse lubatavust. Liidetud kohtuasjades C-446/12-C-449/12 lahendas kohus vaidlust, mis oli tekkinud olukorras, kus Hollandi õigusega nähti ette, et passide väljaandmiseks kogutud sõrmejälgi hoitakse nn keskregistris ning neid võib kasutada riikliku julgeoleku, kuritegevuse ennetamise ja kuriteo ohvrite identifitseerimise eesmärkidel. Kaebajad taotlesid passe, kuid keeldusid sõrmejälgi andmast, leides, et tegemist on ülemäärase privaatsuse riivega.

Kohus leidis, et määruse nr 2252/2004 liikmesriikide poolt väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta artikli 4(3) tuleb tõlgendada nii, et see ei kohusta liikmesriike oma õigusaktides tagama, et nimetatud määruse kohaselt kogutud ja salvestatud biomeetrilisi andmeid ei koguta, töödelda ega kasutata muul otstarbel kui passi või reisidokumendi väljaandmiseks, sest see aspekt ei kuulu määruse kohaldamisalasse. Eeltoodud kaalutlused ei takista siseriiklikul kohtul vajaduse korral kontrollida, kas kõik biomeetriliste andmete kasutamise ja säilitamisega seotud siseriiklikud meetmed on kooskõlas siseriikliku õigusega ning EIÕK-ga. Kohus ei andnud täpsemat hinnangut Hollandi siseriiklikule õigusele.[130]

7.2. Ristkasutus isiku tuvastamiseks ja isikusamasuse kontrollimiseks erinevate avalik-õiguslike menetluste käigus

Isikuandmete töötlemiseks (sh ristkasutamiseks) peab olema õiguslik alus, mis on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede, millega kaitsta eelkõige üldist avalikku huvi pakkuvaid olulisi eesmärke. Kuna nõusolek ei saa olla avalik-õiguslikes menetluses sobivaks õiguslikuks aluseks (vt lk 24), peab õiguslik alus tulenema seadusest. On oluline märkida, et EL õigus ei reguleeri isikuandmete töötlemist siseriiklikes andmebaasides ega nendes ja nende vahel toimuvat andmete ristkasutust. EL-i pädevuses on ristkasutus EL-i andmebaaside vahel (nt SIS II ja VIS-süsteem).

Siseriiklikult ristkasutuse õigusliku aluse loomisel läbi teha nn kaalumistest, et kontrollida, kas õiguslik alus vastab isikuandmete kaitse üldmääruse art 6(4) tingimustele. Sõltumata asjaolust, et EL siseriiklike andmebaasidega seonduvat ei reguleeri, peab nendes ja nende vahel toimuv isikuandmete töötlemine siiski vastama isikuandmete töötlemise nõuetele, ah nendele, mis võivad tuleneda EL-i õigusaktidest.

Isiku tuvastamine ja isikusamasuse kontroll toimub EL-i õigusaktide kohaselt peaasjalikult a) dokumentide põhjal (pass, reisidokument, elamisluba jms); b) andmebaasides olevate andmete põhjal (VIS, EES, Eurodac). Kuna isiku dokumenti saab kontrollida vahetult või siseriiklike andmekogude põhjal (puudub keskne EL-i andmebaas), siis küsimus on eelkõige selles, kas ja kuidas saab riik ühe avalik-õigusliku menetluse käigus EL-i andmebaasist saadud ja töödeldud andmeid töödelda teise avalik-õigusliku menetluse raames.

Kokkuvõte:

- Biomeetriliste andmete töötlemine isiku tuvastamiseks ja isikusamasuse tuvastamiseks avalik-õiguslike menetluste raames on EL-i õiguse tasandil reguleeritud selliste menetluste raames, mis on EL-i pädevuses (nt illegaalimenetlus, piiriületuse menetlus, viisamenetlus).
- EL-i andmebaasidest saadud andmeid võib reeglina töödelda üksnes sellel eesmärgil, milleks päring tehti, edasine töötlemine on üldjuhul keelatud või piiratud konkreetse üksikjuhtumi vajadusega. Kolmandatele isikutele nende menetluste käigus saadud

[130] Euroopa Kohtu otsus ühendatud kohtuasjades C-446/12-C-449/12 *Willems jt,* p-d 51, 53.

andmete avaldamine on reeglina keelatud. Erandiks võib olla erakorraline terroriaktide või raskete kuritegudega seotud olukord.

- Siseriiklike avalik-õiguslike menetluste raames kogutud isikuandmete ristkasutamist siseriiklikult reguleeritud menetluste raames EL-i õigus spetsiifiliselt ei reguleeri.

(a) VIS-süsteem

Õigusakt	Säte	Sõnastus
Nõukogu otsus 2008/633/JSK, 23. juuni 2008, mis käsitleb liikmesriikide määratud ametiasutuste ja Europoli juurdepääsu viisainfosüsteemile (VIS) terroriaktide ja muude raskete kuritegude vältimise, avastamise ja uurimise eesmärkidel	Artikkel 1	Käesolevas otsuses sätestatakse tingimused, mille kohaselt liikmesriikide määratud ametiasutused ja Euroopa Politseiamet (Europol) võivad saada juurdepääsu viisainfosüsteemi (VIS) andmetega tutvumiseks terroriaktide ja muude raskete kuritegude vältimise, avastamise ja uurimise eesmärkidel.

VIS-süsteem võimaldab piiriametnikel biomeetriliste andmete abil kindlaks teha, kas dokumendi esitaja on selle õige omanik ning tuvastada dokumentideta või võltsitud dokumentidega isikuid.[131] Liikmesriikidel on lubatud töödelda VIS-is asuvaid isikuandmeid terroriaktide, muude raskete kuritegude vältimise, avastamise ja uurimise eesmärkidel. [132] Kuivõrd biomeetriliste andmete töötlemine on sõnaselgelt Nõukogu otsusega 2006/633/JSK lubatud, siis on töötlemise aluseks üldmääruse art 9(2)(g) mõttes Euroopa Liidu õigus.

VIS-ist saadud andmete töötlemine peab piirduma terroriaktide ja muude raskete kuritegude vältimise, avastamise, uurimise ja nende eest vastutusele võtmise eesmärgi täitmisega.[133]

Juurdepääsu saamise tingimused täpsemalt on järgmised:

a. juurdepääs andmetega tutvumiseks peab olema vajalik terroriaktide ja muude raskete kuritegude vältimise, avastamise ja uurimise eesmärgil;

b. juurdepääsu peab olema vaja konkreetsel juhtumil;

c. kui on alust arvata, et VISi andmete kasutamine aitab oluliselt kaasa mõne kõnealuse kuriteo vältimisele, avastamisele või uurimisele.[134]

Liikmesriigid peavad VIS-st saadud andmeid kaitsma teatud turvameetmetega[135], sh kaitsma andmeid füüsiliselt, kontrollima andmekandjaid, takistama loata töötlemist, tagama andmeedastuse kontrolli jms. Andmesubjektidele tuleb tagada ka teatud õigused (nt tutvuda enda kohta käivate andmetega – vastavalt selle liikmesriigi õigusele, kus isik oma õigusi teostab). Liikmesriik, kes ei ole andmeid VIS-i sisestanud, võib andmeid puudutavat teavet

[131] Handbook on European Data Protection Law, lk 168

[132] Nõukogu otsus 2008/633/JSK art 1(1)

[133] *Ibid*, art 8(3)

[134] *Ibid*, art 5(1)

[135] *Ibid*, art 9

edastada ainult siis, kui ta on eelnevalt andnud andmeid sisestanud liikmesriigile võimaluse esitada oma seisukoht. Vastav õiguste kataloog on toodud otsuse 2008/633/JSK artiklis 14.

VIS-i andmetega tutvumisega seotud andmetöötlustoimingud tuleb registreerida, et kontrollida otsingu lubatavust, andmetöötluse seaduslikkust ning rakendada enesekontrolli ja tagada süsteemi nõuetekohane toimimine, andmete terviklikkus ja turvalisus[136].

(b) SIS II andmebaas

SIS II määrus	Artikkel 20 (2) (f)	2. Teave, mis käsitleb isikuid, kelle kohta on hoiatusteade sisestatud, sisaldab kõige rohkem järgmist: f. sõrmejäljed;
	Artikkel 22	Fotosid ja sõrmejälgi, nagu osutatud artikli 20 lõike 2 punktides e ja f, kasutatakse tingimusel, et järgitakse järgmisi sätteid: d. fotod ja sõrmejäljed sisestatakse üksnes pärast spetsiaalse kvaliteedikontrolli läbiviimist, et kindlustada andmete kvaliteedi suhtes kehtestatud miinimumstandardite järgimine. Spetsiaalse kvaliteedikontrolli määratlus kehtestatakse artikli 51 lõikes 2 osutatud korras, ilma et see piiraks korraldusasutuse moodustamist käsitleva õigusakti sätete kohaldamist; e. fotosid ja sõrmejälgi kasutatakse üksnes nende kolmanda riigi kodanike isiku tuvastamiseks, kelle andmed on leitud SIS II-s teostatud tähtnumbrilise päringu tulemusel; 3. niipea kui tehnika seda võimaldab, võib sõrmejälgi samuti kasutada kolmanda riigi kodaniku isiku tuvastamiseks tema biomeetrilise tunnuse alusel. Enne nimetatud funktsiooni rakendamist SIS II-s esitab komisjon aruande nõutava tehnoloogia kättesaadavuse ja töövalmiduse kohta, mille osas konsulteeritakse Euroopa Parlamendiga.
	Artikkel 29 (1)	Käesoleva määruse kohaselt SIS II sisestatud hoiatusteateid hoitakse ainult niikaua, kui on vaja nende eesmärkide saavutamiseks, milleks hoiatusteade sisestati.

[136] *Ibid*, art 16

	Artikkel 31	1. Liikmesriigid võivad töödelda artiklis 20 osutatud andmeid riiki sisenemise või oma territooriumil viibimise keelamiseks. 2. Andmeid võib kopeerida ainult tehnilisel otstarbel, kui selline kopeerimine on artiklis 27 osutatud asutustele vajalik vahetu päringu teostamiseks. Kõnealuste koopiate suhtes kohaldatakse käesoleva määruse sätteid. Ühe liikmesriigi sisestatud hoiatusteateid ei tohi kopeerida N.SIS II-st teistesse siseriiklikesse andmefailidesse. 3. Lõikes 2 osutatud tehnilisi koopiaid, mille tulemusena moodustuvad *off-line* andmebaasid, võib säilitada ajavahemikuks, mis ei ületa 48 tundi. Hädaolukorras võib seda ajavahemikku pikendada kuni hädaolukorra lõppemiseni. Olenemata esimesest lõigust ei ole tehnilised koopiad, mille tulemusena moodustuvad viisasid välja andvate asutuste poolt kasutatavavad *off-line* andmebaasid, enam lubatud ühe aasta möödumisel vastava asutuse edukast ühendamisest viisainfosüsteemi sideinfrastruktuuriga, nagu see sätestatakse tulevases määruses, mis käsitleb viisainfosüsteemi (VIS) ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta, välja arvatud koopiate puhul, mis on tehtud üksnes sellises hädaolukorras kasutamiseks, mil võrk on olnud enam kui 24 tunni jooksul ligipääsmatu. Liikmesriigid peavad kõnealuste koopiate ajakohastatud registrit, teevad selle registri kättesaadavaks siseriiklikele järelevalveasutustele ning tagavad kõnealuste koopiate suhtes kõigi käeoleva määruse sätete, eriti artikli 10 sätete kohaldamise. 4. Taolistele andmetele antakse juurdepääsuluba üksnes artiklis 27 osutatud siseriikliku asutuse pädevuse piires ja nõuetekohaselt volitatud töötajatele. 5. Andmeid ei või kasutada halduslikel eesmärkidel. Erandina võivad käesoleva määruse kohaselt sisestatud andmeid kasutada kooskõlas iga liikmesriigi õigusaktidega artikli 27 lõikes 3 osutatud asutused oma ülesannete täitmiseks. 6. Vastavalt käesoleva määruse artiklile 24 sisestatud andmeid ning otsuse 2006/000/JSK artikli 38 lõike 2 punktide d ja e kohaselt sisestatud isikutega seotud dokumente käsitlevaid andmeid võib kasutada käesoleva

		määruse artikli 27 lõikes 3 sätestatud otstarbel kooskõlas iga liikmesriigi õigusaktidega. 7. Andmekasutust, mis ei vasta lõigetele 1–6, käsitatakse iga liikmesriigi siseriikliku õiguse kohaselt väärkasutusena. 8. Iga liikmesriik edastab korraldusasutusele nende pädevate asutuste nimekirja, kellel on vastavalt käesolevale otsusele lubatud vahetult otsida SIS II-te sisestatud andmeid, ning nimekirja mis tahes hilisemad muudatused. Selles nimekirjas on iga asutuse puhul märgitud, milliseid andmeid ja millisel eesmärgil ta võib otsida. Korraldusasutus tagab nimekirja iga-aastase avaldamise Euroopa Liidu Teatajas. 9. Kui ühenduse õigusega ei nähta ette erisätteid, kohaldatakse liikmesriigi N.SIS II-te sisestatud andmete suhtes vastava liikmesriigi õigust.
Nõukogu otsus 2007/533/JSK, 12. juuni 2007, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist	Artikkel 56	Euroopa Nõukogu 28. jaanuari 1981. aasta konventsiooni (üksikisikute kaitse kohta isikuandmete automaattöötlusel) artikli 6 esimeses lauses loetletud andmekategooriate töötlemine on keelatud.

Lisaks VIS-süsteemile on Schengeni viisaruumis kasutusel täiendavad infosüsteemid, milles töödeldakse isikuandmeid, sh biomeetrilisi andmeid. SIS II andmebaasis, mis koosneb tsentraalsest süsteemist C-SIS ja siseriiklikust osast N-SIS, registreeritakse kohustuslikus korras hoiatusteateid isikute ja esemete kohta, sh võidakse registreerida isiku sõrmejäljed. Rassilist kuuluvust, poliitilisi vaateid või usulisi või muid veendumusi kirjeldavaid isikuandmeid ning andmeid tervisliku seisundi või seksuaalelu kohta ei või SIS II süsteemis registreerida.[137]

SIS II süsteemis andmete (sh sõrmejälgede andmete) kasutamine liikmesriigi poolt isiku territooriumile lubamise või keelamise hindamiseks lubatud, kuid mitte kohustuslik.[138] Andmeid võib kopeerida ainult tehnilisel otstarbel, kui selline kopeerimine on konkreetselt määruses viidatud asutustele vajalik vahetu päringu teostamiseks. See tähendab, et andmete töötlemine peab olema kooskõlas isikuandmete kaitse määruses sätestatud tingimustega ning töötlemine võib toimuda üksnes järgmises ulatuses[139]:

a. andmete kopeerimine on lubatud ainult tehnilisel otstarbel, kui selline kopeerimine on pädevale asutusele vajalik vahetu päringu teostamiseks;

b. selliseid koopiad võib säilitada *off-line* andmebaasides kuni 48 tundi, hädaolukorra puhul võib ajavahemikku pikendada hädaolukorra lõppemiseni;

c. andmete kasutamine halduslikel eesmärkidel on keelatud.

[137] Nõukogu otsus 2007/533/JSK art 56

[138] VIS-määrus, art 31(1)

[139] *Ibid*, art 31

Samas ei reguleeri SIS II määrus otseselt SIS II osaks oleva siseriikliku süsteemi N.SIS II andmete töötlemist. Seega võib riik N.SIS II süsteemi kogutud andmetega talitada vastavalt siseriiklikule õigusele.

(c) EES-süsteem

Õigusakt	**Säte**	**Sõnastus**
EES-määrus	Põhjenduspunkt 20	Riiki sisenemise ja riigist lahkumise süsteem peaks säilitama ja töötlema tähtnumbrilisi andmeid ja biomeetrilisi andmeid peamiselt selleks, et parandada välispiiride haldamist, hoida ära ebaseaduslikku sisseränet ja hõlbustada rändevoogude juhtimist. Lisaks peaksid riiki sisenemise ja riigist lahkumise süsteemi kogutud isikuandmed olema kättesaadavad terroriaktide ja muude raskete kuritegude ennetamiseks, avastamiseks ja uurimisele kaasaaitamiseks üksnes käesolevas määruses kehtestatud tingimustel. Biomeetriliste andmete kasutamine hoolimata selle mõjust reisijate privaatsusele on õigustatud kahel põhjusel. Esiteks on biomeetriliste andmete kasutamine usaldusväärne meetod nende kolmandate riikide kodanike tuvastamiseks, kellel ei ole liikmesriikide territooriumil viibides reisidokumenti või muud isikut tõendavat dokumenti, mis on ebaseaduslike rändajate puhul tavapärane. Teiseks on biomeetrilised andmed usaldusväärsemad seaduslike rändajate riiki sisenemise ja riigist lahkumise andmete võrdlemisel. Näokujutise kasutamine koos sõrmejälgedega võimaldab vähendada registreerimist vajavate sõrmejälgede, koguarvu, tagades samas täpse tuvastamise.
	Põhjenduspunkt 29	Isikuandmete kaitsmiseks ja süstemaatiliste otsingute välistamiseks tuleks riiki sisenemise ja riigist lahkumise süsteemi andmeid töödelda ainult erijuhtudel ning kui see on vajalik terroriaktide või muude raskete kuritegude ennetamiseks, avastamiseks või uurimiseks. Määratud ametiasutused ja Europol peaksid taotlema juurdepääsu riiki sisenemise ja riigist lahkumise süsteemile üksnes siis, kui neil on piisavalt alust arvata, et selle abil saadakse teavet, mis aitab olulisel määral kaasa terroriakti või muu raske kuriteo ennetamisele, avastamisele või uurimisele.
	Artikkel 49 (2) ja (3)	2. Riikide ametiasutuste poolt käesoleva määruse põhjal toimuva isikuandmete töötlemise suhtes, välja arvatud käesoleva

		määruse artikli 1 lõikes 2 osutatud eesmärkidel, kohaldatakse määrust (EL) 2016/679. 3. Liikmesriikide määratud asutuste poolt käesoleva määruse põhjal toimuva isikuandmete töötlemise suhtes käesoleva määruse artikli 1 lõikes 2 osutatud eesmärkidel kohaldatakse direktiivi (EL) 2016/680.

Liikmesriigid on kohustatud pidama arvet rändajate riiki sisenemise ja riigist lahkumise üle, et seeläbi tagada kontroll Schengeni välispiiri üle. Rändajate üle arve pidamise käigus on liikmesriigid kohustatud töötlema biomeetrilisi andmeid.[140]

Samas on riiki sisenemise ja riigist lahkumise süsteemi andmeid keelatud kasutada süstemaatiliste otsingute teostamiseks; andmete töötlemine on lubatud üksnes erijuhtudel ning kui see on vajalik terroriaktide või muude raskete kuritegude ennetamiseks, avastamiseks või uurimiseks. Määratud ametiasutused ja Europol peaksid taotlema juurdepääsu riiki sisenemise ja riigist lahkumise süsteemile üksnes siis, kui neil on piisavalt alust arvata, et selle abil saadakse teavet, mis aitab olulisel määral kaasa terroriakti või muu raske kuriteo ennetamisele, avastamisele või uurimisele.[141] Isikuandmete kaitse tagamiseks, tuleb liikmesriikidel isikuandmete töötlemisel järgida isikuandmete kaitse üldmäärust ning õiguskaitseasutuste direktiivis ettenähtud nõudeid.[142]

7.2.2. Koostalitusvõime raamistik

Kavandatav EL-i koostalitusvõime raamistik (vt ka p 6.7) seab eesmärgiks luua otsinguportaal, mis võimaldab samaaegselt teha päringuid kõigi EL-i julgeoleku, piiride ja rände haldamise valdkonna süsteemides.[143] Seejuures ei oleks ametnikel automaatset juurdepääsu kõikidele andmetele, mida ühise otsinguportaali läbi võiks kuvada. Juurdepääsuõigused on seotud õigustega konkreetsele alussüsteemile (st immigratsiooniametniku õigused isikusamasuse kontrollimiseks EES süsteemi läbi on reguleeritud EES määruses). Selleks, et juurdepääsuõigusi hallata, on tehtud ettepanek kaheetapilise juurdepääsu rakendamiseks, millest esimeses saaks ametnik päringu vastuseks, millis(t)es infosüsteemi(de)s isiku kohta andmeid on (ilma reaalse juurdepääsuta) ning teises etapis saab ametnik taotleda juurdepääsu. Juurdepääs antakse kooskõlas vastava süsteemi jaoks kehtestatud eeskirjade ja menetlustega.

Praktikas tähendab see seda, et näiteks piirivalveasutus saaks juurdepääsu piirikontrolli teostamisel isikusamasuse kontrollimise eesmärgil EES süsteemile kasutades EES-määruse art-s 23(2) sätestatud isikuandmeid, kuid sõrmejälgede alusel saab ta juurdepääsu näiteks juhul, kui ametnikul on kahtlused, et isik on juba teiste andmetega süsteemis registreeritud. Sama moodi võib immigratsiooniasutusel olla õigus teha EES süsteemis päringuid, et kontrollida, kas isik täidab liikmesriigis viibimise tingimusi, kuid kui sellel asutusel ei pruugi olla õigust pääseda ligi SIS II süsteemis olevatele hoiatusteadetele, kui see pole vastavalt liikmesriigi õiguses reguleeritud.[144] Selliselt on andmetele piiratud juurdepääs, mis võimaldab tagada

[140] EES määrus pp 20

[141] *Ibid*, pp 29

[142] *Ibid*, art 49(2), 49(3)

[143] Ettepanek 2017/0352(COD) lk 2

[144] SIS II määrus art 27 (3)

andmesubjekti õigusi ja vältida andmete ülemäärast töötlemist. Analoogset süsteemi oleks põhimõtteliselt võimalik rakendada ka siseriiklike andmebaaside puhul.

7.3. Ristkasutus isiku tuvastamiseks ja isikusamasuse kontrollimiseks teenusena eraõiguslikele isikutele

7.3.1. Rahvusvaheline õigus

Õigusakt	Säte	Sõnastus
Konventsioon 108+	Artikkel 3 (1)	1. Iga osapool kohaldab käesolevat Konventsiooni tema jurisdiktsioonile alluvale isikuandmete töötlemisele avalikus ja erasektoris, tagades seeläbi iga üksikisiku õiguse tema isikuandmete kaitseks.
	Artikkel 5 (1)	1. Andmete töötlemine peab olema taotletava õiguspärase eesmärgiga proportsionaalne ning töötlemise igal sammul peegeldama õiglast tasakaalu kõigi huvide vahel, sõltumata sellest, kas need on avalikud või erasfääris, ning kaalul olevate õiguste ja vabaduste vahel.
	Artikkel 14	2. Isikuandmeid võib edastada sellisele riigile või rahvusvahelisele organisatsioonile, kes ei ole konventsiooni osaline, ainult siis, kui on tagatud isikuandmete asjakohane kaitse vastavalt konventsiooni sätetele. 4. Isikuandmete edastamine võib toimuda, kui: a. andmesubjekt on andnud selgesõnalise, konkreetse ja vaba nõusoleku pärast seda, kui teda on teavitatud asjakohaste kaitsemeetmete puudumisest tulenevatest riskidest; või b. andmesubjekti konkreetsed huvid nõuavad seda konkreetsel juhul; või c. valitsevad õigustatud huvid, eriti olulised avalikud huvid, on seadusega ette nähtud ja selline üleandmine on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede; või d. see on vajalik ja proportsionaalne meede demokraatlikus ühiskonnas sõnavabaduse jaoks.

Kokkuvõte:

- Rahvusvaheline õigus ei keela avalik-õiguslikes menetlustes hõivatud biomeetriliste andmete edastamisest eraõiguslikele isikutele isiku tuvastamiseks või isikusamasuse kontrollimiseks, kui täidetud on biomeetriliste andmete töötlemise üldnõuded.

Rahvusvahelise õiguse õigusaktid ei erista andmete edastamist eraõiguslikele isikutele. Vastavalt Konventsiooni 108+ sõnastusele peavad selle osalisriigid tagama isikuandmete töötlemise vastavalt Konventsiooni nõuetele nii avalikus kui ka erasektoris. Kuna Konventsiooni 108+ ei ole otsekohalduv ning see tuleb üle võtta siseriiklikusse õigusesse[145], tuleb osalisriigil tagada, et siseriiklikus õiguses ei oleks vastuolu Konventsioonis toodud põhimõtetega.

Isikuandmete töötlemise põhimõtted Konventsiooni 108+ kohaselt on toodud analüüsi peatükis 3.1. Isikuandmete edastamist üldiselt reguleerib Konventsiooni artikli 14 lg 4. Konventsioon ei sea absoluutset keeldu avalik-õiguslikes menetlustes kogutud isikuandmete edastamisele eraõiguslikele isikutele, kuid mis tahes töötlemiseks peab olema õiguslik alus ning töötlemine peab vastama isikuandmete töötlemise nõuetele, sh arvestades biomeetriliste andmete töötlemisele seatud täiendavaid nõudeid.

7.3.2. Euroopa Liidu õigus

Õigusakt	**Säte**	**Sõnastus**
Isikuandmete kaitse üldmäärus	Artikkel 9 (4)	4. Liikmesriigid võivad säilitada või kehtestada täiendavad tingimused, sealhulgas piirangud seoses geneetiliste, biomeetriliste või terviseandmete töötlemisega.
	Artikkel 6 (4)	4. Kui isikuandmete töötlemine muul eesmärgil kui see, milleks isikuandmeid koguti, ei põhine andmesubjekti nõusolekul või liidu või liikmesriigi õigusel, mis on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede, et tagada artikli 23 lõikes 1 osutatud eesmärkide täitmine, võtab vastutav töötleja selle kindlakstegemiseks, kas muul eesmärgil töötlemine on kooskõlas eesmärgiga, mille jaoks isikuandmeid algselt koguti, muu hulgas arvesse a. seost nende eesmärkide, mille jaoks isikuandmeid koguti, ja kavandatava edasise töötlemise eesmärkide vahel; b. isikuandmete kogumise konteksti, eelkõige andmesubjektide ja vastutava töötleja vahelist seost; c. isikuandmete laadi, eelkõige seda, kas töödeldakse isikuandmete eriliike

[145] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, pp 31

		vastavalt artiklile 9 või süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmeid vastavalt artiklile 10; d. kavandatava edasise töötlemise võimalikke tagajärgi andmesubjektide jaoks; e. asjakohaste kaitsemeetmete olemasolu, milleks võivad olla näiteks krüpteerimine ja pseudonümiseerimine.
Õiguskaitseasutuste direktiiv	Artikkel 9 (1)	1. Artikli 1 lõikes 1 sätestatud eesmärkidel pädevate asutuste poolt kogutavaid isikuandmeid ei tohi töödelda muudel kui artikli 1 lõikes 1 sätestatud eesmärkidel, välja arvatud juhul, kui selline töötlemine on lubatud liidu või liikmesriigi õigusega. Kui isikuandmeid töödeldakse sellistel muudel eesmärkidel, kohaldatakse määrust (EL) 2016/679, välja arvatud juhul, kui isikuandmeid töödeldakse tegevuse käigus, mis ei kuulu liidu õiguse kohaldamisalasse.
	Artikkel 10	Selliste isikuandmete töötlemine, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, ning geneetiliste andmete, füüsilise isiku kordumatuks tuvastamiseks kasutatavate biomeetriliste andmete, tervist või seksuaalelu või seksuaalset sättumust käsitlevate andmete töötlemine on lubatud üksnes siis, kui see on rangelt vajalik, sellele kohaldatakse andmesubjekti õiguste ja vabaduste kaitsmiseks asjakohaseid kaitsemeetmeid ning üksnes järgmistel juhtudel: a. see on lubatud liidu või liikmesriigi õigusega; b. et kaitsta andmesubjekti või teise füüsilise isiku elulisi huve või c. selliselt töödeldakse isikuandmeid, mille andmesubjekt on ilmselgelt avalikustanud.
EES-määrus	Artikkel 41 (1), (2) ja (5)	1. Riiki sisenemise ja riigist lahkumise süsteemis säilitatavaid andmeid ei edastata ega tehta kättesaadavaks ühelegi kolmandale riigile, rahvusvahelisele organisatsioonile ega eraüksusele. 2. Erandina käesoleva artikli lõikest 1 võivad piirivalveasutused või immigratsiooniasutused üksikjuhtudel edastada käesoleva määruse artikli 16 lõikes

		1 ning artikli 17 lõike 1 punktides a, b ja c osutatud andmeid käesoleva määruse I lisas nimetatud kolmandale riigile või rahvusvahelisele organisatsioonile, kui see on vajalik kolmandate riikide kodanike isikusamasuse tõendamiseks üksnes tagasisaatmise eesmärgil, ainult juhul, kui on täidetud üks järgmistest tingimustest: a. komisjon on vastu võtnud otsuse isikuandmete asjakohase kaitse kohta kõnealuses kolmandas riigis kooskõlas määruse (EL) 2016/679 artikli 45 lõikega 3; b. ette on nähtud asjakohased määruse (EL) 2016/679 artiklis 46 osutatud kaitsemeetmed, näiteks liidu või liikmesriigi ja asjaomase kolmanda riigi vahel kehtiva tagasivõtulepinguga, või c. kohaldatakse määruse (EL) 2016/679 artikli 49 lõike 1 punkti d. 5. Käesoleva määruse artikli 16 lõikes 1 ning artikli 17 lõike 1 punktides a, b ja c osutatud andmeid võib edastada ainult juhul, kui kõik järgnevad tingimused on täidetud: a. andmed edastatakse kooskõlas liidu õiguse asjakohaste sätetega, eelkõige andmekaitsesätetega, sealhulgas määruse (EL) 2016/679 V peatükiga, samuti tagasivõtulepingutega ning andmed edastanud liikmesriigi õigusega; b. kolmas riik või rahvusvaheline organisatsioon on nõus andmeid töötlema ainult neil eesmärkidel, milleks need esitati, ning c. asjaomase kolmanda riigi kodaniku kohta on väljastatud direktiivi 2008/115/EÜ kohaselt vastu võetud tagasisaatmisotsus, tingimusel et selle täitmist ei ole peatatud ning tingimusel et otsust ei ole edasi kaevatud, mille tulemusena võidakse tagasisaatmisotsuse täitmine peatada. 6. Isikuandmeid, mis liikmesriik või Europol saab õiguskaitse eesmärgil riiki sisenemise ja riigist lahkumise kesksüsteemist, ei edastata ega tehta kättesaadavaks ühelegi kolmandale riigile, rahvusvahelisele organisatsioonile ega liidus või väljaspool seda loodud eraõiguslikule isikule. See keeld kehtib ka juhul, kui nimetatud andmeid töödeldakse

		edasi liikmesriigi või liikmesriikidevahelisel tasandil vastavalt direktiivile (EL) 2016/680.
	Artikkel 17 (1) (c)	1. Piirivalveasutus koostab viisanõudest vabastatud kolmandate riikide kodanike isikliku toimiku, sisestades c. parema käe sõrmejälgede andmed kui need on olemas ja nende puudumisel vasaku käe vastavad sõrmejälgede andmed, sõrmejälgede andmed peavad olema piisava lahutusvõime ja kvaliteediga, et neid saaks kasutada automaatseks biomeetriliseks võrdlemiseks;
Eurodac määrus	Artikkel 35	1. Isikuandmeid, mis liikmesriik või Europol saab kesksüsteemist käesoleva määruse kohaselt, ei edastata ega tehta kättesaadavaks ühelegi kolmandale riigile, liidus või väljaspool seda loodud rahvusvahelisele organisatsioonile ega eraõiguslikule üksusele. See keeld kehtib ka juhul, kui nimetatud andmeid töödeldakse edasi liikmesriigi või liikmesriikidevahelisel tasandil raamotsuse 2008/977/JSK artikli 2 punkti b mõistes. 2. Ühest liikmesriigist pärinevaid ja kokkulangevuse järel liikmesriikide vahel artikli 1 lõikes 2 sätestatud eesmärgil vahetatavaid andmeid ei edastata kolmandatele riikidele, kui esineb tõsine oht, et sellise edastamise tagajärjel võidakse andmesubjekti piinata, ebainimlikult või alandavalt kohelda või karistada või rikkuda mis tahes muid tema põhiõigusi. 3. Lõigetes 1 ja 2 nimetatud keelud ei piira liikmesriigi õigust edastada kõnealuseid andmeid sellistele kolmandatele riikidele, kelle suhtes kohaldatakse määrust (EL) nr 604/2013.

Kokkuvõte:

- EL-i õigus ei loo õiguslikku alust avalik-õiguslikes menetlustes hõivatud isikuandmete edastamisele eraõiguslikele isikutele isiku tuvastamise või isikusamasuse kontrollimise eesmärgil.
- Siseriiklikult reguleeritud avalik-õiguslikes menetlustes hõivatud biomeetriliste andmete edastamisele on riigil võimalik vastavalt isikuandmete kaitse üldmäärusele luua vastav õiguslik alus, kui see vastab artikli 9 ja artikli 6(4) tingimustele, sh tuleb läbi viia vastav kaalumine, ning mis vastab artiklis 23 toodud eesmärkidele.

- EL-i pädevusse kuuluvate avalik-õiguslike menetluste käigus kogutud biomeetriliste andmete edastamine kolmandatele isikutele võib olla keelatud või piiratud teatud eeldustega.

Euroopa Liidu õigus ei loo õiguslikku alust riigi poolt avalikes-õiguslikes menetlustes hõivatud biomeetriliste andmete edastamiseks eraõiguslikele isikutele. Edastamine eraõiguslikule isikule võib olla sisuliselt biomeetriliste andmete edasine töötlemine, seega kohalduvad sellisele andmete edastamisele sätted biomeetriliste andmete töötlemisele ning nõuded andmete edasiseks kasutamiseks (isikuandmete kaitse üldmääruse art 6(4) tingimused). Seega kohalduvad sellisele andmeedastusele samad üldpõhimõtted, mis igale isikuandmete töötlemise tegevusele. Olukorras, kus riik näiteks delegeerib avaliku võimu ülesande eraõiguslikule isikule (olukorras, kus tegemist ei ole riigi tuumikfunktsioonidega ja see on lubatav) halduslepingu alusel vastavalt volitusnormile, võib andmete edastamine olla lubatav eraõiguslikule isikule kui eraõiguslikule isikule on üle antud avaliku võimu ülesanne.

Biomeetriliste andmete töötlemiseks peab olema vastav õiguslik alus isikuandmete kaitse üldmääruse art-le 9. Kui riik on kogunud andmed avalik-õiguslikes menetlustes kehtival õiguslikul alusel, peab nende edastamine olema kooskõlas edastamise tingimustega. Seega on riigil põhimõtteliselt võimalik luua täiendavaid õiguslikke aluseid biomeetriliste isikuandmete edastamiseks eraõiguslikele isikutele, kuid selleks peab riik olema läbi teinud isikuandmete kaitse üldmääruse artikli 9(2)(g) ja artikli 6(4) kohase kaalumise. Analoogselt kohalduvad isikuandmete töötlemisel süütegude tõkestamise eesmärgil õiguskaitseasutuste direktiivist tulenevad nõuded: biomeetriliste andmete töötlemine peab olema rangelt vajalik ning sellele kohaldatakse õiguskaitseasutuste direktiivi artiklis 10 toodud nõudeid ning edasine töötlemine toimub vastavalt isikuandmete kaitse üldmääruse artiklis 6(4) toodud nõuetele.

Kui isikuandmed on kogutud teatud Euroopa Liidu poolt reguleeritud avalik-õiguslike menetluste käigus Euroopa Liidu andmebaasidesse, siis nende kaudu saadud andmete edastamine kolmandatele isikutele võib siiski olla keelatud. See tähendab, et kui Eesti saab biomeetrilised andmed nt Eurodac süsteemist, siis üldreegli kohaselt ei tohi selliseid andmeid edastada nt eraõiguslikule isikule ka mitte isikutuvastuse või isikusamasuse kontrollimise eesmärgil.

Schengeni välispiiri ületamise süsteemi määrus piirab selgelt süsteemis talletatud andmete edasise kasutamise. Sellele piirangule kehtivad teatud erandid, kuid need erandid ei kehti sõrmejälgede edasisele kasutamisele eraõiguslike isikute poolt. Erandi alla kuuluvatest andmetest on biomeetrilised andmed üksnes isiku näokujutis ning sõrmejäljed ning nende edastamine võib olla lubatud teatud riikidele ja rahvusvahelistele organisatsioonidele, kui see on vajalik kolmandast riigist pärit isiku tagasisaatmise eesmärgil ning on täidetud art 41(2) ja 41(3) toodud tingimused. Seega ei saa Schengeni välispiiri ületamise süsteemis talletatud sõrmejälgi edastada eraõiguslikele isikutele, sh isiku tuvastamise või isikusamasuse kontrollimiseks.

Eurodac määruse kohaselt on samuti keelatud Eurodacist saadavate andmete edastamine kolmandale riigile, rahvusvahelisele organisatsioonile või eraõiguslikule isikule. Erand on üksnes riikidele, kelle puhul kohaldatakse määrust 604/2013 (s.t. seoses varjupaigataotluste läbivaatamisega).

8. BIOMEETRILISTE ANDMETE EDASTAMINE TEISTELE RIIKIDELE JA RAHVUSVAHELISTELE ORGANISATSIOONIDELE

Avalik-õiguslikes menetlustes kogutud andmete edastamine teistele riikidele ja rahvusvahelistele organisatsioonidele on olemuselt andmete edasine kasutamine. Seega peab selline edastamine ehk töötlemine vastama isikuandmete edasise kasutamise nõuetele (vt peatükk 7). Eeldusel, et andmete algseks kogumiseks on õiguslik alus, vajab andmete edastamine samuti õiguslikku alust.

Käesolev peatükk analüüsib biomeetriliste andmete edastamist teistele riikidele ja rahvusvahelistele organisatsioonidele. Teisisõnu on tegemist olukorraga, kus andmesubjekti biomeetrilisi andmeid töödeldakse avalik-õiguslikus suhtes, ehkki andmete vastuvõtjaks ja töötlejaks võib olla teises riigis olev asutus. Vastavalt tellija ülesandepüstitusele analüüsime eelkõige olukordi, kus andmete edastamise eesmärk on andmesubjekti isiku tuvastamine või isikusamasuse kontrollimine. On oluline märkida, et teises riigis asuval asutusel võib endal olla iseseisev õiguslik alus andmesubjekti andmete töötlemiseks oma siseriikliku või muu temale kehtiva õiguse alusel, kuid selleks, et andmete edastamine oleks õiguspärane, peab olema selge õiguslik alus andmete edastamiseks ABIS-e süsteemist teisele riigile või rahvusvahelisele organisatsioonile nimetatud eesmärgil.

Käesoleva peatüki alapeatükis „Euroopa Liidu õigus“ ei ole korratud alapeatükis 7.3.2 välja toodud sätteid. Kuna olemuselt on kolmandale riigile või rahvusvahelisele organisatsioonile isikuandmete edastamine analoogne eraõiguslikule isikule edastamisega, kehtivad sellistele töötlemistegevustele samad üldnõuded ning seega neid ei korrata. Käesolevas peatükis tuuakse välja konkreetselt isikuandmete edastamisega seotud sätted.

8.1. Rahvusvaheline õigus

Õigusakt	Säte	Sõnastus
Moderniseeritud isikuandmete töötlemisel isiku kaitse konventsioon 108 **(Konventsioon 108+)**	Artikkel 14	1. Osalisriik ei keela üksnes isikuandmete kaitse eesmärgil isikuandmete edastamist andmete vastuvõtjale, kes allub teise konventsiooni osalisriigi õigusele, ega sea edastamise tingimuseks eraldi luba. See osalisriik võib seda siiski teha, kui on tegelik ja tõsine risk, et edastamine teisele osalisriigile või sellelt osalisriigilt või riigilt, kes ei ole osalisriik, võiks viia konventsiooni sätete eiramiseni. Osalisriik võib seda ka teha juhul kui on kaitse osas seotud ühtlustatud reeglitega riikide vahel, kes kuuluvad regionaalsesse rahvusvahelisse organisatsiooni. 2. Kui andmete vastuvõtjale kohaldub selle riigi või rahvusvahelise organisatsiooni õigus, kes ei ole konventsiooni osalisriik, võib isikuandmete edastamine toimuda üksnes juhul kui tagatud on piisav andmekaitse tase, mis põhineb käesoleva konventsiooni sätetel. 3. Isikuandmeid võib edastada sellisele riigile või rahvusvahelisele organisatsioonile, kes ei ole

		konventsiooni osaline, ainult siis, kui on tagatud isikuandmete asjakohane kaitse vastavalt konventsiooni sätetele. 5. Sõltumata eelmistes paragrahvides toodud sätetest, võib iga osapool ette näha, et isikuandmete edastamine võib toimuda juhul kui: a. andmesubjekt on andnud oma selgesõnalise, konkreetse ja vaba nõusoleku pärast seda, kui teda on asjakohaste turvameetmete puudumisest tingitud riskidest teavitatud; b. konkreetsel juhul nõuavad seda andmesubjekti erilised huvid; c. on ülekaalukas õigustatud huvi, eelkõige avalik huvi, mis on sätestatud seadusega ning selline edastamine on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede; või d. see on sõnavabaduseks demokraatlikus ühiskonnas vajalik ja proportsionaalne meede. 6. Isikuandmete edastamine võib toimuda, kui: a. andmesubjekt on andnud selgesõnalise, konkreetse ja vaba nõusoleku pärast seda, kui teda on teavitatud asjakohaste kaitsemeetmete puudumisest tulenevatest riskidest; või b. andmesubjekti konkreetsed huvid nõuavad seda konkreetsel juhul; või c. valitsevad õigustatud huvid, eriti olulised avalikud huvid, on seadusega ette nähtud ja selline üleandmine on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede; või d. see on vajalik ja proportsionaalne meede demokraatlikus ühiskonnas sõnavabaduse jaoks.

Kokkuvõte:

- Rahvusvaheline õigus ei keela avalik-õiguslikes menetlustes hõivatud biomeetriliste andmete edastamisest teistele riikidele või rahvusvahelistele organisatsioonidele isiku tuvastamiseks või isikusamasuse kontrollimiseks, kui täidetud on biomeetriliste andmete töötlemise üldnõuded ning andmete edastamise eeldused, sh õigusliku aluse olemasolu ja täiendavate kaitsemeetmete rakendamine.

Rahvusvaheline õigus tunnustab andmete vaba liikumise tähtsust rahvusvahelise koostöö arendamisel. Konventsioon 108+ kohaldub ka isikuandmete edastamisele, sätestamata seejuures erisätteid andmete edastamisele konkreetsetes valdkondades või konkreetsetel eesmärkidel. Andmete edastamise oluliseks eelduseks on asjakohaste kaitsemeetmete rakendamine. Konventsiooniga mitte-liitunud riikidele on andmete vaba edastamine lubatud juhul kui:

- Selle riigi või rahvusvahelise organisatsiooni õigusaktid tagavad asjakohaste turvameetmete rakendamise või
- On olemas *ad hoc* või standardsed kaitsemeetmed, mis on antud õiguslikult siduvate ja jõustatavate instrumentide poolt, mille on vastu võtnud ja rakendanud isikud, kes on seotud andmete edastamise ja edasise töötlemisega.

Seega lubab rahvusvaheline õigus andmeid edastada teistele riikidele (s.o. riikidele, mis ei ole Konventsioon 108+ osalisriigid) ja rahvusvahelistele organisatsioonidele, kui rakendatud on täiendavaid garantiisid isikuandmete turvalisuse tagamiseks. Lisaks peab biomeetriliste andmete edastamiseks olema tagatud, et asjakohased kaitsemeetmed oleks kehtivas õiguses sätestatud ning need peavad täiendama Konventsioonis toodud kaitsemeetmeid.[146]

8.2. Euroopa Liidu õigus

Õigusakt	**Säte**	**Sõnastus**
Isikuandmete kaitse üldmäärus	Artikkel 1 (3)	Isikuandmete vaba liikumist liidus ei piirata ega keelata põhjustel, mis on seotud füüsiliste isikute kaitsega isikuandmete töötlemisel.
	Artikkel 44	Töödeldavate või pärast kolmandale riigile või rahvusvahelisele organisatsioonile edastamist töötlemiseks ette nähtud isikuandmete edastamine toimub ainult juhul, kui vastutav töötleja ja volitatud töötleja on täitnud kooskõlas käesoleva määruse teiste sätetega käesolevas peatükis sätestatud tingimused, sealhulgas juhul, kui kolmas riik või rahvusvaheline organisatsioon saadab isikuandmed edasi muule kolmandale riigile või rahvusvahelisele organisatsioonile. Kõiki käesoleva peatüki sätteid kohaldatakse selleks, et tagada, et käesoleva määrusega tagatud füüsiliste isikute kaitse taset ei kahjustata.
	Artikkel 49 (1) (g)	1. Artikli 45 lõike 3 kohase kaitse piisavuse otsuse või artikli 46 kohaste asjakohaste kaitsemeetmete, sealhulgas siduvate kontsernisiseste eeskirjade puudumise korral võib kolmandale riigile või rahvusvahelisele organisatsioonile isikuandmete ühekordne või korduv edastamine olla lubatud ainult ühel järgmistest tingimustest:

[146] Vt analüüsi peatükk 3.1

		e. edastamine on vajalik avalikust huvist tulenevatel kaalukatel põhjustel; g. edastamine tehakse registrist, mis liidu või liikmesriigi õiguse kohaselt on mõeldud avalikkuse teavitamiseks ja on tutvumiseks avatud kas laiemale avalikkusele või kõigile, kes suudavad tõendada õigustatud huvi, kuid ainult sellisel määral, nagu konkreetsel juhul on täidetud tutvumist käsitlevad tingimused, mis on liidu või liikmesriigi õigusega ette nähtud.
Õiguskaitseasutuste direktiiv	Artikkel 35	1. Liikmesriigid näevad ette, et pädevad asutused edastavad töödeldavaid või pärast kolmandatele riikidele või rahvusvahelistele organisatsioonidele edastamist töötlemiseks, sealhulgas andmete kolmandatele riikidele ja rahvusvahelistele organisatsioonidele edasi saatmiseks mõeldud isikuandmeid üksnes juhul, kui on täidetud käesoleva direktiivi muude sätete kohaselt vastu võetud liikmesriigi sätted ja käesolevas peatükis sätestatud tingimused, nimelt: a. edastamine on vajalik artikli 1 lõikes 1 sätestatud eesmärkidel; b. isikuandmeid edastatakse vastutavale töötlejale kolmandas riigis või rahvusvahelises organisatsioonis, mis on artikli 1 lõikes 1 osutatud eesmärkidel pädev asutus; c. juhul kui isikuandmeid edastatakse või tehakse kättesaadavaks teisest liikmesriigist, on kõnealune liikmesriik andnud edastamiseks eelnevalt loa kooskõlas oma siseriikliku õigusega; d. komisjon on artikli 36 kohaselt võtnud vastu kaitse piisavuse otsuse või kui sellist otsust ei ole vastu võetud, siis on kehtestatud või võetud artikli 37 kohased piisavad kaitsemeetmed, või kui artikli 36 kohane kaitse piisavuse otsus või 37 kohased piisavad kaitsemeetmed puuduvad, kohaldatakse artikli 38 kohaselt erandeid eriolukordades, ning e. andmete edasisaatmise korral muule kolmandale riigile või rahvusvahelisele organisatsioonile annab andmed algselt edastanud pädev asutus või sama liikmesriigi muu pädev asutus loa edasisaatmiseks, olles võtnud

		nõuetekohaselt arvesse kõiki asjakohaseid tegureid, sealhulgas süüteo raskust, isikuandmete algse edastamise eesmärki ja isikuandmete kaitse taset selles kolmandas riigis või rahvusvahelises organisatsioonis, kuhu isikuandmed edasi saadetakse. 2. Liikmesriigid näevad ette, et andmete edastamine lõike 1 punkti c kohaselt ilma teise liikmesriigi eelneva loata on lubatud üksnes juhul, kui isikuandmete edastamine on vajalik liikmesriigi või kolmanda riigi avalikku julgeolekut ähvardava vahetu ja tõsise ohu ennetamiseks või liikmesriigi olulise huvi seisukohast ning eelnevat luba ei ole võimalik õigeaegselt saada. Eelneva loa andmise eest vastutavat asutust teavitatakse viivitamata. 3. Kõiki käesoleva peatüki sätteid kohaldatakse selleks, et tagada füüsiliste isikute kaitse käesoleva direktiiviga ette nähtud tasemel.
	Artikkel 36 (1)	1. Liikmesriigid näevad ette, et isikuandmeid võib kolmandale riigile või rahvusvahelisele organisatsioonile edastada siis, kui komisjon on teinud otsuse, et asjaomane kolmas riik või asjaomase kolmanda riigi territoorium või asjaomase kolmanda riigi üks või mitu kindlaksmääratud sektorit või rahvusvaheline organisatsioon tagab isikuandmete kaitse piisava taseme. Selliseks edastamiseks ei ole vaja eriluba.
Nõukogu otsus 2008/615/JSK, 23. juuni 2008, piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega	Artikkel 14	1. Kuritegude ärahoidmiseks ning avaliku korra ja julgeoleku tagamiseks piiriülese mõõtmega suursündmuste, eelkõige spordiürituste ja Euroopa Ülemkogu kohtumiste korral, edastavad liikmesriigid nii taotluse saamisel kui ka enda algatusel üksteisele isikuandmeid, kui lõplikud süüdimõistvad kohtuotsused või muud asjaolud annavad põhjust uskuda, et andmesubjektid sooritavad sündmuse ajal kuritegusid või ohustavad avalikku korda või julgeolekut; isikuandmeid esitatakse sellises ulatuses, nagu selliseid andmeid on andmeid edastava liikmesriigi siseriikliku õiguse kohaselt lubatud edastada. 2. Isikuandmeid võib töödelda ainult lõikes 1 sätestatud eesmärkidel ning seoses konkreetse sündmusega, mille jaoks need edastati. Edastatud andmed kustutatakse

		viivitamata, kui lõikes 1 osutatud eesmärgid on saavutatud või ei ole enam saavutatavad. Edastatud andmed kustutatakse igal juhul hiljemalt ühe aasta pärast.
VIS määrus	Artikkel 31	1. Käesoleva määruse kohaselt VISis töödeldud andmeid ei edastata ega tehta kättesaadavaks kolmandatele riikidele ega rahvusvahelistele organisatsioonidele. 2. Erinevalt lõikest 1 võib artikli 9 lõike 4 punktides a, b, c, k ja m osutatud andmeid edastada või teha kättesaadavaks lisas loetletud kolmandatele riikidele või rahvusvahelistele organisatsioonidele, kui see on üksikjuhul vajalik kolmanda riigi kodanike isikusamasuse tuvastamiseks, kaasa arvatud tagasisaatmise eesmärgil, kui on täidetud järgmised tingimused: a. komisjon on vastu võtnud otsuse isikuandmete asjakohase kaitse kohta kõnealuses kolmandas riigis kooskõlas direktiivi 95/46/EÜ artikli 25 lõikega 6 või ühenduse ja kõnealuse kolmanda riigi vahel kehtib tagasivõtmisleping või kohaldatakse direktiivi 95/46/EÜ artikli 26 lõike 1 punkti d sätteid; b. kolmas riik või rahvusvaheline organisatsioon on nõus kasutama andmeid ainult sellel eesmärgil, milleks need esitati; c. andmed edastatakse või tehakse kättesaadavaks kooskõlas ühenduse õiguse, eriti tagasivõtmislepingute, ning andmed edastanud või kättesaadavaks teinud liikmesriigi õiguse asjakohaste sätetega, kaasa arvatud andmete turvalisuse ja andmekaitse kohta kehtivate õigusnormidega, ning d. andmed VISi sisestanud liikmesriik või liikmesriigid on andnud oma nõusoleku.
SIS-määrus	Põhjenduspunkt 18	Käesoleva otsuse kohaldamisel SIS II-s töödeldavaid andmeid ei edastata kolmandatele riikidele ega rahvusvahelistele organisatsioonidele ega tehta neile kättesaadavaks. Tõhusat teabevahetust edendades on aga kohane tugevdada koostööd Euroopa Liidu ja Interpoli vahel, edendades tõhusat passiandmete vahetust. Kui SIS II-st edastatakse isikuandmeid Interpolile, peaks nendele andmetele tagama kohase kaitsetaseme,

		kehtestades lepingus ranged kaitsemeetmed ja tingimused.
	Artikkel 54	Vastavalt käesolevale otsusele SIS II-s töödeldavaid andmeid ei edastata kolmandatele riikidele ega rahvusvahelistele organisatsioonidele ega tehta neile kättesaadavaks.

Kokkuvõte:

- EL-i õigus ei loo õiguslikku alust avalik-õiguslikes menetlustes hõivatud isikuandmete edastamisele teistele riikidele või rahvusvahelistele organisatsioonidele isiku tuvastamise või isikusamasuse kontrollimise eesmärgil.
- Siseriiklikult reguleeritud avalik-õiguslikes menetlustes hõivatud biomeetriliste andmete edastamisele on riigil võimalik vastavalt isikuandmete kaitse üldmäärusele luua vastav õiguslik alus, kui see vastab artikli 9 ja artikli 6(4) tingimustele, sh tuleb läbi viia vastav kaalumine, ning vastab artiklis 23 toodud eesmärkidele.
- Euroopa Liidu pädevusse kuuluvate avalik-õiguslike menetluste käigus kogutud biomeetriliste andmete edastamine kolmandatele isikutele võib olla keelatud või piiratud teatud eeldustega.

Euroopa Liidu õiguse põhimõtted toetavad eelkõige andmete vaba liikumist Euroopa Liidus. Andmete vaba liikumise põhimõtet on laiendatud kogu Euroopa Majanduspiirkonnale (s.t. Euroopa Liidu riigid + Norra, Island ja Liechtenstein). Kuna Euroopa Liidus rakendatakse ühtseid andmekaitse standardeid, ei ole ühenduse sees andmete liikumine seotud nii kõrge riskiga kui näiteks kolmandatesse riikidesse andmete edastamisel. Seetõttu on isikuandmete edastamisel kolmandatesse riikidesse (sh avaliku sektori asutustele kui ka rahvusvahelistele organisatsioonidele) isikuandmete kaitse üldmäärusega reguleeritud.

Andmete edastamine on lubatud üksnes juhul, kui see vastab isikuandmete kaitse üldmääruses sätestatud tingimustele. Täiendavaid meetmeid tuleb rakendada just juhul, kui andmete importija on kolmandas riigis. Teatud eesmärkidel andmete edastamisel võivad kehtida erisätted (nt süütegude ennetamise, uurimise, avastamise või nende eest vastutusele võtmise või kriminaalkaristuse täitmisele pööramise eesmärgil vastavalt õiguskaitseasutuste direktiivile).

Isikuandmete edastamine võib aset leida, kui kolmas riik tagab piisava andmekaitse taseme või kui andmete vastutava ja volitatud töötleja vahel on sobivad kaitsemeetmed kehtestatud (nt andmetöötluse leping). Teatud erakorralistes olukordades on isikuandmete edastamine lubatud isegi juhul kui puudub piisav andmekaitse tase ning kasutusele ei ole võetud asjakohaseid kaitsemeetmeid.

Erinevalt rahvusvahelise õiguse raamistikust, on Euroopa Liidus kaks võimalust, kuidas lubatakse kolmandatele riikidele andmete edastamine: Euroopa Komisjoni hinnang või vastutava ja volitatud töötleja vahel rakendatud kaitsemeetmed. Euroopa Komisjoni piisavusotsused võivad kehtida ka üksnes teatud tüüpi andmeedastusele või sektorile või kindlale territooriumile. Antud meetmete sisu ja nõuded jäävad käesoleva analüüsi ulatusest välja.

Üldjuhul võib liikmesriik ise sätestada täiendavaid aluseid isikuandmete töötlemiseks, sh biomeetriliste andmete töötlemiseks ja edastamiseks. Teatud Euroopa Liidu pädevuses olevate menetlusliikide puhul võib nende raames kogutud andmete edastamine olla piiratud või sootuks

keelatud (vt analüüsi ptk 7.3.2). Näiteks on Eurodaci süsteemist biomeetriliste andmete edastamine kolmandale riigile või rahvusvahelisele organisatsioonile keelatud. Sama üldreegel kehtib ka VIS ja SIS II süsteemist andmete edastamiseks teistele riikidele või rahvusvahelistele organisatsioonidele. VIS-süsteemi puhul näiteks on lubatud erandjuhtumil isikuandmete edastamine teatud kolmandatele riikidele või rahvusvahelistele organisatsioonidele, kui see on üksikjuhul vajalik kolmanda riigi kodanike isikusamasuse tuvastamiseks, kuid sõrmejäljed ei kuulu selle erandi alla.[147]

Samas on piiriülese mõõtmega suursündmuste korral liikmesriigid kohustatud kuritegude ärahoidmiseks ning avaliku korra ja julgeoleku tagamiseks edastama üksteisele isikuandmeid – seda ulatuses, milles andmeid on lubatud edastada andmeid edastava liikmesriigi siseriikliku õiguse kohaselt.[148]

[147] Määrus 767/2008 art 31(2)

[148] Nõukogu otsus 2008/615/JSK art 14

9. BIOMEETRILISTE ANDMETE TÖÖTLEMINE JA EDASTAMINE ERAÕIGUSLIKES SUHETES

Käesolev peatükk analüüsib olukorda, kus eraõiguslik isik töötleb biomeetrilisi andmeid puhtalt eraõiguslikus suhtes (s.t. andmeid ei töödelda avalik-õiguslikus suhtes või riigilt üle võetud avalik-õigusliku ülesande täitmiseks). Eelduslikult on vastavad biomeetrilised andmed saadud küll riigilt (ABIS-e süsteemist), kuid õigusaktist tulenevat kohustust andmeid selliselt töödelda eraõiguslikul isikul ei ole. Teisisõnu soovib eraõiguslik isik biomeetrilisi andmeid töödelda isiku tuvastamiseks või isikusamasuse kontrollimiseks täiendava garantiina enda eraõiguslikes suhetes. Küsimus põhineb eeldusel, et riigil on lubatud ja tehniliselt võimalik biomeetrilisi andmeid eraõiguslikele isikutele edastada. Seejuures on oluline tuvastada, millisel õiguslikul alusel saaks eraõiguslik isik riigi poolt hõivatud biomeetrilisi andmeid töödelda ning millised on selle töötlemise tingimused.

9.1. Rahvusvaheline õigus

Rahvusvaheline õigus ei reguleeri spetsiifiliselt biomeetriliste andmete töötlemist (erandiks Konventsioon 108+, mis artiklis 6 määratleb biomeetrilised andmed ning kohustab osalisriiki võtma nende töötlemiseks asjakohaseid kaitsemeetmeid) ega erista ka isikuandmete töötlemist avalik-õiguslike ja eraõiguslike isikute poolt. Seega on ka eraõiguslike isikute poolt biomeetriliste andmete töötlemisel täies ulatuses kehtivad punktis 3.1 kirjeldatud printsiibid.

9.2. Euroopa Liidu õigus

Euroopa Liidu õigus		
Euroopa Liidu põhiõiguste harta	Artikkel 8	1. Igaühel on õigus oma isikuandmete kaitsele. 2. Selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. Igaühel on õigus tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist. 3. Nende sätete täitmist kontrollib sõltumatu asutus.
Isikuandmete kaitse üldmäärus	Artikkel 5	2. Isikuandmete töötlemisel tagatakse, et a. töötlemine on seaduslik, õiglane ja andmesubjektile läbipaistev („seaduslikkus, õiglus ja läbipaistvus“); b. isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus; isikuandmete edasist töötlemist avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgil ei loeta artikli 89 lõike 1 kohaselt algsete

		eesmärkidega vastuolus olevaks („eesmärgi piirang“); c. isikuandmed on asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt („võimalikult väheste andmete kogumine“); d. isikuandmed on õiged ja vajaduse korral ajakohastatud ning et võetakse kõik mõistlikud meetmed, et töötlemise eesmärgi seisukohast ebaõiged isikuandmed kustutaks või parandataks viivitamata („õigsus“); e. isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse; isikuandmeid võib kauem säilitada juhul, kui isikuandmeid töödeldakse üksnes avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgil vastavalt artikli 89 lõikele 1, eeldusel et andmesubjektide õiguste ja vabaduste kaitseks rakendatakse käesoleva määrusega ettenähtud asjakohaseid tehnilisi ja korralduslikke meetmeid („säilitamise piirang“); f. isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid („usaldusväärsus ja konfidentsiaalsus“); 3. Lõike 1 täitmise eest vastutab ja on võimeline selle täitmist tõendama vastutav töötleja („vastutus“).
	Artikkel 9 (1) ja 9 (2)	1. Keelatud on töödelda isikuandmeid, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilisi andmeid, füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid, terviseandmeid või andmeid füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta.

		2. Lõiget 1 ei kohaldata, kui kehtib üks järgmistest asjaoludest: a) andmesubjekt on andnud selgesõnalise nõusoleku nende isikuandmete töötlemiseks ühel või mitmel konkreetsel eesmärgil, välja arvatud juhul, kui liidu või liikmesriigi õiguse kohaselt ei saa andmesubjekt lõikes 1 nimetatud keeldu tühistada; b) töötlemine on vajalik seoses vastutava töötleja või andmesubjekti tööõigusest ning sotsiaalkindlustuse ja sotsiaalkaitse valdkonna õigusest tulenevate kohustuste ja eriõigustega niivõrd, kuivõrd see on lubatud liidu või liikmesriigi õigusega või liikmesriigi õiguse kohase kollektiivlepinguga, millega kehtestatakse asjakohased kaitsemeetmed andmesubjekti põhiõiguste ja huvide kaitseks; c) töötlemine on vajalik selleks, et kaitsta andmesubjekti või teise füüsilise isiku elulisi huve, kui andmesubjekt on füüsiliselt või õiguslikult võimetu nõusolekut andma; d) töödeldakse poliitilise, filosoofilise, religioosse või ametiühingulise suunitlusega sihtasutuse, ühenduse või muu mittetulundusühingu õiguspärase tegevuse raames, mille suhtes kohaldatakse vajalikke kaitsemeetmeid, ning tingimusel, et töötlemine käsitleb ainult asjaomase ühingu liikmeid või endisi liikmeid või isikuid, kes on kõnealuse ühinguga püsivalt seotud tema tegevuse eesmärkide tõttu, ning et isikuandmeid ei avalikustata väljaspool seda ühingut ilma andmesubjekti nõusolekuta; e) töödeldakse isikuandmeid, mille andmesubjekt on ilmselgelt avalikustanud; f) töötlemine on vajalik õigusnõude koostamiseks, esitamiseks või kaitsmiseks või juhul, kui kohtud täidavad oma õigust mõistvat funktsiooni; g) töötlemine on vajalik olulise avaliku huviga seotud põhjustel liidu või liikmesriigi õiguse alusel ning on proportsionaalne saavutatava

		eesmärgiga, austab isikuandmete kaitse õiguse olemust ja tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks; h) töötlemine on vajalik ennetava meditsiini või töömeditsiiniga seotud põhjustel, töötaja töövõime hindamiseks, meditsiinilise diagnoosi panemiseks, tervishoiuteenuste või sotsiaalhoolekande või ravi võimaldamiseks või tervishoiu- või sotsiaalhoolekandesüsteemi ja -teenuste korraldamiseks, tuginedes liidu või liikmesriigi õigusele või tervishoiutöötajaga sõlmitud lepingule ja eeldusel, et lõikes 3 osutatud tingimused on täidetud ja kaitsemeetmed kehtestatud; i) töötlemine on vajalik rahvatervise valdkonna avalikes huvides, nagu kaitse suure piiriülese terviseohu korral või kõrgete kvaliteedi- ja ohutusnõuete tagamine tervishoiu ning ravimite või meditsiiniseadmete puhul, tuginedes liidu või liikmesriigi õigusele, millega nähakse ette sobivad ja konkreetsed meetmed andmesubjekti õiguste ja vabaduste kaitseks, eelkõige ametisaladuse hoidmine, j) töötlemine on vajalik avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgil vastavalt artikli 83 lõikele 1, tuginedes liidu või liikmesriigi õigusele, ning on proportsionaalne saavutatava eesmärgiga, austab isikuandmete kaitse õiguse olemust ning tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks. 3. Lõikes 1 osutatud isikuandmeid võib töödelda lõike 2 punktis h osutatud eesmärkidel, kui neid andmeid töötleb töötaja, kellel on liidu või liikmesriigi õiguse või pädevate riiklike asutuste kehtestatud eeskirjade alusel ametisaladuse hoidmise kohustus, või kui neid andmeid töödeldakse sellise isiku vastutusel või kui neid andmeid töötleb mõni teine isik, kellel on liidu või liikmesriigi õiguse või pädevate riiklike asutuste kehtestatud eeskirjade alusel samuti saladuse hoidmise kohustus.

		4. Liikmesriigid võivad säilitada või kehtestada täiendavad tingimused, sealhulgas piirangud seoses geneetiliste, biomeetriliste või terviseandmete töötlemisega.
	Artikkel 9 (4)	Liikmesriigid võivad säilitada või kehtestada täiendavad tingimused, sealhulgas piirangud seoses geneetiliste, biomeetriliste või terviseandmete töötlemisega.
	Artikkel 4 (11)	Käesolevas määruses kasutatakse järgmisi mõisteid: 11) andmesubjekti „nõusolek“– vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega;
	Artikkel 7	1. Kui töötlemine põhineb nõusolekul, peab vastutaval töötlejal olema võimalik tõendada, et andmesubjekt on nõustunud oma isikuandmete töötlemisega. 2. Kui andmesubjekt annab nõusoleku kirjaliku kinnitusena, mis puudutab ka muid küsimusi, esitatakse nõusoleku taotlus viisil, mis on muudest küsimustest selgelt eristatav, ning arusaadaval ja lihtsasti kättesaadaval kujul, kasutades selget ja lihtsat keelt. Sellise kinnituse mis tahes osa, mille puhul on tegemist käesoleva määruse rikkumisega, ei ole siduv. 3. Andmesubjektil on õigus oma nõusolek igal ajal tagasi võtta. Nõusoleku tagasivõtmine ei mõjuta enne tagasivõtmist nõusoleku alusel toimunud töötlemise seaduslikkust. Andmesubjekti teavitatakse sellest enne nõusoleku andmist. Nõusoleku tagasivõtmine on sama lihtne kui selle andmine. 4. Selle hindamisel, kas nõusolek anti vabatahtlikult, tuleb võimalikult suurel määral võtta arvesse asjaolu, kas lepingu täitmise, sealhulgas teenuse osutamise tingimuseks on muu hulgas seatud nõusoleku isikuandmine andmete töötlemiseks, mis ei ole vajalik kõnealuse lepingu täitmiseks.

Kokkuvõte:

- Euroopa Liidu õigus ei loo õiguslikku alust avalik-õiguslikes menetlustes hõivatud isikuandmete edastamisele eraõiguslikele isikutele eraõiguslikus suhtes kasutamise eesmärgi.
- Eraõiguslikus suhtes biomeetriliste andmete töötlemine võib aset leida andmesubjekti nõusolekul või muul õiguslikul alusel.

9.2.1. Õigusaktid

(a) Euroopa Liidu põhiõiguste harta

Euroopa Liidu põhiõiguste harta ei erista isikuandmete töötlemist avalik-õiguslike ja eraõiguslike isikute poolt. Seega kehtivad punktis 3.2.1. kirjeldatud põhimõtted ka biomeetriliste andmete töötlemisele eraõiguslike juriidiliste isikute poolt eraõiguslikes suhetes.

(b) Isikuandmete kaitse üldmäärus

Isikuandmete kaitse üldmääruse sisalduv seaduslikkuse nõue tähendab, et isikuandmete töötlemiseks peab alati olema õiguslik alus. Biomeetriliste andmete töötlemise võimalikud alusel on nimetatud üldmääruse art-s 9(2).

Liikmesriigid võivad nendele tingimustele lisaks kehtestada täiendavaid tingimusi, sealhulgas piiranguid seoses geneetiliste, biomeetriliste või terviseandmete töötlemisega. Geneetiliste andmete töötlemise näitel on selliseks täiendavaks tingimuseks näiteks inimgeeniuuringute seadus, mis reguleerib geeniuuringute tegemist ning geenivaramu pidamist[149]. ABIS-e regulatsiooni väljatöötamisel oleks võimalik luua täiendav õiguslik alus biomeetriliste andmete kasutamiseks eraõiguslike isikute vahelistes suhetes näiteks turvalisuse tagamise eesmärgil. Seejuures tuleb arvesse võtta, et õiguslik alus peab vastama isikuandmete kaitse üldmääruse art 6(3) tingimustele, ehk peab muuhulgas olema vajalik avalikes huvides oleva ülesande täitmiseks, vastama avaliku huvi eesmärgile ning olema proportsionaalne taotletava eesmärgiga.

Viite sellele, et biomeetriliste andmete töötlemiseks antav täiendav õiguslik alus peab vastama nimetatud tingimustele, annab määruse põhjenduspunkt 51, mille kohaselt eriliiki isikuandmeid ei tohiks töödelda, välja arvatud määruses sätestatud konkreetsetel juhtudel, kui töötlemine on lubatud, „võttes arvesse seda, et liikmesriikide õiguses võib kehtestada konkreetseid andmekaitse-eeskirju, et kohandada käesoleva määruse eeskirjade kohaldamist juriidilise kohustuse täitmiseks või avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks“.

Üldmääruse art 9(2)(b), (d), (h), (i) ja (j) alusel võib liikmesriigi õigusega näha ette kohustusi ja eriõiguseid eraõiguslikele isikutele järgmistes valdkondades: tööõigus, sotsiaalkindlustus, sotsiaalkaitse; poliitiliste, filosoofiliste, religioosse või ametiühingulise suunitlusega sihtasutuse, ühenduse või muu mittetulundusühingu õiguspärane tegevus; meditsiin ja sotsiaalhoolekanne; rahvatervis; arhiveerimine, teadus- või ajaloouuringud, statistika. Üldmääruse art 9(2)(g) näeb ette õigusliku aluse töötlemiseks olukorras, kus töötlemine vajalik „olulise avaliku huviga seotud põhjustel liigu või liikmesriigi õiguse alusel“. Määruse põhjenduspunkti 52 kohaselt on tööõiguse, sotsiaalkaitseõiguse, terviseturbe, -seire ja hoiatamisega seotud eesmärkidel toimuvad töötlemistoimingud näited konkreetsetest avalikes huvides toimuvatest töötlemistoimingutest.

[149] Seletuskiri isikuandmete kaitse seaduse rakendamise seaduse eelnõu juurde, lk 25. Kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/96c37d10-383c-40ad-87be-a8583008b994/Isikuandmete%20kaitse%20seaduse%20rakendamise%20seadus (27.11.2018)

Art 9(2)(g) sisaldub niisiis võrreldes konkreetsete avalikes huvides toimuvate töötlemistoimingutega üldisem õiguslik alus, mis annab volituse töödelda biomeetrilisi andmeid *olulise* avaliku huviga seotud põhjustel. Põhjenduspunktis 52 sisalduv näidisloetelu avalikes huvides toimuvast töötlemisest näitab, et ka art 9(2)(g) on võimalik tugineda eraõiguslikul isikul, kui töötlemine kannab *olulise* avaliku huvi eesmärki. Eesti õiguses on seda samuti tunnustatud: näiteks isikuandmete kaitse seaduse rakendamise seaduse eelnõu § 38 p 3 annab õiguse kindlustusandjale töödelda terviseandmeid, mida on eelnõu seletuskirjas põhjendatud samuti art 9(2)(g) sätestatud olulise avaliku huviga: oluline avalik huvi on kiire tervisekahjustuse tõttu tekkinud kulude hüvitamine kahjustatud isikul[150].

Valdkonnaüleseks asjakohaseks õiguslikuks aluseks võivad olla veel andmesubjekti selgesõnaline nõusolek, töötlemise vajalikkus õigusnõude koostamiseks, esitamiseks või kaitsmiseks, füüsilise isiku eluliste huvide kaitse ning andmesubjekti poolt avalikustatud isikuandmete töötlemine. Biomeetriliste andmete töötlemise kontekstis eraõiguslike isikute poolt eraõiguslike ülesannete täitmiseks on viimased kaks (eluliste huvide kaitse ning andmesubjekti poolt avalikustatud andmete töötlemine) pigem erandlikud. Üksikjuhtumitel võib isikuandmeid töödelda õigusnõude koostamise, esitamise või kaitsmise eesmärgil, kui töötlemine on selle eesmärgi täitmiseks vajalik.

Õiguslikuks aluseks ABIS-est saadud biomeetriliste andmete töötlemiseks võib olla andmesubjekti selgesõnaline nõusolek (üldmääruse art 9(2)(a)). Üldmääruse art 4(11) kohaselt defineeritakse andmesubjekti nõusolekut kui „vabatahtlikku, konkreetset, teadlikku ja ühemõttelist tahteavaldust, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega“. Lisaks art 4(11) tulenevatele kriteeriumitele peab isikuandmete eriliikide töötlemiseks antav nõusolek olema „selgesõnaline“.

Kehtiva nõusoleku kriteeriume on selgitatud üldmääruse põhjenduspunktides 32-33 ning 42-43. Lisaks on isikuandmete kaitse direktiivi art 29 alusel asutatud andmekaitse töörühm (Euroopa Andmekaitsenõukogu eelkäija) andnud välja suunised määruse (EL) 2016/679 kohase nõusoleku kohta[151]. Kokkuvõtvalt peab biomeetriliste andmete töötlemiseks antav nõusolek vastama järgmistele kriteeriumidele:

- Nõusolek peab olema vabatahtlikult antud

Kui andmesubjektil ei ole tõelist valikuvõimalust, kui ta tunneb sundi nõustuda või kui tal tuleb nõusoleku andmata jätmise korral taluda negatiivseid tagajärgi (nt kulusid, ebasoosivat suhtumist vms), on nõusolek kehtetu. Kui nõusolek on osa mitte-läbiräägitavatest tingimustest (osa tüüptingimustest), ei peeta seda vabatahtlikult antuks.[152] Kui lepingu täitmine ja teenuse osutamine sõltub nõusoleku andmisest, ei ole nõusolek vabatahtlik.[153] See puudutab olukordi, kus küsitud andmed ei ole lepingu täitmiseks vajalikud, kuid lepingu täitmise tingimuseks on seatud nende saamine nõusoleku alusel[154] (samas on oluline märkida, et erinevalt isikuandmete kaitse üldmääruse art 6(1) (mitte-eriliigiliste isikuandmete töötlemise õiguslikud alused) ei näe art 9(2) isikuandmete eriliikide töötlemise õigusliku alusena ette andmesubjektiga sõlmitud

[150] Seletuskiri isikuandmete kaitse seaduse rakendamise seaduse eelnõu juurde, lk 47-48. Kättesaadav: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/wp259_rev_0.1_et.pdf (26.11.2018)

[151] Artikli 29 alusel asutatud andmekaitse töörühma suunised kehtiva nõusoleku kohta

[152] *Ibid*, lk 5.

[153] Isikuandmete kaitse üldmäärus art 7(4), pp 42.

[154] Artikli 29 alusel asutatud andmekaitse töörühma suunised kehtiva nõusoleku kohta, lk 9.

ükskõik millise lepingu täitmist või lepingu sõlmimist). Lisaks ei ole nõusolek tõenäoliselt vabatahtlik, kui pooled on ebavõrdses jõuvahekorras, näiteks töösuhtes[155]. Nõusolekut ei saa lugeda vabatahtlikuks ka siis, kui isikuandmeid töödeldakse korraga mitmel eesmärgil ja töötleja ei saa iga eesmärgi jaoks eraldi nõusolekut.[156]

- Nõusolek peab olema konkreetne

Konkreetsuse nõude täitmiseks peab vastutav töötleja sõnastama täpselt töötlemise eesmärgi, tagama nõusolekutaotluse üksikasjalikkuse ning eraldama teabe, mis on seotud nõusoleku saamisega, selgelt muid küsimusi puudutavast teabest. Tulenevalt eesmärgi piirangu põhimõttest tuleb iga erineval eesmärgil toimuva töötlemise jaoks saada eraldi nõusolek.[157]

- Nõusolek peab olema teadlik

Kehtiva nõusoleku saamiseks tuleb andmesubjekti teavitada vähemalt järgmisest: vastutava töötleja andmed, iga töötlemistoimingu eesmärk, mille jaoks nõusolekut küsitakse, millist liiki andmeid kogutakse ja kasutatakse, nõusoleku tagasivõtmise õiguse olemasolu, vajaduse korral teave andmete kasutamise kohta automatiseeritud otsuste tegemisel ning võimalike ohtude kohta andmete edastamisel kolmandatesse riikidesse, mis on tingitud kaitse piisavuse otsuse ja asjakohaste kaitsemeetmete puudumisest. Nimetatud teave tuleb esitada selgelt ja kättesaadavas vormis, keskmisele inimesele arusaadavalt ning see teave ei tohi olla peidetud üldistesse tingimustesse.[158]

- Nõusolek peab olema ühemõtteline tahteavaldus

Üldmääruse artikli 4(11) kohaselt peab nõusolek olema ühemõtteline tahteavaldus avalduse vormis või selge nõusolekut väljendava tegevusena. See tähendab, et andmesubjekt peab olema astunud konkreetse töötlemisega nõustumiseks tahtliku sammu. Tegevusetust, näiteks eeltäidetud kastikeses linnukese aktsepteerimist ei saa lugeda ühemõtteliseks tahteavalduseks.[159]

- Nõusolek peab olema antud selgesõnaliselt

Et biomeetrilised andmed on eriliigilised isikuandmed üldmääruse art 9(1) mõttes, nõutakse nende töötlemiseks selgesõnalist nõusolekut. Sõna selgesõnaline viitab viisile, kuidas andmesubjekt oma nõusolekut väljendab. See tähendab, et andmesubjekt peab esitama nõusoleku kohta sõnaselge avalduse. Endastmõistetav viis selle tagamiseks, et nõusolek on selgesõnaline, on kinnitada nõusolekut selgelt kirjalikus avalduses, kuid see ei ole siiski ainus viis, kuidas saada selgesõnaline nõusolek. Näiteks digitaal- või veebikeskkonnas võib andmesubjektil olla võimalik esitada nõutav avaldus täites elektroonilise vormi, saates e-kirja, laadides üles skaneeritud dokumendi või kasutades digiallkirja. Üks viis selgesõnalise nõusoleku tagamiseks võib olla kaheastmeline nõusoleku kontroll.[160]

- Nõusolekut peab saama igal ajal tagasi võtta

[155] *Ibid*, lk 7.

[156] *Ibid*, lk 10; isikuandmete kaitse üldmääruse pp 32

[157] *Ibid*, lk 12-13.

[158] *Ibid*, lk 13-14.

[159] Isikuandmete kaitse üldmääruse art 4(11), pp 32.

[160] Artikli 29 alusel asutatud andmekaitse töörühma suunised kehtiva nõusoleku kohta, lk 19-20.

Üldmääruse artikli 7(3) kohaselt peab andmesubjektil olema õigus oma nõusolek igal ajal tagasi võtta sama lihtsalt, kui oli nõusolekut anda. See ei mõjuta enne tagasivõtmist nõusoleku alusel toimunud töötlemise seaduslikkust. Andmesubjekti tuleb tagasivõtmise õigusest enne nõusoleku andmist teavitada. Andmesubjektil peab olema võimalik nõusolek tagasi võtta ilma kahjulike tagajärgedeta, näiteks ei tohi nõusoleku tagasivõtmisega kaasneda teenuse taseme alandamine või tasu tõstmine.[161]

Kui vastutav töötleja on saanud andmesubjektilt kehtiva nõusoleku biomeetriliste andmete töötlemiseks või kui konkreetsel juhul on võimalik tugineda mõnele muule töötlemise õiguslikule alusele, peab vastutav töötleja järgima isikuandmete töötlemise üldpõhimõtteid, mis on sätestatud üldmääruse art 5. Muuhulgas tuleb järgida eesmärgi piirangu põhimõtet ning mitte töödelda biomeetrilisi andmeid viisil, mis on andmete esialgse töötlemise eesmärgiga vastuolus, ning võimalikult väheste andmete kogumise põhimõtte kohaselt mitte töödelda rohkem isikuandmeid kui on vajalik konkreetse eesmärgi täitmiseks (näiteks ei ole panga poolt lepingu sõlmimiseks vajaliku isikusamasuse tuvastamiseks ilmselt vaja skaneerida 10 sõrmejälge). Lisaks tuleb igal konkreetsel juhul analüüsida, kui kaua on isikuandmete säilitamine konkreetse eesmärgi täitmiseks vajalik – lepingu sõlmimiseks isikusamasuse tuvastamise korral võib näiteks olla vajalik isikuandmete töötlemise üldpõhimõtete täitmiseks kustutada biomeetrilised andmed eraõigusliku juriidilise isiku süsteemidest niipea, kui isikusamasus on tuvastatud. Lisaks isikuandmete kaitse üldprintsiipidele peab iga eraõiguslikust isikust vastutav töötleja tagama andmesubjekti õiguste teostamise võimalikkuse vastavalt isikuandmete töötlemise III peatükile, sh tagama andmesubjekti õiguse tutvuda andmetega, nõuda andmete parandamist, põhjendatud juhtudel andmete kustutamist või töötlemise piiramist, õiguse andmete ülekandmisele ning õiguse esitada oma seisukoht ja vaidlustus automatiseeritud töötlusel põhinevale üksikotsusele.

Kui eraõiguslik juriidiline isik soovib isikuandmeid teistele eraõiguslikele isikutele edasi anda, siis peab selleks töötlemistoiminguks samuti olema õiguslik alus (nt kehtiv nõusolek, mis vastab eelpool kirjeldatud kriteeriumitele) ning peab järgima kõiki eelnimetatud printsiipe ja kohustusi. Kui andmete vastuvõtja asub kolmandas riigis, tuleb järgida isikuandmete edastamise põhimõtteid, mis on reguleeritud isikuandmete kaitse üldmääruse V peatükis ning kirjeldatud käesoleva analüüsi 8. peatükis.

[161] *Ibid*, lk 22.

10. SUMMARY

The foregoing legal analysis of international law and European Union law has highlighted the complex nature of personal data processing carried out by the public sector. With regards to biometric data, collection of fingerprints and facial images for issuing identification and travel documents, fingerprints and DNA in criminal proceedings is already well established in law. Nevertheless, the permissibility of further use of such biometric data is still a complicated issue and requires balancing by the legislator in order to weigh the freedoms, rights and interests of all the parties involved.

Based on the instructions of the Ministry of Interior of the Republic of Estonia, we have analysed the possibility of creating a joint automatic biometric identification system (ABIS) from legal point of view, with focus solely on international law and European Union law. The focus of the legal analysis has been on the following key issues:

a. The legal obstacles for creating a consolidated database for the collection and processing of biometric data by the state;

b. The requirements for hardware and software used for processing of biometric data;

c. The obligations which the national law must follow in the processing of biometric data;

d. The processing of biometric data in proceedings in public law;

e. Cross-usage of biometric data: including further use in other legal proceedings in public law, by other states and international organisations and by private persons.

The analysis focuses on the proceedings which fall in the competence of the European Union and the respective databases which contain the data collected in the course of these proceedings. European Union has several central databases which are mainly used for the purposes of enabling identical procedures for the Member States, more specifically in areas like border control (Schengen area external borders), visa applications, asylum procedures, illegal migration, issuing of identification and travel documents. However, these databases are also accessible for cooperation in relation to criminal proceedings and more specifically in fight against terrorism and serious crimes. Since European Union law does not regulate the establishment and operation of national databases, the main focus of this analysis was to identify the extent and conditions for using the data collected from EU databases in the national proceedings.

The summary findings to these key issues from international law and European Union law are as follows:

1. The processing of biometric data collected in different proceedings in one consolidated database is subject to the general principles of personal data processing (i.e. purpose limitation, legality, data minimisation, transparency, retention limitation and application of appropriate safeguards).

Exceptions to these principles are possible, but this requires a valid legal basis, which is subject to balancing by the legislator.

2. Under the technological neutrality principle, the requirements for hardware and software are established in law only as general requirements without specifying technical details or technical requirements to systems. A data controller must apply a risk-based approach and evaluate the potential risks associated with the intended data processing and apply appropriate technical measures to mitigate such risks.

3. Under general rules of the GDPR, processing of biometric data is prohibited, unless any exceptions apply. In any case, there must exist a valid legal basis for the processing of biometric data for the specific purposes.

4. Before establishing a legal basis under national (or EU law) the legislator must perform the following balancing act:

   4.1. Data processing must be proportionate the purpose pursued;

   4.2. Data processing must respect the nature of data protection law;

   4.3. Appropriate and specific means are ensured for the protection of the fundamental rights and interests of the data subject.

5. In most proceedings regulated by EU law, the member states are obligated to collect biometric data and transfer this data to the central EU databases. Comparison of the data is often voluntary (this depends on the necessity which is evaluated by the responsible authority), as is collection of data from EU databases for investigation, detection and prosecution in criminal offences.

6. Cross-usage of data is generally restricted by the principle of purpose limitation, i.e. biometric data can only be processed for other purposes if the purposes of such further processing are compliant with the purposes of its initial collection.

7. If further processing is not compliant with the purposes of initial collection/processing, a separate legal basis for such processing must be established (by law or, for example, consent of the data subject of this is possible).

8. Further processing of personal data received from EU central databases is generally prohibited or permitted only to a limited extent and for specific reasons established under the respective EU legal acts. This also applies to transferring such personal data to third countries, international organisations and private persons.

9. Processing of biometric data by private persons is subject to a suitable valid legal basis, for example on the basis of the consent of the data subject (or other valid legal basis).

11. KASUTATUD KIRJANDUS

11.1. Õigusaktid

1. Konventsioon 108+
2. Konventsioon 108
3. Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt (ICCPR)
4. Euroopa inimõiguste ja põhivabaduste kaitse konventsioon
5. Euroopa Liidu põhiõiguste harta
6. United Nations. Standard Minimum Rules for the Administration of Juvenile Justice ("The Beijing Rules"). 29.11.1985, rule 21
7. Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta
8. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK
9. Euroopa Parlamendi ja nõukogu määrus (EL) 2016/794, 11. mai 2016, mis käsitleb Euroopa Liidu Õiguskaitsekoostöö Ametit (Europol) ning millega asendatakse ja tunnistatakse kehtetuks nõukogu otsused 2009/371/JSK, 2009/934/JSK, 2009/935/JSK, 2009/936/JSK ja 2009/968/JSK
10. Nõukogu otsus 2008/615/JSK, 23. juuni 2008, piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega
11. Euroopa Parlamendi ja Nõukogu määrus (EÜ) nr 767/2008, 9. juuli 2008, mis käsitleb viisainfosüsteemi (VIS) ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta
12. Nõukogu otsus 2007/533/JSK, 12. juuni 2007, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist
13. Euroopa Parlamendi ja Nõukogu määrus (EÜ) nr 444/2009, 28. mai 2009, millega muudetakse nõukogu määrust (EÜ) nr 2252/2004 liikmesriikide väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta
14. Nõukogu määrus (EÜ) nr 1030/2002, 13. juuni 2002, millega kehtestatakse ühtne elamisloavorm kolmandate riikide kodanike jaoks
15. Nõukogu määrus (EÜ) nr 380/2008, 18. aprill 2008, millega muudetakse määrust (EÜ) nr 1030/2002, millega kehtestatakse ühtne elamisloavorm kolmandate riikide kodanike jaoks
16. Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 810/2009, 13. juuli 2009, millega kehtestatakse ühenduse viisaeeskiri
17. Euroopa Parlamendi ja Nõukogu määrus (EÜ) nr 767/2008, 9. juuli 2008, mis käsitleb viisainfosüsteemi (VIS) ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta
18. Nõukogu otsus 2008/633/JSK, 23. juuni 2008, mis käsitleb liikmesriikide määratud ametiasutuste ja Europoli juurdepääsu viisainfosüsteemile (VIS) terroriaktide ja muude raskete kuritegude vältimise, avastamise ja uurimise eesmärkidel

19. Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 390/2009, 23. aprill 2009, millega muudetakse viisasid käsitlevaid ühiseid konsulaarjuhiseid diplomaatilistele ja konsulaaresindustele seoses biomeetria kasutuselevõtmisega ning viisataotluste vastuvõtmise ja menetlemise korraldamise sätete lisamisega

20. Euroopa Parlamendi ja nõukogu määrus (EL) 2016/399, 9. märts 2016, mis käsitleb isikute üle piiri liikumist reguleerivaid liidu eeskirju

21. Euroopa Parlamendi ja nõukogu määrus (EL) 2017/458, 15. märts 2017, millega muudetakse määrust (EL) 2016/399 seoses asjaomastes andmebaasides tehtava kontrolli tugevdamisega välispiiridel

22. Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1987/2006, 20. detsember 2006, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist

23. Euroopa Parlamendi ja nõukogu määrus (EL) 2017/2226, 30. november 2017, millega luuakse riiki sisenemise ja riigist lahkumise süsteem liikmesriikide välispiire ületavate kolmandate riikide kodanike riiki sisenemise ja riigist lahkumise andmete ja sisenemiskeeluandmete registreerimiseks ning määratakse kindlaks riiki sisenemise ja riigist lahkumise süsteemile õiguskaitse eesmärgil juurdepääsu andmise tingimused ning millega muudetakse Schengeni lepingu rakendamise konventsiooni ning määruseid (EÜ) nr 767/2008 ja (EL) nr 1077/2011

24. Euroopa Parlamendi ja nõukogu määrus (EL) nr 604/2013, 26. juuni 2013, millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku või kodakondsuseta isiku esitatud rahvusvahelise kaitse taotluse läbivaatamise eest

25. Austria Vabariigi, Belgia Kuningriigi, Hispaania Kuningriigi, Luksemburgi Suurhertsogiriigi, Madalmaade Kuningriigi, Prantsuse Vabariigi ja Saksamaa Liitvabariigi vahelise eelkõige terrorismi-, piiriülese kuritegevuse ja ebaseadusliku rände vastases võitluses piiriülese koostöö tõhustamise leping (Prümi leping)

26. Nõukogu otsus 2008/615/JSK, 23. juuni 2008, piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega

27. Nõukogu otsus 2008/616/JSK, 23. juuni 2008, millega rakendatakse otsust 2008/615/JSK piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega

28. Euroopa Parlamendi ja nõukogu direktiiv 2008/115/EÜ, 16. detsember 2008, ühiste nõuete ja korra kohta liikmesriikides ebaseaduslikult viibivate kolmandate riikide kodanike tagasisaatmisel

11.2. Õigusaktide eelnõud ja algatused

29. Ettepanek: NÕUKOGU OTSUS, millega antakse liikmesriikidele luba ratifitseerida Euroopa Liidu huvides protokoll, millega muudetakse Euroopa Nõukogu konventsiooni üksikisikute kaitse kohta isikuandmete automaattöötlusel (ETS nr 108) nr COM/2018/451 final

30. Ettepanek: Euroopa Parlamendi ja Nõukogu määrus liidu kodanike isikutunnistuste ning vaba liikumise õigust kasutavatele liidu kodanikele ja nende pereliikmetele väljaantavate elamislubade turvalisuse suurendamise kohta nr COM(2018) 212 final - 2018/0104 (COD)

31. Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega luuakse kesksüsteem nende liikmesriikide väljaselgitamiseks, kellel on teavet kolmandate riikide kodanike ja kodakondsuseta isikute suhtes tehtud süüdimõistvate kohtuotsuste kohta, et täiendada ja toetada Euroopa karistusregistrite infosüsteemi (ECRIS-TCN-süsteem), ning muudetakse määrust (EL) nr 1077/2011 COM/2017/0344 final - 2017/0144 (COD)

32. Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega luuakse ELi infosüsteemide (politsei- ja õiguskoostöö, varjupaik ja ränne) koostalitlusvõime raamistik nr COM(2017) 794 final - 2017/0352 (COD)

33. Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega muudetakse määrust (EÜ) nr 767/2008, määrust (EÜ) nr 810/2009, määrust (EL) 2017/2226, määrust (EL) 2016/399, määrust XX/2018 [koostalitlusvõimet käsitlev määrus] ja otsust 2004/512/EÜ ning tunnistatakse kehtetuks nõukogu otsus 2008/633/JSK, nr COM(2018) 302 final - 2018/0152 (COD)
RAPORT ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse Schengeni infosüsteemi (SIS) loomist, toimimist ja kasutamist riigipiiri ületamise kontrolli valdkonnas ning millega muudetakse määrust (EL) nr 515/2014 ja tunnistatakse kehtetuks määrus (EÜ) nr 1987/2006 (COM(2016)0882 - C8-0533/2017 - 2016/0408(COD))

34. RAPORT ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse Schengeni infosüsteemi (SIS) loomist, toimimist ja kasutamist politseikoostöös ja kriminaalasjades tehtavas õigusalases koostöös ning millega muudetakse määrust (EL) nr 515/2014 ja tunnistatakse kehtetuks määrus (EÜ) nr 1986/2006, nõukogu otsus 2007/533/JSK ja komisjoni otsus 2010/261/EL (COM(2016)0883 - C8-0530/2016 - 2016/0409(COD))

35. RAPORT ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus Schengeni infosüsteemi kasutamise kohta ebaseaduslikult riigis viibivate kolmandate riikide kodanike tagasisaatmiseks(COM(2016)0881 - C8-0532/2016 - 2016/0407(COD))

36. Proposal for a directive of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final - 2012/0010 (COD)

11.3. Õigusaktide seletuskirjad ja seadusandja või järelevalveasutuse suunised

37. ÜRO Inimõiguste Komitee “CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8.04.1988”

38. Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

39. Komisjoni teatis Euroopa Parlamendile ja nõukogule Parimate tulemuste saavutamine võrgu- ja infoturbe direktiivi rakendamisel – jõupingutused direktiivi (EL) 2016/1148 (meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus) tulemuslikuks rakendamiseks COM/2017/0476 final

40. ENISA, NCSS Good Practice Guide Designing and Implementing National Cyber Securit Strategies, November 2016

41. ENISA, Inventory of Risk Management / Risk Assessment Methods

42. Seletuskiri isikuandmete kaitse seaduse rakendamise seaduse eelnõu juurde

43. Artikli 29 alusel asutatud andmekaitse töörühma suunised kehtiva nõusoleku kohta

11.4. Kohtupraktika

44. Euroopa Kohus (CJEU) C-291/12, Schwarz v. Bochum, 17.10.2013

45. Euroopa Inimõiguste Kohus (ECtHR) M.K. v. France, No. 76100/13, 18.04.2013

46. Euroopa Kohus (CJEU) C-275/06, Promusicae v. Telefónica de Espana SAU, kohtujuristi arvamus 18.07.2007

47. ECtHR, S. and Marper v. United Kingdom, Nos. 30562/04, 30566/04, 04.12.2008

48. Euroopa Kohus (CJEU) liidetud kohtuasjad C-293/12 and C-594/12, Digital Rights Ireland Ltd and Seitlinger and Others, 08.04.2014

49. ECtHR, S. and Marper v. United Kingdom, Nos. 30562/04 and 30566/04, 04.12.2008

50. Euroopa Kohus (CJEU), liidetud kohtuasjad C-203/15 ja C-698/15, Tele2 Sverige and Secretary of State for the Home Department, 21.12.2016

51. EIK lahend 20511/03 I v Soome

52. Euroopa Kohus (ECJ) ühendatud kohtuasjades C-446/12-C-449/12 Willems jt,

11.5. Muu kirjandus ja materjalid

53. Siseturvalisuse arengukava 2015-2020

54. Fletcher, Bevin. Brainprints: The Biometric of the Future? Laboratory Equipment, September 2016, vol 53, issue 4

55. Handbook on European Data Protection Law. 2018 Edition. Luxembourg: Publications office of the European Union, 2018

56. European Union Agency for Fundamental Rights (FRA). Fundamental rights and the interoperability of EU information systems: borders and security (2017)

57. EDPS. Opinion on the Second EU Smart Borders Package (2016)

58. Euroopa Komisjon. Ülevaade teabehaldusest vabadusel, turvalisusel ja õigusel rajaneval alal, 20.07.2010

59. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

60. The OECD Privacy Framework, 2013

61. OECD, Managing Digital Security and Privacy Risk

62. Euroopa Liidu Võrgu- ja Infoturbeameti (ENISA) juhised

63. Euroopa Andmekaitsenõukogu isikuandmete kaitse üldmäärus suunised, soovitused, parimad tavad

64. Isikuandmete töötleja üldjuhend, Andmekaitse Inspektsioon, 2018

65. Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679