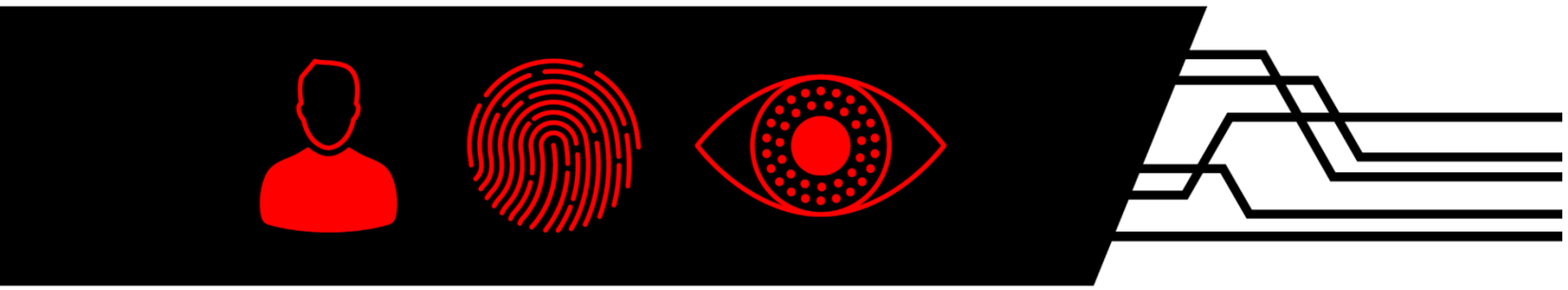


Biomeetriliste ja biograafiliste andmete alusel isiku tuvastamine ja isikusamasuse kontrollimine: ELi liikmesriikide õiguslikud regulatsioonid

Uuringu aruanne

Tallinn, juuli-oktoober 2016

Rakendusuuringu tellis Eesti Vabariigi Siseministeerium programmi “Valdkondliku teadus- ja arendustegevuse tugevdamine” (RITA) raames. Projekti rahastati 50% ulatuses RITA tegevuse kaks raames Euroopa Regionaalarengu Fondist ja 50% ulatuses Siseministeeriumi eelarvest.

Autorid / Authors:

Jekaterina Tšikova (Krabu Grupp OÜ) on identiteedihalduse ja IT-valdkonna ekspert. / Jekaterina Tšikova (Krabu Grupp LLC) is an Identity Management and IT Expert.

Mari Pedak (e-Riigi Akadeemia SA) on identiteedihalduse valdkonna ekspert; uuringu läbiviimise eest vastutanud projektijuht. / Mari Pedak (Estonian e-Governance Academy Foundation) is an Identity Management Expert and a Project Manager responsible for carrying out the research.

Helar Laasik (De Sapientia Partnerid OÜ) on identiteedihalduse valdkonna ekspert. / Helar Laasik (De Sapientia Partnerid LLC) is an Identity Management Expert.

Katrin Nyman-Metcalf, PhD (e-Riigi Akadeemia SA) on õigusvaldkonna ekspert; avaliku teabe ja andmekaitse valdkonna, sh identiteedihalduse valdkonna jurist. / Katrin Nyman-Metcalf, PhD (Estonian e-Governance Academy Foundation) is a Legal Expert; Public Information and Data Protection, incl. Identity Management Lawyer.

Sisukord / Table of Contents

Research "Biometric and Biographical Data-based Personal Identification and Identity Verification: Legal Regulations of European Union Member States"

Research Report Summary

The purpose of this applied research was to attain an overview of the legal regulations across the European Union (EU) and Schengen Area member states in the field of biometric and biographical data-based personal identification and identity verification, and to determine whether the cross-usage of biographical and biometric data is enabled in various proceedings in the public and private sectors.

The research covered nine EU Member States – Estonia, Austria, Holland, Latvia, Portugal, Germany, Finland and the United Kingdom, and two parties to the Schengen Agreement – Norway and Switzerland. The research was based on two main data collection methods: (primarily internet) searches via publicly available information sources and interviews with identity domain experts. In addition to legal acts, important court cases were analysed and public discussion in the field was observed. Unfortunately, the interviews did not yield the expected input, because knowledgeable identity experts were very busy due to the actuality of their domain. This issue has been compensated through the search and analysis of additional data sources.

The study showed that the processing of non-sensitive biometric and biographical data in the public sector, including their cross-use in different public sector proceedings and transfer to private entities, is only permitted if the data are necessary in fulfilling legal obligations. The rules governing the processing of sensitive, including biometric personal data, are highly restrictive: the processing of biometric data in public sector proceedings is generally prohibited, except in cases where the processing is necessary to fulfil an obligation arising from law, such as the issuance of biometric identity documents. The purpose of data processing must always be clearly defined and personal data may only be processed for this defined purpose.

With regard to the private sector, the observed countries generally do not have separate regulations for biometric data collection and processing by private parties; the same laws are applicable to everyone. Basic rules are applied in such cases: since the data subject is the owner of his/her personal data, his/her consent is required for his/her data processing. Thus, data subject consent is the main (but not the only!) mechanism for justifying the processing of personal data in private sector relations.

The main focus in both the public and private sectors should be on the balance between privacy and security when processing personal data – the proportionality and necessity of data processing must be strictly examined. Even if the data are not used today, the collection of personal data might still violate someone's privacy.

Identity management is the area over which the EU has no control, and identity management rules differ from country to country. However, identity management strategies do not recommend the creation of a unified or completely interoperable identity system. Rather, it is important to establish an adequate international technical interoperability that enables people to use secure cross-border electronic services and identity documents.

The EU is more active in regulating the electronic identity field than any other identity issue. EU regulation No. 910/2014 on electronic identification and trust services for electronic transactions in

the internal market (eIDAS) brings together a number of rules related to e-Identity and digital signature. This creates a common basis for secure electronic communication between citizens, businesses and public authorities, thereby increasing the efficiency of public and private sector internet-based services, e-Business and e-Commerce across the EU.

The EU's competence is greater in the data protection area, which is regulated by several directives and regulations, though individual member states have implemented details of these rules differently. This is one of the reasons why data protection in the EU is currently fragmented and uneven. The situation must change in 2018, when the new General Data Protection Regulation (GDPR) No. 2016/679 enters into force.

Estonia is a country with rather conservative but moderate data protection policies. Estonia provides an adequate level of data protection while leaving control over personal data in peoples' own hands and creating opportunities for the use of various public and private services.

As a result of the study, a number of recommendations and proposals for improving Estonia's identity management practices have been produced. The most important recommendations to be highlighted are the following:

- Estonia has extensive experience in the area of identity management and is a global leader in the context of e-Government. The authors of this Analysis Document, as well as many interviewed experts, recommend continuation of the current model that has been a key to the country's success, where:
    - identity management is performed by the state and in a centralised manner;
    - a person's identity is based on a personal code;
    - an identity card with electronic functionality is a compulsory national identity document;
    - a population registry is responsible for the management of a basic set of personal data, as well as for the quality and actuality of the population's personal data;
    - the identity schemes in use are based on reliable technologies (PKI) and allow people control over and responsibility for their identity.
- Travel Documents Assessment Centre should be restored in order to ensure strong identity management and help customer service representatives.
- Personal identification is not regulated by legislation in either Estonia or in the other studied countries, and the interpretation of terms varies significantly. The basic principles of personal identification should be regulated as a system of primary and secondary laws; both Personal Identification Best Practices and Identity Management Glossary should be drafted for public and private sector institutions in order to avoid semantic confusions.
- The authorities involved into the issuance of identity documents should carry out self-evaluation (Identity Management Audit) according to the "ICAO guide for assessing security of handling and issuance of travel documents", ver. 4, 2016.
- The use of the biometric data template should always be preferred to the use of direct biometric data due to security reasons – the template requires less protection.
- Estonian identity management should be compatible with the environment being created by means of the EU's current Data Protection Reform. Dialogue on the proportionality is important when applying modern technological solutions that are necessary for secure identity management, on the one hand, and protecting people's privacy and avoiding the misuse of personal data, on the other hand.

The results of this research can be used in Estonian Identity Policy planning and implementation.

The Analysis Document is public and does not contain information that would require access restrictions to be imposed.

1. Kokkuvõte

Käesoleva rakendusuuringu eesmärk oli saada ülevaade Euroopa Liidu (EL) ja Schengeni lepinguga ühinenud riikide biomeetriliste ja biograafiliste andmete alusel isiku tuvastamise ja isikusamasuse kontrollimise alasest õiguslikust regulatsioonist ning selgitada välja kas valimis olnud riikides on lubatud biomeetriliste ja biograafiliste andmete ristkasutamine avalik-õiguslikes ja eraõiguslikes suhetes.

Uuring hõlmas üheksat ELi liikmesriiki – Eestit, Austriat, Hollandit, Läti, Portugali, Rootsit, Saksamaad, Soomet ja Suurbritanniat ning kahte Schengeni lepinguga ühinenud riiki – Norrat ja Šveitsi. Uuring on tehtud kahe peamise andmete kogumise meetodi abil: otsingud (peamiselt interneti abil) avalikult kättesaadavate infoallikatest ning intervjuud identiteedi valdkonna ekspertidega. Lisaks õigusaktidele otsiti olulisi kaasusi ning jälgiti selle valdkonna avalikku arutelu. Kahjuks ei andnud intervjuud loodetud mahus sisendit, sest valdkonna aktuaalsuse tõttu on asjatundlikud identiteedieksperdid väga hõivatud ja seda tuli korvata täiendavate allikate otsimisega ja analüüsimisega.

Uuringu tulemusena selgus, et biomeetriliste ja biograafiliste andmete töötlemine, sh ristkasutamine avalik-õiguslikes menetlustes ja edastamine eraõiguslikele isikutele on lubatud vaid juhul, kui andmed on vajalikud õigusaktides sätestatud kohustuse täitmiseks. Delikaatsete, sh biomeetriliste andmete töötlemist reguleerivad reeglid on väga piiravad: biomeetriliste isikuandmete töötlemine avaliku sektori menetlustes on enamasti keelatud, välja arvatud juhul kui töötlemine on vajalik seadusest tuleneva kohustuse täitmiseks, nt biomeetriliste isikut tõendavate dokumentide väljaandmiseks. Andmetöötluse eesmärk peab olema selgelt defineeritud ja töötlemine on lubatud ainult defineeritud eesmärgil.

Erasektoris toimuva biomeetriliste andmete kogumise ja töötlemise kohta eraldi regulatsioone enamasti ei ole, kõigi suhtes kehtivad samad seadused. Siin rakendatakse põhilisi reegleid – kuna andmesubjekt on andmete omanik, siis on vajalik sellise andmetöötluse jaoks tema luba. Seega on eraõiguslikes suhetes peamiseks (kuid mitte ainsaks) isikuandmete töötlemist õigustavaks mehhanismiks andmesubjekti nõusolek.

Isikuandmete töötlemisel tuleb peamist tähelepanu pöörata tasakaalule privaatsuse ja turvalisuse vahel – peab rangelt vaatama andmete töötlemise proportsionaalsust ja vajalikkust. Isegi kui tänapäeval neid andmeid ei kasutata, võib nende kogumine igal juhul riivata privaatsust.

Identiteedihaldus on valdkond, mille üle ei ole ELil pädevust ja reeglid identiteedi suhtes erinevad riigiti. Samas ei soovita identiteedihalduse strateegiad ühtset või globaalselt täiesti interoperatiivset identiteedisüsteemi. Oluline on luua piisav rahvusvaheline tehniline interoperatiivsus, et inimesed saaksid piiriüleselt kasutada turvalisi elektroonilisi teenused ja isikut tõendavaid dokumente.

EL on elektroonilise identiteedi valdkonna reguleerimise suhtes aktiivsem kui muude identiteedikäsimuste suhtes. 2014. aastal vastu võetud eIDAS määrus muudab mitmed e-identiteedi ja digitaalallkirja kasutamisega seotud reeglid liikmesriikide vahel ühtlasemaks. See loob ühise aluse turvalisele elektroonilisele suhtlusele kodanike, ettevõtjate ja ametiasutuste vahel, suurendades sellega avaliku ja erasektori internetipõhiste teenuste, e-äri ja e-kaubanduse tõhusust liidus.

Andmekaitse valdkonnas on ELi pädevus suurem ning valdkonda reguleerivad mitmed direktiivid ja määrused, aga detailides on liikmesriigid rakendanud neid eeskirju erinevalt. See on üks põhjusi, miks andmekaitse on ELis praegu killustatud ja ebaühtlane. See olukord peaks muutuma alates 2018. aastast, kui jõustub ELi uus andmekaitsemäärus nr 2016/679.

Eesti kuulub pigem mõõduka aga konservatiivse andmekaitsepoliitikaga riikide hulka, mis tagab piisava andmekaitse, jättes inimestele kontrolli nende identiteedi üle ja luues samal ajal võimalusi mitmesuguste avalike ja erateenuste kasutamiseks.

Uuringu tulemusena on koostatud mitmed soovitused ja ettepanekud Eesti identiteedihalduse valdkonna täiustamiseks. Olulisemate soovitustena võib välja tuua järgmised:

- Eesti omab identiteedihalduse valdkonnas pikaajalist kogemust ning on e-riigi kontekstis liidripositsioonil maailmas. Analüüsidokumendi autorid ja mitmed küsitletud identiteedieksperdid soovitavad jätkata Eestis seni edu garanteerinud mudeliga, kus:
    - identiteedihaldus toimub riigi poolt ja tsentraliseeritult;
    - isikute identiteet põhineb isikukoodil;
    - elektroonilise funktsionaalsusega isikutunnistus on kohustuslik siseriiklik isikut tõendav dokument;
    - rahvastikuregister on isikuandmete põhikomplekti haldaja ning andmete kvaliteedi ja aktuaalsuse eest vastutaja;
    - kasutatavad identiteediskeemid põhinevad usaldusväärsetel tehnoloogiatel (PKI) ja jätavad inimestele kontrolli ja vastutust nende identiteedi üle.
- Tugeva identiteedihalduse tagamiseks ja abiks klienditeenindajatele tuleks taastada reisidokumentide hindamise keskus.
- Ei Eestis ega teistes uuritud riikides pole isikutuvastamine seaduse tasandil reguleeritud ja kasutusel olev semantika on väga erinev. Tuleks reguleerida isikutuvastamise üldpõhimõtted seaduse ja alamate õigusaktide süsteemina, koostada avaliku ja erasektori asutuste jaoks isikutuvastamise head tavad ja identiteedihalduse sõnastik vältimaks semantilisi probleeme.
- Tuleks viia Eestis läbi enesehindamine (identiteedihalduse auditeerimine) vastavalt „ICAO guide for assessing security of handling and issuance of travel documents“ ver 4, 2016.
- Otseste biomeetriliste andmete kasutamisele tuleb turvalisuse huvides eelistada alati biomeetriliste andmete malli kasutamist, kuna malli tuleb vähem kaitsta.
- Eesti identiteedihaldus peab olema vastavuses ELi andmekaitsereformiga loodava keskkonnaga. Oluline on dialoog proportsionaalsuse üle, rakendades turvaliseks identiteedihalduseks vajalikke kaasaegseid tehnoloogilisi lahendusi ühelt poolt ning kaitstes inimeste privaatsust ja vältides andmete mistahes väärkasutamist teiselt poolt.

Uuringu tulemusi saab kasutada Eesti identiteedipoliitika planeerimisel ja realiseerimisel.

Analüüsidokument on avalik ega sisalda infot, millele oleks vaja kehtestada ligipääsupiirang.

2. Sissejuhatus

Veel kümme aastat tagasi ei osatud Euroopa ega maailma tasemel hinnata identiteedihalduse tähtsust. Maailma globaliseerumine ning infoühiskondade teke ja areng on selle valdkonna toonud rambivalgusesse. Maailma arenguorganisatsioonid ja Euroopa Liit on identiteedihalduse kuulutanud üheks arenguprioriteediks.

Joonis 1. ÜRO säästva arengu eesmärgid aastani 2030

ÜRO säästva arengu üks eesmärke aastani 2030[1] on kindlustada kõigile maailma elanikele juriidiline identiteet (inglise keeles *Legal identity*), sh kõigi sündide registreerimine. Selle, eesmärgi nr 16.9[2] näol on tegemist äärmiselt ambitsioonika ülesandega, sest käesoleval ajal ei oma 1,5 miljardit maakera elanikku mingit ametlikku identiteeti ei paberil ega digitaalselt[3]. See "identiteedilõhe" ei võimalda kõigil inimestel osaleda poliitilises, majanduslikus ja sotsiaalses sfääris.[4] Teisiti öeldes, ei saa juriidilise identiteedita inimesed avada pangaarveid, saada haridust või meditsiinilist abi, nad on ilma pensionita või võimaluseta pöörduda oma huvide kaitseks kohtusse.[5] Arengueesmärgi täitmine eeldab, et maailmas on loodud ühine arusaam identiteedist kui sellisest ning identiteedihaldusest kui tervikust. Samad töövahendid ei sobi vähese kirjaoskusega ühiskondadele ja infoühiskondadele, ometi – elades ühel ja samal planeedil – peavad nemadki omavahel suhtlema.

Euroopa Liit jõudis identiteedihalduse tähtsuse mõistmiseni läbi digitaalse ühisturu arendamise. 1990. aastal vastu võetud digitaalallkirja direktiivile[6] pandud suured lootused ei täitunud, sest tehnilise infrastruktuuri arendamise kõrval ignoreeriti isikutuvastamise tähtsust. Läbimurdeni jõuti alles 2014. aastal, mil kehtestati (otsekohalduv) regulatsioon[7], millega liikmesriike suunatakse arendama identiteedihaldust ja vastastikku identiteete tunnustama.

Identiteedihaldus ei ole oluline ainult õiguste realiseerimise või võimaluste loomise seisukohast. Automatiseeritud töövahendid võimaldavad protsesse ka kiirendada. Kuid samal ajal tekib võimalus ka andmete kiiremaks ja suuremahulisemaks väärkasutamiseks. See tähendab, et mistahes uute

[1] http://www.terveilm.ee/leht/blogi/saastva-arengu-eesmargid-ja-eesti-milline-on-meie-agenda-2030/

[2] ÜRO säästva arengu 16. eesmärk on "õiglaste, rahumeelsete ja kaasavate ühiskondade edendamine" ja alameesmärk 16.9 on "Anda 2030. aastaks kõikidele inimestele õiguslikult määratletud identiteet, sealhulgas registreerida kõik sünnid". Vt http://www.terveilm.ee/leht/teabekeskuse-teemad/eesmark-oiglaste-rahumeelsete-ja-kaasavate-uhiskondade-edendamine/

[3] Estimates by the ID4D Group at the World Bank, 2015.

[4] Gelb, A. & Clark, J. 2013. "Identification for Development: The Biometrics Revolution," Center for Global Development; World Bank. 2016. Identification for Development Strategic Framework.

[5] Draft "Declaration of Common Principles. Identification for Sustainable Development: Toward the Digital Age"

[6] Hetkel kehtetu "EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV 1999/93/EÜ elektroonilisi allkirju käsitleva ühenduse raamistiku kohta"

[7] eIDAS ehk EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) nr 910/2014, 23. juuli 2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ

identiteediga seotud meetodite kasutusele võtmisel peab esiplaanile seadma inimeste privaatsuse ja turvalisuse.

Eesti kuulub identiteedivaldkonnas maailma juhtivate riikide hulka, kus juba 1990-nendatel aastatel määrati olulised identiteedihalduse komponendid kindlaks ja kus alates 2002. aastast on efektiivselt ja turvaliselt toiminud digitaalse identiteedi haldus. Nii identiteedi- kui sellega otseselt seotud isikut tõendavate dokumentide poliitika kujundamine on kuulunud Siseministeeriumi pädevusse.

„Eesti infoühiskonna arengukava 2020“ sisaldab infoühiskonna arendamise põhimõtetes nõuet tagada kasutajate turvatunne ning säilitada inimeste põhiõiguste, isikuandmete ja identiteedi kaitse. „Eesti siseturvalisuse arengukava 2015-2020“ alaeesmärkideks on usaldusväärne ja turvaline identiteedihaldus, mis saavutatakse kasutajasõbraliku ja turvalise identiteedihaldussüsteemi loomise kaudu. Turvalise ja tõhusa identiteedihaldussüsteemi baaskomponendiks on identiteedihaldust reguleerivad õiguslikud alused.

Nagu juba öeldud, kujundati Eesti identiteedihalduse põhijooned välja juba 2000-ndate aastate alguses. Tolle ajal eeldati, et kasutusele võetud tehnoloogiate (eelkõige krüptograafia valdkonnas) areng toimub kiiremini ja suured muudatused tuleb sisse viia nelja-viie aasta pärast. Sellist murrangut toimunud ei ole ja süsteem funktsioneerib (eriti kui võrrelda teiste riikidega) üsna stabiilselt. See omakorda annab võimaluse süsteemselt arendada tõsikindla füüsilise isiku tuvastamise, identiteedi loomise ja isikusamasuse kontrollimise protsesse. Parim viis on alustada maailma parimate praktikate uurimisest.

Uuringu esmane **eesmärk** ongi saada ülevaade Euroopa Liidu (edaspidi *EL*) ja Schengeni lepinguga ühinenud riikide biomeetriliste ja biograafiliste andmete alusel isiku tuvastamise ja isikusamasuse kontrollimise alasest õiguslikust regulatsioonist. Uuringu valimis on üheksa EL liikmesriiki (Eesti, Suurbritannia, Läti, Holland, Austria, Portugal, Rootsi, Saksamaa, Soome) ja kaks Schengeni lepinguga ühinenud riiki (Norra ja Šveits).

Teine **eesmärk** on välja selgitada kas ja kuidas on nimetatud riikides lubatud erinevate avalik-õiguslike ja eraõiguslike menetluste käigus kogutud biomeetriliste ja biograafiliste andmete ristkasutamine suhetes riigiga, eraõiguslikes suhetes ning erinevate valdkondade menetluste vahel (riik vs riik/EL institutsioon, riigiasutus vs riigiasutus, riik vs erasektor, erasektor vs erasektor).

Uuringu „Biomeetriliste ja biograafiliste andmete alusel isiku tuvastamine ja isikusamasuse kontrollimine: EL liikmesriikide õiguslikud regulatsioonid“ tegid Eesti Vabariigi Siseministeeriumi tellimusel Krabu Grupp OÜ, e-Riigi Akadeemia SA ja De Sapientia Partnerid OÜ.

2.1. Kasutatud mõisted

Mõiste/lühend	Kirjeldus
AKA, andmekaitseasutus, järelevalveasutus (ingl. *Data Protection authority, DPA, supervisory authority*)	Sõltumatu riiklik andmekaitseasutus, mis tegeleb kõigi isikuandmete töötlemisega seotud tegevuste järelevalvega. Igas ELi liikmesriigis AKA loomise kohustus tuleneb andmekaitsedirektiivist
Andmekaitse eest vastutavad isikud (ingl. *Data Protection Officer, DPO*)	Mitmetes riikides on asutused ja ka eraettevõtted määranud andmekaitse eest vastutavaid isikuid, kes vastutavad andmekaitsega seotud õigusaktide jälgimise eest
Andmekaitsedirektiiv 95/46/EÜ	Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba

	liikumise kohta. Direktiiviga kehtestatakse reguleeriv raamistik, et saavutada tasakaal üksikisiku privaatsuse kõrgetasemelise kaitse ja isikuandmete vaba liikumise vahel Euroopa Liidus (EL). Seetõttu on direktiiviga kehtestatud ranged piirangud isikuandmete kogumise ja kasutamise suhtes ning iga ELi liikmesriik peab asutama sõltumatu riikliku andmekaitseasutuse, mis tegeleb kõigi isikuandmete töötlemisega seotud tegevuste järelevalvega. Direktiiv asendatakse nn isikuandmete kaitse üldmääruse ehk Euroopa Parlamendi ja Nõukogu määrusega (EL) 2016/679 "Füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta" (vastu võetud 27.04.2016, ülevõtmise tähtaeg 25.05.2018)
Andmesubjekt	Tuvastatav või tuvastatud isik
Artikli 29 töörühm	Kõikide liikmesriikide andmekaitseasutuste kui ka Euroopa Andmekaitseinspektori esindajatest koosnev sõltumatu nõuandeorgan, mis on asutatud Andmekaitsedirektiivi artikli 29 alusel ning üksikisikute kaitseks seoses isikuandmete töötlemisega
Biomeetrilised isikuandmed	Delikaatsete isikuandmete erikategooria. Konkreetse tehnilise töötlemise abil saadavad isikuandmed isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist, näiteks näokujutis ja sõrmejälgede andmed
BSN (holl. *Burgerservicenummer*)	Kodaniku teenindusnumber
CIO	Informatsiooni juhtivföderaalametnik (*ingl. Chief Information Officer)*, Digitaalse Austria föderaalplatvormi (ingl. *Die Plattform Digitales Österreich*) esimees
Delikaatsed isikuandmed, tundlikud isikuandmed	Isikuandmete erikategooria: isikuandmed, mis paljastavad rassilist või etnilist päritolu, poliitilisi vaateid, usulisi või filosoofilisi veendumusi, ametiühingusse kuulumist, tervislikku seisundit või seksuaalelu käsitlevad andmed ning biomeetrilised isikuandmed
eIDAS	Euroopa Parlamendi ja Nõukogu määrus (EL) 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ. Määrus ühtlustab Euroopa Liidu elektroonilise identiteedi ja digitaalallkirja kasutamise põhimõtteid ning rakendub täies mahus 2018. aasta septembris
E-identiteet, elektrooniline identiteet, digitaalne identiteet, eID	Isikusamasuse kasutamine elektroonilises (digitaalses) keskkonnas
eIDM	Hollandi organisatsiooniline ja tehniline isikute identiteedi-atribuutide defineerimise, määratlemise ja administreerimise taristu
EL, liit	Euroopa Liit
Elektrooniline allkiri	Digitaalallkiri

Elektrooniline isikut tõendav dokument, elektrooniline dokument	Elektroonilises keskkonnas isikutuvastamist võimaldav isikut tõendav dokument
Euroopa Andmekaitseinspektori institutsioon (ingl. *European Data Protection Supervisor, EDPS*)	ELi Institutsioon, mille eesmärk on tagada, et ELi institutsioonid ja asutused järgiksid isikuandmete töötlemist reguleerivaid rangeid andmekaitseeskirju ja tagaksid isikuandmete töötlemisel inimeste õigust eraelu puutumatusele
Füüsiline identiteet	Isikusamasuse kasutamine füüsilises keskkonnas
Identiteet, isikusamasus	Omaduste hulk, mis teeb isiku unikaalseks võrreldes teiste isikutega ja kajastab konkreetseks sünnipäraseks isikuks olemist ehk ühe kindla isiku järjepidevat iseendaks olemist. See on konkreetse isikuandmete komplekti lahutamatu kuulumine konkreetse füüsilise keha juurde
Identiteedihaldus (ingl. *Identity management*)	Vajalike identiteetide atribuutide elutsükli, väärtuste ja võimalike metaandmete haldamise protsessid ja poliitikad. Hõlmab kogu identiteediteabe (sh isiku tuvastamise ja isikusamasuse kontrolli) ja identiteedi tagamist
Isikuandmed, andmed	Mistahes info andmesubjekti kohta
Isikuandmete kaitse üldmäärus (*General Data Protection Regulation, GDPR*)	Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (vastu võetud 27.04.2016, ülevõtmise tähtaeg 25.05.2018). Määruse eesmärk on tugevdada ja ühtlustada andmekaitse ELis ning reguleerida isikuandmete edastamist väljapoole ELi andmaks elanikele tagasi kontrolli nende isikuandmete üle ja lihtsustamaks regulatiivset keskkonda rahvusvahelise äri jaoks. Määrus sisaldab erandeid töötajate isikuandmete töötlemise ja riigi julgeoleku tagamiseks töötlemise jaoks – neid valdkondi võib endiselt reguleerida riigi tasemel
Isikuandmete piiriülene edastamine (ingl. *Cross-Border Transfer of Personal Data*)	Isikuandmete edastamine või edastamiste kogum kolmandasse riiki, mis ei ole ELi liikmesriik
Isikuandmete piiriülese edastamise tüüptingimused (ingl. *Standard Conditions for Cross-Border Transfer of Personal Data*)	Isikuandmete piiriülese edastamise tüüptingimisi kirjeldab andmekaitsedirektiivi peatüki IV „Isikuandmete edastamine kolmandatesse riikidesse“ artiklid 25 ja 26
Isikuandmete töötlemine (ingl. *Personal data processing*)	Iga isikuandmetega tehtav toiming või toimingute kogum, olenemata sellest, kas see on automatiseeritud või mitte, näiteks kogumine, salvestamine, korrastamine, säilitamine, kohandamine või muutmine, väljavõtete tegemine, päringu teostamine, kasutamine, üleandmine, levitamine või muul moel avaldamine, ühitamine või ühendamine, sulgemine, kustutamine või hävitamine (vastavalt andmekaitsedirektiivi artiklile 2 (b))
Isikuandmete töötlemise tüüptingimused (ingl. *Standard Conditions for Personal Data Processing*)	Mittedelikaatsete isikuandmete töötlemise tüüptingimisi kirjeldab andmekaitsedirektiivi artikkel 7 ning delikaatsete, sh biomeetriliste isikuandmete töötlemise tüüptingimusi – sama direktiivi artikkel 8
(Isiku)andmetega seotud rikkumine (ingl. *Data breach*)	Turvanõuete rikkumine, mis võib põhjustada üksikisikutele füüsilise, materiaalse või mittemateriaalse kahju, nagu kontrolli kaotamine oma isikuandmete üle või õiguste piiramine, juhuslik või ebaseaduslik hävitamine, kaotsiminek, muutmine,

	diskrimineerimine, identiteedivargus või pettus, rahaline kahju, pseudonümiseerimise loata tühistamine, maine kahjustamine, ametisaladusega kaitstud andmete konfidentsiaalsuse kadu või mõni muu majanduslik või sotsiaalne kahju asjaomasele üksikisikule
Isikukood	Isikukood on riigi poolt kodanikele, alaliselt riigis elavatele isikutele ja e-residentidele antav unikaalne numbrikombinatsioon, mille järgi on isikut võimalik tuvastada. Isikukoodid moodustatakse eri riikides erinevalt
Isikutuvastus, isikusamasuse tuvastus, isiku identifitseerimine (ingl. *Personal identification*)	Isikusamasuse tõestamine – protsess, mille käigus pädev avalik-õiguslik asutus veendub põhjalike järelpäringute tulemusel, et isik on see, kes ta väidab ennast olevat
Isikusamasuse kontroll (ingl. *Identity verification*)	Isiku (väidetava) identiteedi kontroll; kontrollprotseduur, mille käigus võrreldakse isikut ja talle pädeva asutuse poolt välja antud dokumenti (milleks võib olla isikut tõendav dokument, elektrooniline sertifikaat, salajane võti vms) eesmärgiga veenduda, et isik on see, kes ta väidab ennast olevat
ITD	Isikut tõendav dokument
Küpsised (ingl. *Cookies*)	Väike tekstifail, mille veebisait salvestab kasutaja arvutisse või mobiilseadmesse, kui kasutaja saiti külastab. See võimaldab veebisaidil teatud ajavahemikuks jätta meelde kasutaja toimingud ja eelistused (näiteks kasutajanimi, keel, kirjasuurus ning muud eelistused kuvamisel)
Lepingu tüüptingimused, andmeedastusleping (ingl. *Standard contractual clauses, = Model clauses*)	Lepingu tüüptingimused isikuandmete vastutava ja vastutava töötleja vahel, mille alusel ebapiisava andmekaitse tasemega välisriigis asuv andmete vastuvõtja tagab, et täidab Andmekaitsedirektiivis kehtestatud isikuandmete kaitse nõudeid. Lepingu tüüptingimuste vastuvõtmine ei takista ettevõtjatel kasutada muid vahendeid, nagu juhtumipõhiseid lepingulisi kokkuleppeid, selle tõestamiseks, et nad kasutavad andmete edastamisel piisavaid tagatisi Andmekaitsedirektiivi artikli 26 lõike 2 tähenduses
LR, liikmesriik	Euroopa Liidu liikmesriik
Lähiväljaside (ingl. *Near Field Connection, NFC*)	Kontaktivaba kiibiliidese edasiarendus, mis võimaldab raadiosageduslikus lähiväljas (sagedusel 13.56 MHz) toimivaid kontaktivabasid andmevahetusseansse, kasutatakse autentimis- ja makselahenduste puhul
MKM	Eesti Vabariigi Majandus- ja Kommunikatsiooniministeerium
MoC (ingl. *Match-on-card*)	MoC on sõrmejälgede kaartidel hoidmise ja võrdlemise kontseptsioon, mis tõendab kaardiomaniku füüsilist kohalolekut ja tagab selle abil turvalise isikutuvastuse (http://www.matchoncard.com/what-is-moc)
Määrus 2252/2004 biomeetriliste reisidokumentide kohta	Nõukogu määrus (EÜ) 2252/2004 liikmesriikide väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta ja eelnimetatud määruse muudatused – kirjeldab biomeetriliste reisidokumentide tehnilisi nõudeid
PPA	Eesti Vabariigi Politsei- ja Piirivalveamet
Privacy Shield, *EU-US Privacy Shield*	Uus Atlandiüleseid andmevoogusid reguleeriv andmekaitseraamistik (lõplik versioon kinnitatud 2016. aasta juulis artikkel 31 komitee poolt), mis asendab Euroopa kohtu 6.10.2015 tühistatud *Safe Harbor* andmevahetuslepet. *Privacy*

	*Shield*iga kehtestatakse võrreldes *Safe Harbor*iga rangemad kohustused USAs asuvatele ettevõtetele, mis peavad kaitsma Euroopa Liidu residentide isikuandmeid. Samuti pannakse uue korraga USA kaubandusministeeriumile ja föderaalsele kaubanduskomisjonile rangema seire ja täitmise tagamise kohustus, mille jaoks tuleb muu hulgas teha tihedamat koostööd Euroopa andmekaitseasutustega
Pseudonümiseerimine	Isikuandmete töötlemine sellisel viisil, et isikuandmeid ei saa enam täiendavat teavet kasutamata seostada konkreetse andmesubjektiga tingimusel, et sellist täiendavat teavet hoitakse eraldi ja andmete tuvastatud või tuvastatava füüsilise isikuga seostamise vältimise tagamiseks rakendatakse tehnilisi ja korralduslikke meetmeid
Registreerija (ingl. *Registration Authority*, *RA*)	Registreerija sertifitseerimispoliitika mõistes
RIA	Eesti Vabariigi Riigi Infosüsteemi Amet
Safe Harbor	ELi ja USA vahel kehtinud andmekaitselepe, mille tühistas Euroopa kohus 6.10.2015, kuna see ei taganud tegelikkuses sellist piisavat andmekaitse taset, nagu seda nõuab ELi õigus. Seda asendas 2016. aasta juulis uus andmevoogusid reguleeriv andmekaitseraamistik *Privacy Shield*
Siduvad ettevõtluseeskirjad (ingl. *Binding corporate rules*)	Euroopa isikuandmete kaitse standardi põhjal koostatud tegevusjuhend, mille on heaks kiitnud vähemalt üks andmekaitseasutus, mille rahvusvahelised organisatsioonid koostavad vabatahtlikult ja mida nad vabatahtlikult järgivad, et tagada isikuandmete nõuetekohane kaitse andmete edastamisel või teataval viisil edastamisel äriühingute vahel, mis kuuluvad samasse kontserni ja mis on omavahel seotud asjaomaste eeskirjadega. Neid ei reguleerita sõnaselgelt direktiiviga 95/46/EÜ, kuid need on praktikas välja kujunenud andmekaitseasutuste tegevuse tulemusel ja artikli 29 töörühma toetusel
SK	Sertifitseerimiskeskus AS
SM	Eesti Vabariigi Siseministeerium
STO (ingl. *Certification Authority*, *CA*)	Sertifitseerimisteenuse osutaja
SDG *(*ingl. *Sustainable Development Goal*)	ÜRO säästva arengu eesmärgid
Tagatistase, (ingl. *Level of Assurance, LoA*)	Tase, millel osapool on teatava kindlusega võimeline määratlema, et elektroonilist kinnitust, mis esindab inimest või masinat, kellega/millega ta tehingusse astub, võib usaldada tegelikult kuuluvat sellele isikule või masinale
Tõendiväärtus, tõestusväärtus (ingl. *Evidential Value*)	Teabeüksuse võime tõestada fakte ta loomise, sh looja ja sisu kohta
Tüüptingimused	Olenevalt kontekstist võivad tähendada: a. lepingu tüüptingimusi, b. isikuandmete piiriülese edastamise tüüptingimusi, c. isikuandmete töötlemise tüüptingimusi.

Valge nimekiri	Loetelu kolmandatest riikidest, mille andmekaitse taseme on Euroopa Komisjon lugenud vähemalt samaväärseks ELi omaga. Uuringu koostajate parimal teadmisel on Komisjon kinnitanud, et isikuandmete piisavat kaitset Andmekaitsedirektiivi artikli 25 lõike 6 alusel tagavad Andorra, Argentina, Austraalia, Kanada (kommertsasutused), Šveits, Fääri saared, Guernsey, Iisrael, Mani saar, Jersey, Uus-Meremaa, Uruguay ja ELi-USA vahelise programmi EU-US Privacy Shield põhimõtted
Vastutav töötleja (ingl. *Data controller*)	Füüsiline või juriidiline isik, riigiasutus, esindused või mõni muu organ, kes määrab üksi või koos teistega kindlaks isikuandmete töötlemise eesmärgid ja vahendid; kui töötlemise eesmärgid ja vahendid on kindlaks määratud siseriiklike või ühenduse õigusnormidega, võib vastutava töötleja või tema ametisse määramise sätestada siseriiklikus või ühenduse õiguses
Videovalve (ingl. *Closed Circuit Television, CCTV*)	Foto- ja/või videosalvestus seadmete ja tarkvara kasutamise abil videovalve piirkonnas ning foto- ja/või videosalvestuse säilitamine ja töötlemine
Volitatud töötleja (ingl. *Data processor*)	Füüsiline või juriidiline isik, riigiasutus, esindused või mõni muu organ, kes töötleb isikuandmeid vastutava töötleja nimel

2.2. Uuringu metoodika

Uuringu metoodika on valitud arvestades uuringu mahtu ja selleks võimaldatud aega, mis suures osas langes Euroopa (ekspertide) suvepuhkuste aega.

Esimene samm ülevaate saamiseks riikide õigusruumist on analüüsitava valdkonna avalikult kättesaadavate **õigusaktide kogumine**. Seaduste kogumine viidi läbi deskriptiivse, struktureeritud ja objektiivse meetodiga, mis tähendab, et tehti nimekiri olulistest seadustest ilma neid kommenteerimata. Eesmärgiks seati oluliste seaduste ülesleidmine ja kaardistamine, sest sama valdkonda reguleerivad seadused võivad eri riikides olla erinevate nimetuste ja struktuuriga. See tähendab, et kuigi enamus riikides on olemas valdkonna õiguslik regulatsioon, ei ole alati olemas sama nimetusega seadusi või muid õigusakte. Selle tõttu vaadati seaduse nimetusest sügavamale, et reguleerimise valdkonnast õigesti aru saada, aga rohkemat analüüsi ei tehtud.

Peamiseks andmete kogumise tööriistaks oli internetiotsing. Nii suures ulatuses, kui võimalik, kasutati ametlikke allikaid nagu õigusaktide kogumikud, ametkondade kodulehed jne. ELi materjalid on kergesti kättesaadavad ELi kodulehtedel või seal jagatud viidete kaudu. ELi kodulehed pakuvad rohkesti materjali ka liikmesriikide kohta. Osade riikide kohta oli raske leida andmeid ja/või oli raske aru saada, kas pakutavad andmed on aktuaalsed. Osaliselt õnnestus seda korvata intervjuude kaudu, kuid kahjuks ei õnnestunud saada rahuldavaid vastuseid kõikidest uuringus käsitletud riikidest ja teemadest.[8] Rahuldavaid vastuseid ei saadud Austriast, Šveitsist, Portugalist ja Norrast, kuigi päringuid korrati ja saadeti mitmele erinevale eksperdile. Jätkusid tööd täiendavate allikate otsimiseks ja kasutati ka näiteks advokaadibüroode ja konsultatsioonifirmade tehtud eri riikide **õigusruumi ülevaateid**. Seda meetodit kasutati ka nende riikide puhul, mille kohta vastuseid saada ei olnud võimalik. Ka anti vastustega vähe infot biomeetria kasutamise kohta, kuigi väljasaadetud küsimustikes oli biomeetria eraldi ära mainitud. Ükski vastajatest ei viidanud õigusaktidele, kuigi mõni riik, nt Suurbritannia ja Rootsi kirjeldasid riigi sellealast praktikat (Suurbritannia reisidokumentide väljastamisel, Rootsi kirjavahetuse pidamisel). Meeskond saatis välja jätkuküsmused, millega püüti saada täiendavat tagasisidet biomeetria kohta uurimise all olevatest riikidest.

Intervjuudes kasutati tõendimaterjalil põhinevat meetodit, mis tähendab, et iga väite suhtes küsiti viidet allikale, eelkõige viidet seadusele, ametkonna nimele ja kodulehele vms. Käsitletavates riikides on õigusaktid üldjuhul avalikult elektrooniliselt kättesaadavad nii üldistest seaduste andmebaasidest (elektroonilised andmebaasid ei ole mitmes riigis ametlikud seaduse allikad) kui ka ametkondade kodulehtedelt. Intervjuude käigus kontrolliti varem kogutud materjali aktuaalsust, kui see oli olnud ebaselge. Uurimismeeskond andis kaaskirjas ka selgesti teada, et uuring viiakse läbi riigi tellimusel ning piiratud ligipääsu sisaldava infoga vastuseid ei avalikustata. Vaatamata sellele ei sisaldanud vastused piiratud ligipääsuga infot. Seega ei sisalda analüüsidokument ka infot, millele oleks vaja kehtestada ligipääsupiirang.

Kohtulahendite leidmise metoodika kohaselt pakkusid huvi eelkõige rahvusvaheliste kohtute – Euroopa Liidu Kohus ning Euroopa Inimõiguste Kohus – lahendid. Säärased kohtulahendid on teatud määral alati algatatud siseriiklike juhtumite jätkuna, nii et need pakuvad üldisemat pilti sellest, mis Euroopa õiguse (laias mõistes) alusel vastuvõetav on. Osalt nimetatakse ka riikide kohtulahendeid, eriti, kui intervjueeritavad mainisid olulisi otsuseid. Kohtulahenditele lisaks võivad omada tähtsust

[8] Sama probleemi ees seisid uurijad, kes viisid 2015. aastal MKM-i tellimusel läbi digitaalallkirja kasutamise uuringut. Kehtivate sertifikaatide arvu väljaselgitamisel ei saadud piisavalt infot Hispaania, Prantsusmaa, Saksamaa, Portugali, Itaalia ja Kreeka puhul.

ka eri asutuste otsused. Igasugused otsused on illustratsiooniks, mida tähendavad ja kuidas tõlgendatakse seadusi, aidates aru saada, mis võib olla hea mudel ka praktikas.

Varasemate uuringute – s.t. sekundaarsete allikate – valik on tehtud subjektiivselt, valides neid uuringuid, mille osas käesoleva uuringu autorid leidsid, et need annavad lisandväärtust/taustainfot õigusaktidele, kohtulahenditele ja muudele primaarsetele allikatele.

Intervjuudele eelnes kontaktisikute otsimine, kaardistamine ja valitud isikutega kontakti loomine. Kirjalike intervjuude läbiviimiseks töötati välja küsimustik (vt lisa 1). **Intervjuud viidi läbi** biomeetriliste ja biograafiliste andmete kasutamise valdkonna juristide ja ekspertide-praktikutega. Küsimustikule vastajate loetelu on toodud lisas 2. Intervjueeritavate otsimiseks kasutati isiklikke tööalaseid kontakte ning samuti avalikult kättesaadavaid kontakte, mida otsiti identiteedihalduse eest vastutavate ametite kodulehtede ja professionaalse sotsiaalvõrgustiku LinkedIn[9] kaudu. Eriti väärtuslikud olid kohtumised Eesti digitaalse identiteedi ekspertidega ja saab väita, et Eesti ekspertidel on olemas parimad teadmised ja kogemused.

[9] LinkedIn on maailma suurim professionaalidele orienteeritud sotsiaalvõrgustik, millel on üle 400 miljoni kasutaja.

3. Riikide identiteedihalduse õigusaktid ja praktika

Käesolev peatükk on deskriptiivne ehk siin kirjeldatakse ELi ja eri riikide olukorda. Peatüki koostamisel kasutatud õigusaktide loetelu on lisas 3. Õigusaktide analüüsimisel tehtud järeldusi, võrdlusi ja ettepanekuid leiab ka järgmistes peatükkides.

Identiteedivaldkonnas analüüsiti järgnevaid teemasid (ja samas loogilises järjekorras on ka ülevaade koostatud) – grupp A:

- Identiteedihaldust reguleerivad õigusaktid;
- identiteedihalduse korraldus (pädev amet);
- isiku identiteedi loomine;
- elektrooniline identiteet, mitmetasemeline identiteet.

Grupi A jaoks otsiti vastuseid järgmistele küsimustele:

1) Millistel õigusaktidel ja poliitikadokumentidel (edaspidi *Õigusaktid*) põhineb uuringu fookuses olevate riikide identiteedihalduspoliitika?
2) Kas isikute identiteete hallatakse keskselt ja millise asutuse pädevusse see kuulub?
3) Millistel algandmetel põhineb isiku identiteedi loomine, kuidas see on korraldatud ja kuidas on tagatud mitme identiteedi tekkimise ja kasutamise vältimine?
4) Kas ja kui, siis kuidas on riigis korraldatud teiste EL liikmesriikide ja kolmandate riikide määratletud identiteetide õigsuse kontrollimine?
5) Kas riigis on kasutusel elektrooniline identiteet (digitaalne isikut tõendav dokument) ja kui on, siis kas isiku elektrooniline identiteet põhineb füüsilisel identiteedil ja kuidas see on tagatud?
6) Kuidas hallatakse mitmetasemelisi identiteete ehk ingl. k. *derivative identity*? Millised on nendevahelised seosed, kasutamise valdkonnad ja reeglid?
7) Kuidas on korraldatud seaduslikult toimuv identiteetide muutmine (tunnistajakaitse alla võetud isikud, politseiagendid jt) ja välistatud nende kattumine õigete identiteetidega, kui toimub biomeetriliste andmete töötlemine?

Ülejäänud uuringu osa oli korraldatud järgmiselt – grupp B:

- õigusaktid isikuandmekaitse kohta;
- õigus avalik-õiguslike ja eraõiguslike menetluste käigus kogutud identiteedi andmeid, sealhulgas biomeetrilisi andmeid kasutada eraõiguslikes ja avalik-õiguslikes menetlustes ning edastada eraõiguslikele isikutele;
- õigus identiteedi andmeid, sealhulgas biomeetrilisi andmeid edastada teistele riikidele ja rahvusvahelistele organisatsioonidele (isikuandmete piiriülene edastamine).

Grupi B jaoks otsiti vastuseid järgmistele küsimustele:

1) Millistes avalik-õiguslikes menetlustes ja millistel tingimustel on lubatud isiku identiteedi andmete, eelkõige biomeetriliste andmete töötlemine?
2) Kas eraõiguslikel isikutel on eraõiguslikes suhetes õigus koguda, säilitada ja kolmandatele isikutele edasi anda isiku identiteedi andmeid, sealhulgas biomeetrilisi andmeid ja kui, siis millises ulatuses ja millistel tingimustel?
3) Millistel õigusaktidel ja poliitikadokumentidel (edaspidi *Õigusaktid*) põhineb uuringu fookuses olevate riikide andmekaitsepoliitika?

4) Kuidas on korraldatud isikuandmete kaitse? Millised on õiguslikud piirangud isikuandmete kogumiseks ja töötlemiseks?
5) Kas ja kui, siis millistel tingimustel on lubatud erinevate avalik-õiguslike menetluste käigus kogutud isiku identiteedi andmete, sealhulgas biomeetriliste andmete ristkasutamine teistes avalik-õiguslikes menetlustes?
6) Kas ja kui, siis millistel tingimustel on lubatud erinevate eraõiguslike suhete käigus kogutud isiku identiteedi andmete, sealhulgas biomeetriliste andmete kasutamine avalik-õiguslikes menetlustes?
7) Kas ja kui, siis millistel tingimustel on lubatud erinevate avalik-õiguslike menetluste käigus kogutud isiku identiteedi andmete, sealhulgas biomeetriliste andmete edastamine eraõiguslikele isikutele?
8) Kas ja kui, siis millistel tingimustel on lubatud erinevate avalik-õiguslike menetluste käigus kogutud isiku identiteedi andmete, sealhulgas biomeetriliste andmete edastamine teistele riikidele ja rahvusvahelistele organisatsioonidele?
9) Kas ja kui, siis millised praktikad ja õigusaktid reguleerivad riikide vahel isikuandmete edastamist kriminaal- ja tsiviilmenetlustes (vastastikune õigusabi)?
10) Kuidas muutub riikide seadusandlus peale isikuandmete kaitse üldmääruse jõustumist 25.05.2018?

Et mitmete teemade osas on valimis olnud riikides olukord üsna ühesugune või ühesuguselt puudub, siis on korduste vältimiseks on osa seisukohti siinkohal käsitletud.

Nii näiteks ei ole enamikus riikides reguleeritud mitmetasemelist identiteeti ja seepärast on seda käsitletud ainult nende riikide puhul, kus vastav praktika on olemas.

3.1. Euroopa Liit

A

ELi pädevus on piiratud ja derivatiivne, st see tuleneb sellest, mis pädevust liikmesriigid on lepingute alusel Liidule loovutanud. Samas peab pädevus olema reaalne, mistõttu on ELil õigus oma seadusandlust täiendada, kui areng toob kaasa vajaduse ühtlustada reeglid valdkonnas, mille üle tal on pädevus. Identiteedihaldus on ala, kus ELil on teatud piiratud pädevus ja kus suurem osa reegleid on loodud üsna hiljuti. Andmekaitse valdkonnas on ELi pädevus suurem, mida kinnitab ka hetkel läbiviidav andmekaitsereform[10].

Kõigepealt tuleneb osaline identiteediga seotud pädevus EL ühe põhivabaduse – inimeste vaba liikumise – realiseerimisest. Inimestel peab olema võimalus tõestada oma õigust vabalt liikuda kõikide liikmesriikide poolt aktsepteeritud viisil. Sellise võimaluse loomise parim näide on reisidokumentidele ühtsete nõuete kehtestamine Nõukogu määrusega (EÜ) nr 2252/2004 liikmesriikide poolt väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta[11].

Osaline pädevus tuleneb ka Euroopa Parlamendi ja Nõukogu määrusest (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul, mis võeti vastu 23. juulil 2014. Määrusega ette nähtud vastastikuse identiteetide tunnustamise aluseks on identiteedihalduse alane koostöö.

Samas ei ole ELil pädevust identiteedihalduse kui sellise üle. See tähendab, et juriidiliselt on vajalik tihe koostöö liikmesriikide ja ELi vahel, et isikutel oleks reaalne võimalus kasutada ELi vabadusi.

Niisiis ei tegele EL identiteedi halduse kui sellisega ja selleks ei ole eraldi ametit. Üks ELi omapära, võrreldes suurema osa rahvusvaheliste organisatsioonidega, olles liikmesriikide ülene struktuur, on, et ELi õigusakte rakendavad peamiselt liikmesriikide ametkonnad. Määrused on otsekohaldatavad ja osa liikmesriikide seadusandlusest, mida liikmesriikide organid rakendavad.

ELil ei ole ka pädevust luua isikute identiteeti. Samal põhjusel ei tegele EL ka mitmetasemelise identiteediga. ELi reeglistik on ainult rakendatav nende isikute suhtes, kellele liikmesriik on loonud legaalse identiteedi.

E-teenused, e-kaubandus ja ELi tahe lihtsustada seda, teha seda kättesaadavamaks ja suurendada e-teenuste arvu on viinud selleni, et EL on elektroonilise identiteedi valdkonna reguleerimise suhtes aktiivsem kui muude identiteediküsimuste suhtes. Liikmesriigid otsustavad, kes saab teatud riigi identiteedi ja EL tegeleb sellega, et selle alusel oleks võimalik kasutada õigusi terves liidus. Direktiiv 1999/93/EÜ sätestas reegleid elektrooniliste allkirjade suhtes. Määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ on sisse toonud ühtseid ja üksikasjalikumaid reegleid elektroonilise identiteedi suhtes.

eIDAS, mis kaudselt puudutab identiteedihaldus, reguleerides riikide poolt loodud identiteetide kasutamist teenuste tarbimisel üle kogu Euroopa Liidu, rakendub täies mahus 2018. aasta

[10] http://www.aki.ee/et/eraelu-kaitse/euroopa-andmekaitse-reform

[11] Nõukogu MÄÄRUS (EÜ) nr 2252/2004, 13. detsember 2004, liikmesriikide poolt väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta

septembris. Rakendamise käigus tulevad välja regulatsiooni nõrkused ja täiendamist vajavad kohad. Nii on Eesti juhtiv eID ekspert Tarvi Martens teinud ettepaneku eristada selgelt turvalise allkirjastamise vahendi[12] väljastaja roll[13]. eIDAS paneb hetkel vastutuse STOle, mis üldjuhul ongi aktsepteeritav. Samas on juba teada mitmed näited, kus privaatvõtmed ei ole STO kontrolli all.

B

Õigus isikuandmete kaitsele on Euroopa Liidu tasandil sätestatud Euroopa Liidu põhiõiguste harta artiklis 8, mis peale Lissaboni lepingu jõustumist 2009. aastal muutus osaks ELi põhilepingutest. Harta artikkel 7 sisaldab privaatsuse kaitset. EL ning kõik liikmesriigid on ka seotud Euroopa Inimõiguste Konventsiooniga, kus artikkel 8 privaatsuse kaitse kohta ka sisaldab andmekaitset.

Euroopa liidu õiguses reguleerivad isikuandmete kaitset mitmed direktiivid ja määrused, eelkõige Andmekaitsedirektiiv – Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. Direktiiv kujutab endast reguleerivat üldraamistikku, millega kehtestatakse ranged piirangud isikuandmete kogumise ja kasutamise suhtes. Lisaks on olemas direktiivid, mis reguleerivad isikuandmete kaitset kitsamates valdkondades – nt tarbijakaitset, kasutajate kaitset elektroonilise side sektoris.

Vastavalt Andmekaitsedirektiivile peab iga ELi liikmesriik asutama sõltumatu riikliku andmekaitseasutuse (*edaspidi* AKA), mis tegeleb kõigi isikuandmete töötlemisega seotud tegevuste järelevalvega. Järelevalvet AKAde töö üle teostab Euroopa Andmekaitseinspektori institutsioon.

Andmekaitsedirektiiv asendatakse määrusega (EL) 2016/679 "Füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta", mis võeti vastu 27.04.2016 ja mille ülevõtmise tähtaeg on 25.05.2018. Oluline muudatus on, et määruse kaudu hakkavad kehtima samad reeglid kõikides ELi liikmesriikides. See peaks parandama praegust olukorda, milles on kaunis suuri erinevusi eri riikide andmekaitsedirektiivi tõlgendamises ja selle praktilises rakendamises. Põhiprintsiibid jäävad suurelt osalt samaks, aga uues reeglistikus on andmeid töötlevate subjektide vastutus luua süsteem andmete turvaliseks töötlemiseks selgem.

Kõiki identiteedi andmetega tehtavaid toiminguid peetakse Euroopa Liidu õiguse kohaselt isikuandmete töötlemiseks (artikkel 2 (b)). Andmekaitsedirektiivi artiklid 6-9 sätestavad töötlemise üldreegleid, spetsiifilisemad reeglid kehtestatakse aga siseriiklikul tasemel. Artikkel 7 kirjeldab **mittedelikaatsete isikuandmete töötlemise tüüptingimusi** ning artikkel 8 – **delikaatsete isikuandmete töötlemise tüüptingimusi**. Grupis B kasutatakse mõistet „töötlemise

[12] Turvalise allkirjastamise vahendi all mõistetakse praktilisi rakendusi, mis põhinevad asümmeetrilisel krüptograafial ja mis võimaldavad privaatvõtme loomist, säilitamist ja kasutamist.

[13] Vt Digitaalset allkirja kasutavate tööealiste (15-64-aastased) Euroopa Liidu elanike osakaalu määramine 2015. aastal. Euroopas hetkel kehtiv seadusandlus, aga ka eIDAS, eristab küll vahendit mõistena, kuid paneb vastutuse selle nõuetele vastavuse kohta STO-le. Kuigi praktikas on see paljudel juhtudel aktsepteeritav (STO-d küsivad kiipkaardi tootjalt vastava sertifikaadi ja tegutsevad selle alusel), on see olemuslikult ebakorrektne. STO põhiülesanne on sertifikaadi välja andmisel tagada, et mingi privaatvõti on just selle konkreetse omaniku valduses ning mille kohta STO väljastab omanikule vastava avaliku võtme tõendi ehk sertifikaadi. Vahendi enda kohta tema omadustele garantii andmine on aga mõnel juhul üsna keeruline ja on STO jaoks ülemäärane kohustus. Markantseks näiteks on siin Austrias kasutatav mobiilset autentimist kasutav serveripõhine e-allkirjastamise süsteem, kus privaatvõtmeid säilitatakse serveris (tõenäoliselt turvamoodulis), mida ei halda või ei pruugi hallata sertifikaadi väljaandja. Sama situatsioon tekib pea igasuguses e-allkirjastamise süsteemis, kus vahend ja sellele vastav sertifikaat antakse välja rohkem kui ühe usaldust vajava osapoole poolt.

tüüptingimused“ andmekaitsedirektiivi artiklite 6-8 tähenduses ning analüüsitakse siseriiklikku seadusandlust Euroopa Liidu õigusele vastavuse osas.

Vastavalt Andmekaitsedirektiivi artiklile 8 (1) on **delikaatsete, sh biomeetriliste isikuandmete töötlemine põhimõtteliselt keelatud**. Siiski on olemas erandid (artikkel 8 (2) ja (3)) kõnealusest keelust, nende hulka kuuluvad: andmesubjekti selgesõnaline nõusolek, eluliste huvide kaitse, õiguspärane ja vajalike garantiidega tegevus; õigusnõuete koostamine, esitamine või kaitsmine; märkimisväärne avalik huvi.

Olenemata sellest, kas tegemist on biomeetriliste või muude isikuandmetega, on töötlemise esmatingimuseks andmesubjekti nõusolek – see on reegel number üks eraõiguslikes suhetes. Kuigi nõusolek on peamine isikuandmete töötlemist õigustav mehhanism, ei ole see kindlasti ainus – kehtima jäävad ka sellised põhimõtted nagu lepingulise kohustuse või (liikmesriigi või ELi) seadusjärgse kohustuse täitmine. Põhiprintsiibiks on: **vähemalt üks** töötlemise tingimustest peab olema täidetud.

Mis puudutab isikuandmete töötlemist, sh ristkasutamist avalik-õiguslikes menetlustes ja edastamist eraõiguslikele isikutele, siis see on lubatud vaid juhul, kui andmed on vajalikud õigusaktides sätestatud kohustuse täitmiseks. Andmesubjektil on õigus saada andmete edastamisest teada ja tutvuda edastatavate andmetega.

Identiteedi andmete, sh biomeetriliste andmete kasutamise, säilitamise, ligipääsu jmt õiguslikud küsimused võivad liikmesriigid kehtestada siseriiklikul tasemel. Sealhulgas seda, kas identiteedi andmed hoitakse eraldi andmebaasis, kas toimub andmete ristkasutust teiste andmebaasidega jne. ELil ei ole pädevust andmebaaside üle. Ainuke ELi õigusakt, mis tegeleb otseselt andmebaasidega, on piiratud autoriõiguslike küsimustega[14]. Andmebaaside kasutusega seotud teemad võivad olla ELi pädevuses, aga kuidas andmeid säilitatakse ja asutuste vahel jagatakse, on liikmesriikide pädevuses.

Põhimõtteliselt peavad kõik vastutavad töötlejad andmete töötlemisest teavitama AKAd. Kõik liimesriigid võivad kehtestada erandeid, mille puhul ei ole teavitamine madala riski tõttu kohustuslik. Erandeid ja lihtsustatud teavitamise protseduure võib rakendada nende asutuste suhtes, mis on loonud sõltumatu järelevalveasutuse isikuandmete kaitse üle järelevalve teostamiseks[15].

Mitmetes riikides on asutused ja ka eraettevõtted määranud andmekaitse eest vastutavaid isikuid, kes vastutavad seaduse jälgimise eest, suhtlevad vajadusel AKAdega, koolitavad ja teavitavad andmekaitsega seotud teemadel jne.

Andmekaitsedirektiivi artiklid 25 ja 26 sätestavad töödeldavate või pärast edastamist töötlemiseks kavandatud **isikuandmete edastamise kolmandatesse riikidesse ehk isikuandmete piiriülese edastamise tüüptingimusi**. Üldreegel on, et isikuandmete edastamine on lubatud liikmesriikidest kolmandatesse riikidesse, kus on tagatud andmete piisav kaitse. Kuigi edastamine ei tohiks toimuda, kui ei ole tagatud piisavat kaitset, on direktiivis selle reegliga seoses loetletud mitmeid erandeid, nt kui andmesubjekt ise annab edastamiseks nõusoleku, kui see on vajalik üldiste huvidega seotud põhjustel, lepingu sõlmimise korral, aga ka juhul, kui liikmesriik on kinnitanud ettevõtetele **siduvaid eeskirju** või **lepingu tüüptingimusi**.

[14] EUROOPA PARLAMENDI JA NÕUKOGU 11.03.1996 DIREKTIIV 96/9/EÜ andmebaaside õiguskaitse kohta

[15] EUROOPA PARLAMENDI JA NÕUKOGU 18.12.2000 MÄÄRUS (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta

Andmete edastamisel kolmandatesse riikidesse on oluline, kas nendes riikides on piisav andmekaitse tase, mis küll võib olla teistsugune kui ELis, aga peab tagama samaväärse andmekaitse taseme. EL võib otsustada, et teatud riik on piisavalt sarnasel tasemel – adekvaatsuse otsus – mille järgi selle riigiga tohib andmeid vahetada, kuna riik on nn „valges nimekirjas“. Andmete edastamise üldreeglid on ELi liikmesriikides samad, kuna otsus andmekaitse taseme kohta tehakse ELi tasemel ja kehtib kõikidele liikmesriikidele.

3.2. Austria

A

Austrias on peamiseks digitaalset identiteeti reguleerivaks aktiks „Austria e-valitsuse seadus“[16], mille 2. osa reguleerib identifitseerimist ja autentimist, samuti erinevate isikukoodi liikide kasutamist (isikukood, lähte-isikukood, sektoripõhised isikukoodid).

Föderaaltasandil koordineerib e-riigi arenguid Föderaalne Riigikantselei (*Federal Chancellery*), kogu tegevus toimub „Digital Austria“ platvormil[17], mida juhib riigi CIO.

Austrias on loodud usaldusväärsed digitaalse isikutuvastuse vahendid, kusjuures kasutatakse nii tsentraliseeritud kui detsentraliseeritud privaatvõtmete haldust. Riiklikul tasandil ei väljastata kodanikele massiliselt elektroonilisi enesetuvastuse (ja allkirjastamise) vahendeid. Inimene ise taotleb vajaduse korral vajalikud elektroonilist tuvastamist ja allkirjastamist võimaldavad sertifikaadid (ID-kaart või mID), laialdaselt kasutavad seda võimalust notarid, juristid, riigihangete spetsialistid, ehitusinsenerid jt. Selline kasutusviis tagab aga seda, et kõik välja antud digitaalsed identiteedid on kasutusel.[18]

Passi ja ID-kaardi taotlemisel tuleb esitada alljärgnev informatsioon:

- perekonnaseisuinfo deklaratsioon;
- sünnitunnistus;
- abielutunnistus või muu sarnane dokument;
- kodakondsuse originaaltõend;
- akadeemiliste kraadide tõendid (soovi korral);
- eelmine ID-kaart; ja
- foto.

Digitaalteenuste jaoks võttis Austria kasutusele kodanikukaardi kontseptsiooni, mis võib esineda erineval kujul (st pole piiratud kaardivormiga). Austria kodanikukaart on kontseptsioon, mitte aga spetsiifiline tehnoloogia. See hõlmab kvalifitseeritud elektroonilist allkirja (autentimine), elektroonilist identiteeti (identifitseerimine), esindamise andmeid ja volitusi (esindamine).

On palju rakendamisvorme:

- Panga (sularahaautomaadi) kaardid. Iga pangakaart, mida on välja antud alates 2005. aasta märtsist, on turvaline allkirja andmise vahend. Nüüdseks on kasutuses ka juba uuema põlvkonna kaardid, aga vanu on veel käigus.
- Tervisekindlustuse e-kaardid. Antakse välja 2005. aastast ja on samuti turvaline allkirja andmise vahend. Saavutas 100%lise leviku 2005. aasta novembris (ca 9 miljonit isikut).
- Muud initsiatiivid hõlmavad ametniku teenistuskaarti, sertifitseerimisteenuste osutaja allkirjakaarti, üliõpilase teenistuskaarti jt.

[16] The Austrian E-Government Act. Vt ka Administration on the Net. The ABC guide of eGovernment in Austria. eGovernment ABC. Vienna, May 2014

[17] http://digital.austria.gv.at/

[18] Digitaalset allkirja kasutavate tööealiste (15-64-aastased) Euroopa liidu elanike osakaalu määramine 2015. aastal. Uuringu aruanne. Detsember 2015

Lisaks võivad ka mobiiltelefoniga antud allkirjad kvalifitseeruda täielikult eID-ks ja peetakse kehtivaks kodanikukaardi rakenduseks. Mobiiltelefoniga autentimisel toimuvad krüpto-operatsioonid teenusepakkuja serveris.

„Lähte-PIN“ (mitteavalikustatud personaalne identifitseerimisnumber) on juurnumber, millest tuletatakse sektoripõhised PINid. LähtePINi tohib salvestada ainult kodanikukaardile ja see on seega kasutaja kontrolli all. Sel moel saavad sektoripõhised rakendused (sealhulgas erasektor) luua oma ID numbrid ilma andmehulkade sidumist võimaldamata.

Austria lähenemine eID-le on täiendavalt märkimisväärne, kuna Austria on üks väheseid riike, mis on rakendanud põhjaliku seadustiku, mis käsitleb elektroonilist identifitseerimist ja piiriülest ristkasutatavust. See sai teoks „E-riigi seaduse“ vastuvõtmisega, mis jõustus 2004. aasta 1. märtsil. Välismaiseid eID-sid toetatakse, kuid see nõuab ka välismaalasele lähte-PINi andmist nii, et nad oleksid Austria registritele teada.

Teatud mõttes võib lähte-PINist saadavaid derivatiivPINe lugeda mitmetasemeliseks identiteediks.

B

Üldine andmekaitseseadus on "Föderaalseadus isikuandmete kaitse kohta". Kasutajate isikuandmete kaitset elektroonilise side valdkonnas ja eraelu puutumatust reguleerib "Telekommunikatsiooniseadus 2003" (nt äriline elektrooniline kommunikatsioon, küpsised jne) ning panganduse valdkonnas – „Pangandusseadus“ (pangasaladus). Isikuandmete kaitset mõjutab ka tööõigus – peamine andmekaitsealane õigusakt antud valdkonnas on "Töönõukogu põhiseadus".

Kuigi Austria andmekaitseseadus kasutab Euroopa Liidu omast pisut erinevat sõnastust, on siiski isikuandmete töötlemise reeglid sarnased Euroopa Liidu tüüptingimustega ja andmeid võib töödelda, kui isikuandmete töötlemise tüüptingimused[19] on täidetud. Sarnased põhimõtted kehtivad kõikides uuringus käsitletud riikides.

Õigustatud huvide elluviimine on eelistatum tingimus kui andmesubjekti nõusolek, kuna Austrias on ranged nõuded andmesubjekti nõusoleku saamiseks. Kui isikuandmed ei ole delikaatsed, tuleb ikkagi nende töötlemisest teavitada AKAd. Andmekaitseseadus sisaldab erandeid teatud tüüpi andmete töötlemiseks: soodustavaid sätteid rakendatakse, kui andmeid töödeldakse siseriiklikel või teadusliku uuringu eesmärkidel või kui andmesubjekt ei ole isikuandmete kaudu tuvastatav.

Delikaatseid isikuandmeid võib põhimõtteliselt töödelda, kui delikaatsete isikuandmete töötlemise tüüptingimused[20] on täidetud, kuigi Austria andmekaitseseadus kasutab ka siinjuures pisut erinevat sõnastust. Sarnased põhimõtted kehtivad kõikides uuringus käsitletud riikides.

Delikaatsete isikuandmete töötlemisele peab eelnema nende registreerimine AKAs. Kuigi andmekaitseseadus ei nimeta kriminaalmenetlusega seotud andmeid otseselt delikaatseteks isikuandmeteks, ei saa nende töötlemist alustada enne AKAs registreerimist.

Vastutav töötleja peab töötlemisest teavitama AKAd. Teavitust registreeritakse AKA andmetöötlusregistris (ingl. *Data Processing Register*). Teavitus tuleb üldjuhul esitada ja registreerida enne töötlemist algust, kuid seda võib teha ka pärast, kui kehtib üks tingimustest: töödeldavad isikuandmed:

- ei ole delikaatsed;

[19] Siin ja edasi: Andmekaitsedirektiivi artiklis 7 kirjeldatud isikuandmete töötlemise tüüptingimused

[20] Siin ja edasi: Andmekaitsedirektiivi artiklis 8 kirjeldatud delikaatsete isikuandmete töötlemise tüüptingimused

- ei ole seotud kriminaalmenetlusega;
- ei sisalda andmeid andmesubjekti krediidireitingust;
- neid ei töödelda ühendatud infosüsteemis;
- ei ole jäädvustatud videovalve tulemusena.

Teatud juhtudel on isikuandmete töötlemiseks vajalik töönõukogu nõusolek. Erandeid kohaldatakse erijuhtudel, sealhulgas, kuid mitte ainult:

- avaldatud;
- pseudonümiseeritud;
- "standardiseeritud" (nt raamatupidamislike või videovalve) andmete töötlemisel.

Standardiseeritud andmete töötlemisest ei pea AKAd teavitama. Volitatud töötlejad peavad:

- kasutama andmeid vaid vastutava töötleja juhiste järgi;
- rakendama vajalikke turvameetmeid (eriti hoidma andmeid konfidentsiaalsetena);
- värbama teist volitatud töötlejat vaid vastutava töötleja loal;
- looma koostöös vastutava töötlejaga vajalikud tehnilised ja organisatsioonilised nõuded täitmaks vastutava töötleja kohustust andma õigust teabele ning andmete parandamisele ja kustutamisele;
- andma vastutavale töötlejale üle andmetöötluse tulemused ja andmeid sisaldava dokumentatsiooni või hoidma/hävitama need vastutava töötleja nõudmisel peale töötlemise lõppu; ja
- teha vastutavale töötlejale kättesaadavaks kogu informatsiooni, mis on vajalik kohustuste täitmise kontrollimiseks.

Vastutavad töötlejad peavad tulenevalt andmekaitseseadusest teavitama andmesubjekte andmetega seotud rikkumistest, kui saavad teada andmete süstemaatilisest väärkasutamisest, mis rikub tõsiselt seadust. Elektroonilise side sektoris tegutsevad ettevõtted peavad vastavalt "Telekommunikatsiooniseadusele" teavitama valdkonna kõikidest isikuandmetega seotud rikkumistest.

Isikuandmete edastamine kolmandatesse riikidesse on lubatud AKA loal kui:

- taotlus on legitiimne;
- on tõestatud, et vastuvõtja on taganud andmete piisava kaitse; ja
- saladuse hoidmine on nõuetekohaselt kaitstud.

Ilma AKA loata isikuandmete edastus on lubatud kui andmeedastus põhineb spetsiifilisele ja kehtivale õiguslikule regulatsioonile, sealhulgas, kuid mitte ainult: andmesubjekti nõusolekule kui isikuandmed edastatakse piisava andmekaitsega riiki (kuni "*Safe Harbor*" raamistiku tühistamiseni käsitles Austria seadusandlus kehtivaks andmete edastamist ka *Safe Harbor* firmadele). Teavitamine ja registreerimine on ikkagi vajalik.

AKA teavitamine ja loa saamine (sh lepingu tüüptingimuste kasutamisest teavitamine) on vajalik, kui andmeid edastatakse väljapoole ELi. Kui kasutatakse lepingu tüüptingimusi, on AKA luba endiselt vajalik, kuid selle saamise protseduurid on lihtsamad.

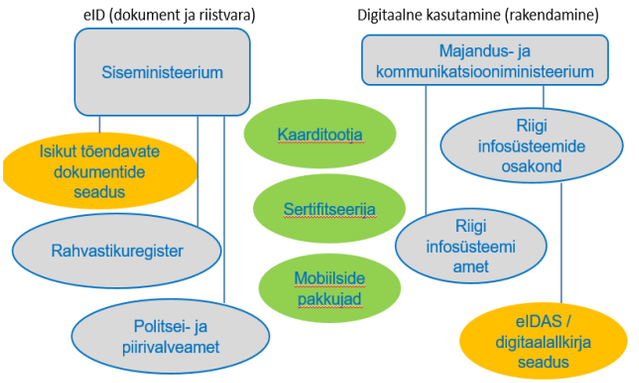
Austria AKA on kinnitanud siduvate ettevõtluseeskirjade kasutamist, kuid praktikas on lepingu tüüptingimuste kasutamine levinum.

3.3. Eesti

A

Kuigi Eesti identiteedihaldus on maailma üks edukaimaid süsteeme, ei tugine see korrastatud identiteedihalduse regulatsioonile.

Eesti identiteedi keskmeks on isikukood, mis on reguleeritud „Rahvastikuregistri seadusega“. Seaduse § 49 kohaselt on isikukood soo ja sünniaja alusel moodustatud isiku üheselt kindlaksmääramist võimaldav arv. Isikukood sisaldub ka isikusertifikaatides ja võimaldab seeläbi siduda kõik identiteedid konkreetse rahvastikuregistrisse kantud inimesega. Rahvastiku arvestuse poliitikat juhib SM.



Joonis 2. Identiteedialane tööjaotus Eestis

Olulised identiteedihaldust mõjutavad õigusaktid on ka „Isikut tõendavate dokumentide seadus“, „Välismaalaste seadus“ ja „Välismaalasele rahvusvahelise kaitse andmise seadus“.

STO on AS Sertifitseerimiskeskus, mille omanikeks on Swedbank, SEB ja Telia. Kuni eIDAS vastava osa rakendumiseni 2016. aasta 1. juulil reguleeris digitaalallkirja kasutamist „Digitaalallkirja seadus“. Seda hakkab asendama „E-identimise ja e-tehingute usaldusteenuste seadus“ (praegu 237 SE, kolmas lugemine 2016. aasta 12.10.), millega reguleeritakse kõik liikmesriigi kompetentsi jäävad teemad, mida ei peetud vajalikuks eIDASga reguleerida. Nende seaduste juhtivministeerium oli ja on MKM. MKM ja otseselt RIA kompetentsi kuuluvad küberturvalisuse ja e-riigi infrastruktuuri küsimused, samuti vastavalt eelmisel aastal tehtud kokkuleppele isikutunnistuse digitaalse osa arendamine PPA ja RIA (SM ja MKM) koostöös.

Isikut tõendavate dokumentide seaduse § 94 ütleb, et dokumenti kantava digitaalset tuvastamist võimaldava sertifikaadi ja digitaalset allkirjastamist võimaldava sertifikaadi annab välja dokumendi väljaandja, seega PPA, mis kannab digitaalse identiteedi väljastamise kontekstis registreerimisasutuse (ingliskeelne lühend *RA*) rolli.

Juba sellisest lühikirjeldusest on näha, et tööjaotus ei ole selge ja üheselt mõistetav. Ka uuringu käigus läbi viidud vestlused Eesti eID ekspertidega näitasid, et igal eksperdil ja riigiasutusel oli suhteliselt autonoomne arusaam identiteedihalduse tööjaotusest.

Uuringu autorid on seisukohal, et kehtiva õiguse kohaselt on identiteedihalduse juhtiv ministeerium siseministeerium.

Hetkel saab ühel isikul olla 3 riigi poolt välja antud digitaalset identiteedikandjat: isikutunnistuse või elamisloa kiibis asuvad, digitaalse isikutunnistuse ehk teise isikukaardi kiibis asuvad ning mobiil-ID sertifikaadid. Isikut tõendavad dokumendid antakse välja isikukoodi olemasolul. Eesti kodanike primaarne isikut tõendav dokument on isikutunnistus, sekundaarsed pass ehk reisidokument, digitaalne isikutunnistus ja mobiil-ID. Ülejäänud residentidel on digitaalse identiteedi kandjaks kas neile väljastatud isikutunnistus või elamisluba, e-residentide digitaalse identiteedi kandjaks on e-residendi kaart, mis on analoogne Eesti kodaniku digitaalsele isikutunnistusele.

Eesti kasutab isikutuvastamisel digitaalset biomeetriat ainult passide ehk reisidokumentide ja elamislubade[21] kuuluvuse määramisel (*match-on-passport* või *match-on-card)*. 2013. aastal SMi tellimisel e-Riigi Akadeemia poolt läbi viidud „ID-1 formaadis dokumentide funktsionaalsuse uuringu“ ajal ei toetanud eID eksperdid üksmeelselt ideed võtta näo- ja sõrmejäljebiomeetria ning selleks vajalik kiip kasutusele ka isikutunnistusel.

B

Üldine andmekaitseseadus on "Isikuandmete kaitse seadus“. Kasutajate isikuandmete kaitset elektroonilise side valdkonnas ja eraelu puutumatust reguleerib lisaks "Elektroonilise side seadus". Samuti mõjutab andmekaitset ja sidet "Infoühiskonna seadus"[22].

Isikuandmeid võib töödelda, kui tüüptingimused on täidetud. AKAs isikuandmete töötlemise registreerimise kohustus kohaldub ainult delikaatsete isikuandmete suhtes. Vastutavad töötlejad peavad esitama AKAle delikaatsete isikuandmete töötlemise registreerimistaotluse vähemalt 1 kuu enne töötlemise algust. AKA keeldub delikaatsete isikuandmete töötlemise registreerimisest, kui

- töötlemiseks puudub seaduslik alus;
- töötlemise tingimused ei vasta AKA nõuetele; ja
- rakendatud turvameetmed ei taga seaduslike nõuete täitmist.

Töötlemise registreerimine on tasuta.

Erandina ei pea isikuandmete töötlemist AKAs registreerima, kui need andmed ei ole delikaatsed isikuandmed või kui asutus on määranud andmekaitse eest vastutava isiku ning registreerinud selle AKAs.

Volitatud töötlejad peavad täitma isikuandmete töötlemise tüüptingimusi. Lisaks on isikuandmete vastutav töötleja kohustatud tagama oma alluvuses isikuandmeid töötlevate isikute väljaõppe isikuandmete kaitse alal.

Isikuandmete kaitse seadus ei sisalda kohustust teavitada AKAd või andmesubjekte andmetega seotud rikkumisest. Teavitamise kohustus tuleneb Elektroonilise side seadusest ja kohaldub ainult elektroonilise side sektoris.

Isikuandmete edastamine on lubatud riikidesse, kus on piisav andmekaitse tase (sh edastamine riiki, mille isikuandmete kaitse taset on Euroopa Komisjon hinnanud piisavaks). Edastamine riikidesse, kus ei ole tagatud andmete piisavat kaitset, on lubatud AKA loal kui:

- vastutav töötleja tagab, et andmesubjekti õigused selles riigis ei saa rikutud (nt kasutades lepingu tüüptingimusi); või
- konkreetsel isikuandmete edastamise juhul on selles riigis tagatud piisav andmekaitse tase.

---

[21] Elamisloa vormi tehnilised nõuded tulenevad Euroopa Liidu Nõukogu määrusest (EÜ) 1030/2002, millega kehtestatakse ühtne elamisloa vorm kolmandate riikide kodanike jaoks (EÜT L 157, 15.06.2002, lk 1–7) ja eelnimetatud määruse muudatusest (EÜ) 380/2008 (ELT L 115, 29.04.2008, lk 1–7).

[22] Lisaks on andmekaitsetkäsitletudandmekaitset käsitletud eri määrustes, mis käsitlevad spetsiifilisi andmetöötlemise süsteeme. Siia kuuluvad näiteks Valitsuse määrus number 252 2009. aastast infosüsteemide turvameetmete süsteemi kohta; Kaitseministeeriumi määrused number 34 2008. aastast arvutite ja kohtvõrkude kaitse nõuete kohta ning number 6 aastast 2009 krüptomaterjalide töötlemise ja kaitse nõuete kohta; MKMi määrus number 93 2009. aastast tehniliste vahendite paigaldamise ja kasutamise ning andmete töötlemise korra kohta; SMi määrus number 13 2013. aastast rahapesu andmebüroo kogutavate andmete registreerimise ja töötlemise korra kohta; Justiitsministeeriumi määrus number 10 2013. aastast andmekaitse inspektsiooni põhimääruse ja koosseisu kohta (viimane muudatus algselt 2007. aastal vastuvõetud määruses).

Ilma AKA loata võib andmeid edastada kui:

- andmesubjekt on andnud nõusoleku edastamiseks;
- isikuandmed edastatakse andmesubjekti elu, tervise või vabaduse kaitseks, kui andmesubjektilt ei ole võimalik nõusolekut saada; või
- kui kolmas isik taotleb teavet, mis on saadud või loodud seaduses või selle alusel antud õigusaktides sätestatud avalikke ülesandeid täites ja taotletav teave ei sisalda delikaatseid isikuandmeid ning sellele ei ole muul põhjusel kehtestatud juurdepääsupiirangut.

AKA teavitamine ja loa saamine (sh lepingu tüüptingimuste kasutamisest teavitamine)on vajalik teatud, eelmises lõigus kirjeldatud, juhtudel.

Eesti on liitunud siduvate ettevõtluseeskirjade vastastikuse tunnustamise süsteemiga. Kuid AKA ei ole esitanud ühtegi avalikku arvamust siduvate ettevõtluseeskirjade kasutamise kohta ning need eeskirjad ei ole veel praktikas levinud.

3.4. Holland

A

„Kohalike omavalitsuste isikukirjete andmebaasi seadus“ sisaldab klausleid privaatsuse ja turvalisuse kaitsmiseks. „Hollandi passiseadus“ (holl. *Paspoortwet*, ingl. *Dutch Passport Law*) reguleerib erinevat liiki isikut tõendavate dokumentide väljaandmist. Nendeks on passid ja Hollandi ID-kaardid. Juhilubade ja välismaalaste dokumentide, mida Hollandis isikut tõendavateks dokumentideks loetakse, väljaandmist reguleerivad teised seadused.

Palju erinevaid protseduure ja reegleid on sätestatud erinevates õigusaktides. Näiteks hollandlaste kohustus dokumenti kaasas kanda ja seda politsei nõudel esitada või pangas arvet avades või uuele töökohale asudes dokumenti esitada ei ole ühes seaduses koos. Samuti on erinevad ID-kaarti puudutavad nõudmised erinevates sektoripõhistes seadustes.

Isikuidentiteete hallatakse tsentraalselt kohalike omavalitsuste isikukirjete andmebaasis, mis sisaldab kõiki Hollandi rahvastikukirjeid. Registreerimine toimub läbi kohalike omavalitsuste ja on kohustuslik kõigile, isegi tähtajalise elamisloa alusel viibivatele isikutele, keda kutsutakse Hollandis „ajutisteks residentideks“. ID-kaarte väljastavad erinevad asutused, peamiselt elukohajärgses omavalitsuses.

Identiteedihalduse eest Hollandis vastutab Hollandi sise- ja kuningriiklike suhete ministeerium. Andmebaasi peab Isikuandmete andmebaasi ja reisidokumentide agentuur, mis asub nimetatud ministeeriumi haldusalas.

Riigiasutused, sh. maksu- ja tolliadministratsioon, Sotsiaalkindlustuspank ja kohalikud omavalitsused, saavad oma tööks vajalikud isikuandmed kohaliku omavalitsuse isikukirjete andmebaasist, mis sisaldab iga Hollandi elaniku kohtatäisnime, sünniaega ja -kohta, infot vanemate kohta, infot selle kohta, kas nad on abielus või on registreerinud kooselu, infot laste kohta, infot rahvuse[23] ja residentsuse kohta, kodust aadressi, kodaniku teenindusnumbrit ja passi ning ID-kaardi numbreid ja väljaandmise aega.

Avaliku sektori kodaniku teenindusnumber (BSN) on unikaalne number, mis on antud kõigile kohaliku omavalitsuse isikukirjete andmebaasis registreeritud isikutele. Igaüks peab kohalikku omavalitsust teavitama sünnist, aadressi muutusest või surmast. Kodaniku teenindusnumber omistatakse isikule tavaliselt tema registreerimisel andmebaasis. See võimaldab ära hoida eksitavaid või mitmekordseid identiteete. Enne 2007. aastat tunti kodaniku teenindusnumbrit lühendi SOFI all ja see anti välja maksuameti kohalike harukontorite poolt. Igale harukontorile oli antud kindel numbrivahemik. Piirkondades, kus elas palju inimesi, said aga need vahemikud kiiresti välja antud ja kõrvalt hakati lisaks numbreid võtma, mis aga viis topeltnumbrite tekkimisele. Üleminekul SOFIlt BSNile see viga kõrvaldati, andes neile, kellel olid topeltnumbrid, uued numbrid. Number ei sisalda mingit infot selle isiku kohta, kellele see number väljastatud on (näiteks sugu või sünnikuupäeva BSNist välja lugeda ei saa).

Erasektor ei saa identifikaatorina BSNi kasutada. Nad võivad kasutada nime, aadressi jne ning selle kinnitamiseks paluda kodanikul esitada ametlik isikut tõendav dokument, millest nad endale koopiat teha ei tohi.

E-identiteete kutsutakse Hollandis DigiIDks ja Holland töötab riikliku eID lahenduse kallal realiseerimaks täielikku elektrooniliste teenuste kättesaadavust kodanikele ja ettevõtetele 2017.

[23] siin päritoluriigi tähenduses

aasta lõpus – 2018. aasta alguses, ning pakkuda tuge tehingutele erasektoris. DigiID koosneb kasutaja poolt vabalt valitavast kasutajanimest ja salasõnast, viimasel ajal lisati täiendavad meetmed, et paremini sobitada seda kahetegurilise tuvastusega. Seda saab taotleda, edastades BSNi koos sünnikuupäeva ja aadressiga. DigiIDd kasutatakse oma identiteedi tõestamiseks suheldes üle võrgu riigiasutustega, aga ka isikuandmete edastamisel neile asutustele. DigiIDd saab kasutada ka kolmanda osapoole volitamiseks enda nimel tegutsema. DigiID on BSNi elektrooniline jätk. Organisatsioonid, mis tunnistavad DigiIDd kui autentimismeetodit, on kohalikud omavalitsused, maksu- ja tolliamet, politsei, pensionifondid ja tervisekindlustusfirmad. See nimekiri ei ole lõplik.

Holland välistab riikliku identiteedihalduse taristu raames loodud digitaalsete kinnituste kasutamise erasektoris. Selle taristu laiendamine erasektorisse on rangelt piiratud, sest BSNi, eIDMi taristu võtmekomponendi kasutamine on lubatud ainult avalikus sektoris.

B

Üldine andmekaitseseadus on "Hollandi isikuandmete kaitse seadus", mis on aluseks teisestele õigusaktidele, eelkõige "Otsusele erandite kohta", mis vabastab töötlejat etteteatamise kohustusest paljude andmekategooriate töötlemise puhul. Kasutajate isikuandmete kaitset elektroonilise side valdkonnas ja eraelu puutumatust reguleerib "Telekommunikatsiooniseadus" ja seda muutev seadus küpsiste kohta. Andmetega seotud rikkumistest teavitamist reguleerib "Andmetega seotud rikkumisest teavitamise seadus". Seadus rakendab ennetähtaegselt isikuandmete kaitse üldmäärust 2016/679.

Andmekaitseseadus järgib isikuandmete töötlemise tüüptingimusi. Praktikas kasutatakse tihti andmetöötluse seaduslikkuse põhjendamiseks õigustatud huvide elluviimise tingimust. Töötlemine isiklikel ja siseriiklikel eesmärkidel on keelatud. Samuti on keelatud töötlemine ajakirjanduslikel, kirjanduslikel või kunstilistel eesmärkidel, v.a juhul kui see on vajalik teatud kohustuse täitmiseks. Delikaatsete isikuandmete töötlemine on üldjuhul keelatud, kuid on olemas erandid.

Automatiseeritud andmetöötluse puhul tuleb teavitada AKAd või andmekaitse eest vastutavat isikut enne töötlemisega alustamist. Teavitada saab elektrooniliselt või paberkandjal, vormid on kättesaadavad AKA kodulehel. Töötlemise registreerimine on tasuta. Kuigi AKA vaatab taotlust üle ja vajadusel kommenteerib, võib töötlemist alustada enne AKA ametliku loa saamist. Kõiki registreeringuid avaldatakse AKA kodulehel.

Erandid kohaldatakse eri andmekategooriate puhul, nt töötajate, abonentide, võlgnike ja võlausaldajate, klientide andmete töötlemise andmeid ei pea registreerima AKAs (ei puuduta andmete edastamist riikidesse, kus ei ole piisavat andmekaitse taset). Andmekategooriad, töötlemise eesmärgid, andmesubjektid ja andmete säilitamistähtajad on andmekaitseseaduses põhjalikult kirjeldatud ning erand kehtib tingimusel, et töötlemine toimub nende kirjelduste piires. Nõudeid töötlemisele sätestab AKA ning andmekaitseseadus vaid kirjeldab tingimusi, mis vabastavad teavitamise kohustusest.

Volitatud töötleja peab töötlema isikuandmeid vastavalt kirjalikule lepingule, mis sisaldab volitatud töötleja tüüpkohustusi. Vastutav töötleja peab kontrollima nende kohustuste täitmist, nt lepinguliste auditite kaudu.

Vastutavad töötlejad peavad tulenevalt "Andmetega seotud rikkumisest teavitamise seadusest" teavitama tõsisest rikkumisest AKAd ning teatud juhtudel lisaks ka andmesubjekte. Sama seadus lubab AKA määrata otsest trahvi andmekaitseseaduse rikkumise eest. Vastavalt "Telekommunikatsiooniseadusele" peavad elektroonilise side sektoris tegutsevad ettevõtted

teavitama isikuandmetega seotud rikkumistest AKAd. Kui rikkumine võib rikkuda andmesubjektide eraelu puutumatust, siis tuleb teavitada ka neid.

Isikuandmete edastamine kolmandatesse riikidesse on vastavalt Hollandi andmekaitseseadusele lubatud, kui piiriülese edastamise tüüptingimused on täidetud. Kui andmesubjekt ise annab edastamiseks nõusoleku, peab see olema ühemõtteline.

AKA teavitamine ja loa saamine (sh lepingu tüüptingimuste kasutamisest teavitamine) ei ole vajalik, kui piiriülese edastamise tüüptingimused on täidetud. Vastasel juhul tuleb saada üksiklitsents.

Holland on kinnitanud siduvate ettevõtluseeskirjade kasutamist ning on liitunud siduvate ettevõtluseeskirjade vastastikuse tunnustamise süsteemiga. Eriprotseduuri vastastiku tunnistamise jaoks ei ole. Siduvaid ettevõtluseeskirju tuleb esitada koos piiriülese edastamise litsentsi taotlusega.

3.5. Läti

A

Peamised identiteedihaldust reguleerivad seadused on „Isikut tõendavate dokumentide seadus“, „Rahvastikuregistri seadus“, „Perekonnaseisudokumentide registreerimise seadus“, „Biomeetriliste andmete töötlemise süsteemi seadus“ ja „Isikute erikaitse seadus“. Hiljuti võttis Läti Parlament vastu uue „e-identifitseerimise seaduse“.

Lätis hallatakse identiteete keskselt. Kogu Lätit hõlmava identiteedihalduse kesksüsteem on biograafilisi andmeid sisaldav rahvastikuregister. Rahvastikuregistrit haldab kodakondsus- ja migratsioonibüroo (läti *Pilsonības un Migrācijas Lietu Pārvalde*), mis allub Läti Siseministeeriumile. Rahvastiku biomeetrilisi andmeid säilitatakse ja töödeldakse biomeetriliste andmete töötlemise süsteemis siseministeeriumile alluvas infokeskuses.

Avaliku sektori menetlustes vajalik ligipääs identiteediandmetele on reguleeritud seaduste ja/või valitsuse määrustega. Kui seadusandja on sellise määruse heaks kiitnud, siis on ka ligipääs antud. Näiteks juhiloa taotlemise eksamil põhineb identiteedi tuvastus sõrmejäljebiomeetrial. Enne eksamile minekut võetakse sõrmejälg ja seda kontrollitakse väidetava identiteedi vastu biomeetriliste andmete töötlemissüsteemis.

Avalikus sektoris luuakse identiteet sünniakti ja rahvastikuregistris loodud isikukoodi alusel või legaalse staatuse omistamise otsuse alusel, mis toob kaasa uue kirje loomise rahvastikuregistris, näiteks elamisloa andmisel. Sellisel juhul kontrollitakse isikut tõendavat või reisidokumenti ning identiteeti enne kui elamisluba antakse.

Erasektoris sõltub uue identiteedi loomise protseduur nõutavast usaldustasemest ning vastavusest andmetöötluse reeglitele. Tavaliselt nõutakse uue identiteedi registreerimisel isikukoodi ja see kood viib kirjeni rahvastikuregistris. Isikukoodi kehtivust saab kontrollida e-teenuse abil. Isikukood kantakse isikut tõendavasse dokumenti (kohustuslik alates 15. eluaastast) ja sünnitunnistusele. Suure turvalisusega rakenduste nagu näiteks panganduse puhul saab/tuleb teha isikuandmete ristkontrolli rahvastikuregistris. Tavaliselt on isikut tõendava või reisidokumendi ja selle autentsuse kontroll uue kliendi registreerimise protseduuri osa.

Lätis eksisteerib koos mitu elektroonilise identifitseerimise ja autentimise lahendust. Kõige populaarsem on online-panganduses autentimiseks kasutatavad ühekordsed paroolid (koodikaart või PIN-kalkulaator).

eID-kaarte antakse välja alates 2012. aasta 1. aprillist, neil on identifitseerimis-, autentimis- ja digitaalallkirja funktsioonid. Praeguseks on välja antud üle 800 000 kaardi, kuid nende kasutamine autentimiseks on küllaltki madal (ainult kaks protsenti kaardikasutajatest on kasutanud eID funktsioone, näiteks digitaalallkirja andnud). eID-kaart on siiani vabatahtlik ja e-funktsioonid saab aktiveerida, kui kaardi kasutaja saab 14-aastaseks.

Ärisektoris on kasutusel virtuaalne eAllkirja (läti *eParaksts*) kiipkaart (sarnaneb Eesti digitaalse isikutunnistusega) laialt ja sealt pärineb enamik digitaalallkirju. Seda annab välja Läti ainus STO – Läti Riiklik Raadio- ja Telekeskus. eAllkirja kasutatakse www.eparaksts.lv veebilehel dokumentide allkirjastamiseks, verifitseerimiseks, mitmele isikule allkirjastamisele suunamiseks ja grupiallkirjastamiseks (analoogne Eesti digitemplile). Samuti on olemas virtuaalpilve eAllkiri ja selle kasutamine on samas suurusjärgus eID-kaardiga.

Elektrooniline identiteet põhineb tavapäraselt füüsilisel identiteedil ja isikukoodi kasutatakse primaaridentifikaatorina nii eID-kaardi, eAllkirja kaardi, virtuaalse eAllkirja kui ka kõigi

pangapääsmike[24] jaoks. Enne sellise pääsmiku väljastamist kontrollitakse taotleja identiteeti ja esitatud isikut tõendava / reisidokumendi autentsust kohapeal.

Mobiil-ID ei ole Lätis praegu kasutusel.

B

Üldine andmekaitseseadus on "Füüsiliste isikute andmete kaitse seadus". Kasutajate isikuandmete kaitset elektroonilise side valdkonnas ja eraelu puutumatust reguleerivad "Elektroonilise side seadus" ja "Infoühiskonna teenuste seadus".

Isikuandmeid võib töödelda, kui tüüptingimused on täidetud. Andmekaitseseadus sisaldab erandeid teatud tüüpi andmete töötlemiseks. Näiteks andmekaitseseadust ei rakendata, kui füüsilised isikud töötlevad isikuandmeid isiklikel, perekondlikel või majapidamise eesmärkidel ja ei avalda neid kolmandatele isikutele. Andmekaitseseaduse teatud sätteid ei rakendata, kui töötlemine toimub ajakirjanduslikel, kirjanduslikel või kunstilistel eesmärkidel.

Läti õigusruumis loetakse delikaatseteks isikuandmeteks informatsiooni, mis viitab rassilisele või etnilisele kuuluvusele, religioossetele, filosoofilistele või poliitilistele veendumustele, ametiühinguliikmelisusele või annab teavet isiku tervise või seksuaalsete sättumuste kohta. Biomeetriline informatsioon ei ole seejuures midagi eraldiseisvat, vaid on tõlgendamise küsimus – näiteks saab isiku rassilise kuuluvuse tema näokujutise järgi kindlaks teha.

Lähenemisviis biomeetrilise info kasutamisele on sarnane Eesti omale. Nende andmete hõivamine ja ristkasutus on määratletud ülalmainitud biomeetriliste andmete töötlemise süsteemi seadusega. Läti biomeetrilise info töötlemise süsteemi loomisel arvestati vajadust tulevikus multimodaalsust toetada, kuid käesoleval ajal säilitatakse kolm paremat fotot ja üks sõrmejäljekujutis hõivatud sõrme kohta.

Delikaatseid isikuandmeid võib töödelda, kui on täidetud nende töötlemise tüüptingimused või üks allolevatest tingimustest:

- osutatakse sotsiaalabi;
- arendatakse Läti riiklikku arhiivi;
- Tsentraalne Statistikabüroo (ingl. *Central Statistical Bureau*) viib läbi statistilisi uuringuid;
- täidetakse haldusülesandeid või arendatakse riiklikke infosüsteeme; või
- kaitstakse füüsise või juriidilise isiku õigusi või seaduslikke huvisid taotledes hüvitist kindlustuslepingu alusel.

Vastutavad töötlejad peavad registreerima töötlemist AKAs, kui:

- andmeid edastatakse väljapoole ELi/Euroopa majanduspiirkonda;
- vastutava töötleja põhitegevuseks on: finants- või kindlustusteenused, loteriid ja hasartmängud, turu-uuringud ja avaliku arvamuse küsitlused, võlgade sissenõudmine, personali otsimise ja hindamise teenused või krediidireitingu hindamine;
- töödeldakse delikaatseid isikuandmeid, v.a raamatupidamise või personalitöö eesmärkidel või religioosse organisatsiooni poolt;
- töödeldakse infot varasemate süüdimõistvate kohtuotsuste kohta, mis said tehtud kriminaal- või haldusasjus;
- töödeldakse videovalvesüsteemi abil kogutud materjali; või

[24] ingl. k. *token*, füüsiline volitustõend, näiteks kiipkaart või USB kaudu ühendatav seadis

- töödeldakse geneetilisi andmeid. Kui vastutav töötleja on määranud andmekaitse eest vastutava isiku, võidakse töötleja vabastada registreerimise kohustusest.

Isikuandmete töötlemist võib volitada kirjaliku lepingu alusel. Volitatud töötlejad võivad andmeid töödelda ainult lepingus sätestatud määral ja vastutavad töötajad peavad tagama, et volitatud töötleja täidab volitatud töötleja ülesandeid, sh tüüpkohustusi. Vastutav töötleja peab tuvastama volitatud töötlejate isikuid registreerimistaotluses AKAle.

AKA rikkumisest teavitamise üldkohustus puudub, kuid teatud sektorite vastutavad töötlejad võivad olla kohustatud esitama oma valdkonna järelevalveasutusele teavitusi andmetega seotud rikkumistest, kahjulikest kõrvatoimetest, olulistest muutustest jms. Elektroonilise side sektoris tegutsevad ettevõtted peavad teavitama valdkonna kõikidest isikuandmetega seotud rikkumistest vastavalt "Elektroonilise side seadusele" AKAd ja ka andmesubjekte, kui neile võib rikkumisega kaasneda kahju. Andmesubjektide teavitamine ei ole kohustuslik, kui valdkonna teenuse osutaja on võimeline tõestama, et lekitud andmed olid krüpteeritud ja andmeid omandanud isikud ei pääse nendele ligi. Teenuseosutaja peab säilitama infot andmetega seotud rikkumise kohta 18 kuu jooksul rikkumise hetkest.

Isikuandmete edastamine kolmandatesse riikidesse on lubatud, kui on tagatud andmete selline kaitse, mis vastab andmekaitse tasemele Lätis. Sellisteks on Läti tunnustanud vaid Euroopa majanduspiirkonna riike. Siiski on lubatud andmete edastamine ka riikidesse, kus ei ole tagatud andmete piisavat kaitset, tingimusel, et vastutav töötleja võtab endale kohustuse kontrollida vajalike kaitsemeetmete täitmist või vähemalt üks järgmistest eeldustest on täidetud:

- on saadud andmesubjekti nõusolek;
- andmeedastus on vajalik andmesubjekti ja vastutava töötleja vahel sõlmitud lepingu täitmiseks, misjärel isikuandmed edastatakse vastavalt andmesubjektilepingulistele kohustustele;
- andmeedastus on vajalik ja nõutud vastavalt korrale oluliste riiklike ja avalike huvide kaitseks, või on vajalik kohtuvaidluses;
- andmeedastus on vajalik andmesubjekti elu ja tervise kaitseks; või
- andmeedastus puudutab avalikke andmeid või avalikult kättesaadava registri kaudu kogutud andmeid.

Et vastutav töötleja saaks kontrollida vastavate kaitsemeetmete täitmist, sõlmib ta andmete vastuvõtjaga isikuandmete edastamise lepingu. Lepingusse lisatavad sätted on kehtestatud Ministrite kabineti poolt.

Andmete edastamisel riiki, kus ei ole piisavat andmekaitse taset, esitatakse andmete edastamise taotlus AKAle. AKA hindab selle riigi kaitse taset ja väljastab kirjaliku loa andmete edastamiseks, kui töötlejad kasutavad lepingu tüüptingimusi ja/või siduvaid ettevõtluseeskirju (kuni "*Safe Harbor*" raamistiku tühistamiseni lubas Läti seadusandlus edastada andmeid ka vastuvõtjatele, kes olid sertifitseeritud vastavalt *Safe Harbor* põhimõtetele).

Läti on kinnitanud siduvate ettevõtluseeskirjade kasutamist ning on liitunud siduvate ettevõtluseeskirjade vastastikuse tunnustamise süsteemiga. AKA on avaldanud soovituse rahvusvahelistele ettevõtetele võtta vastu siduvaid ettevõtluseeskirju, mis võimaldavad tagada piisava andmekaitse taseme. Kuid:

- siduvad ettevõtluseeskirjad peavad olema heaks kiidetud AKA või ELi teise liikmesriigi vastava järelevalveasutuse poolt; ja
- kohalik vastutav töötleja peab olema registreeritud AKAs.

3.6. Norra

A

Põhiline identiteedihaldust reguleeriv dokument on “Isikuandmete seadus”.

Norras on isikukoodi (nimetatakse ka sotsiaalse turvalisuse numbriks) omamine kohutuslik. Isikukoodi kasutatakse isiku identifitseerimisel ning norra pangaarve avamisel. Isikukood omistatakse kas pärast sündimist või registreerimisel Norra rahvastikuregistris. Rahvastikuregistrit haldab Norra maksuamet. Norras ajutiselt elavad isikud saavad oma isikukoodi samuti registreerimisel rahvastikuregistris.

Riiklikke isikukoode jm identiteediandmeid, sh biomeetrilisi andmeid võib kasutada ainult isikutuvastuse eesmärkidel ja olukordades, kus isikutuvastus on vajalik. Norras kogutakse biomeetrilisi andmeid reisidokumentide jaoks nn biomeetriakioskis, kus hõivatakse foto, sõrmejäljed ja omakäelise allkirja kujutis.

Norras on kolm peamist isikut tõendavat dokumenti: pass, elamisluba ja BankID. Tulevikus (praegu plaani järgi 2017. aastal) lisandub neile ID-kaart. Norra valitsus on isikute autentimise ja passide, elamislubade ja tulevikus ka ID-kaartide väljaandmise kohustuse pannud Norra politseidirektoraadile. Identiteete jagatakse erinevatele avaliku ja erasektori asutustele.

Iga pank on omaenese juur-STO (ingl. *Root-CA*) ja annab välja on BankID’d, mida saab kasutada sisselogimiseks ja teenuste kasutamiseks Norra ametiasutustesse, ülikoolidesse ja pankadesse.

BankID digitaalse identiteedi lahendus töötab ka mobiiltelefonide turvalisel SIM-kaardil ja seda saab kasutada ka kõigi avalikult kättesaadavate teenuste eest tasumiseks.

Norra uue ID-kaardi kasutusele üheks põhjuseks on asjaolu, et pangad ei soovinud enam identiteedihaldusega tegeleda, vaid jääda oma põhitegevuse juurde.

B

Üldine andmekaitseseadus on "Isikuandmete seadus". Seadust rakendab "Isikuandmete määrus". Kasutajate isikuandmete kaitset elektroonilise side valdkonnas ja eraelu puutumatust reguleerivad "Turustamise kontrolli seadus" (turunduskommunikatsioon, küpsised), "e-Kaubanduse seadus" (küpsised) ja "e-Kaubanduse määrus". Isikuandmete kaitset mõjutavad ka erinevad valdkonnaspetsiifilised õigusaktid, nt "Isiklike terviseandmete kogumissüsteemi seadus", "Patsiendiandmete seadus", "Terviseuuringute seadus“, "Biopankade seadus", "Schengeni infosüsteemide seadus", "Valuuta vahetamise registri seadus".

Isikuandmeid võib töödelda, kui tüüptingimused on täidetud. Praktikas kasutatakse tihti andmetöötluse seaduslikkuse põhjendamiseks õigustatud huvide elluviimise tingimust. Andmekaitseseadus sisaldab erandeid teatud tüüpi andmete töötlemiseks. Nt seaduse enamikku sätteid ei rakendata kui füüsiline isik töötleb isikuandmeid majapidamise eesmärkidel. Vastutava ja volitatud töötleja vahel peab olema sõlmitud leping, mille järgi volitatud töötleja täidab oma tüüpkohustusi.

Delikaatseid isikuandmeid võib töödelda, kui nende töötlemise tüüptingimused on täidetud. Samuti on töötlemine lubatud, kui kohustus tuleneb seadusest või on vajalik ajaloolistel, statistilistel või teaduslikel põhjustel ja avalik huvi märkimisväärselt ületab võimalikke kahjusid andmesubjektile. Lisaks on delikaatsete isikuandmete töötlemiseks vajalik AKA luba. Riiklikke isikukoode jm identiteedi andmeid, sh biomeetrilisi andmeid võib kasutada ainult isikutuvastuse eesmärkidel ja olukordades, kus isikutuvastus on vajalik. Videovalve kohas, mida regulaarselt külastab piiratud arv

inimesi, on lubatud ainult juhul, kui on olemas eriline vajadus sellise järelevalve üle ja sellest vajadusest on tuleb teatada.

Vastutav töötleja peab teavitama AKAd enne isikuandmete automatiseeritud töötlemisega alustamist või enne käsitsi täidetava delikaatseid isikuandmeid sisaldava isikuandmete andmebaasi loomist. Teavitus tuleb esitada 30 päeva enne töötlemisega alustamist ja see on tasuta. Teavitamise kohustusega ei kaasne eelneva loa saamise vajadust. Delikaatsete andmete töötlemiseks ja töötlemiseks: telekommunikatsiooni-, kindlustus-, krediidiinfo-, finants- ja pangandusvaldkondades on vajalik saada AKA litsents, mis on tasuta.

Teavitamise/litsentseerimise kohustus puudub, kui andmeid töödeldakse halduseesmärkidel, klientide/tarnijate/abonentidega sõlmitud lepingu täitmiseks või teatud andmekategooriate puhul töötajate andmeid. Andmekaitse eest vastutava isiku määramisel vabastatakse töötleja teavitamise vajadusest, kui AKA on kiitnud seda isikut heaks.

Volitatud töötleja peab töötlema isikuandmeid vastavalt kirjalikule lepingule, mis sisaldab volitatud töötleja tüüpkohustusi.

AKAd tuleb teavitada, kui volitatud töötleja tüüpkohustuste mittetäitmine viis konfidentsiaalsete andmete volitamata avaldamisele.

Isikuandmete edastamine kolmandatesse riikidesse on piiratud. Norra andmekaitseseadus kehtestab piiranguid piiriülesele andmeedastusele. Isikuandmete edastamine on lubatud riikidesse, kui on täidetud piiriülese edastamise tüüptingimused. Alternatiivina võib volitatud töötleja toetuda oma hinnangule, kas isikuandmetele tagatakse piisav kaitse peale nende edastamist väljapoole Euroopa majanduspiirkonda. Lisaks võib AKA lubada andmeedastust isegi juhul, kui ülalmainitud tingimused ei ole täidetud, kui vastutav töötleja võtab vastu piisavad meetmed andmesubjekti õiguste kaitseks. AKA võib määratleda tingimused andmeedastuse jaoks.

Piiriülene andmeedastus ei nõua AKA teavitamist ega loa saamist, v.a juhul, kui see põhineb lepingu tüüptingimustel või siduvatel ettevõtluseeskirjadel. Tüüptingimuste korral on vajalik eelnev teavitamine ja ettevõtluseeskirjade korral AKA loa saamine.

Piiriülene andmeedastus võib põhineda siduvatel ettevõtluseeskirjadel, kui on eelnevalt saadud AKA luba.

3.7. Portugal

A

ID-kaardi väljaandmist reguleerib "Seadus 7/2007 kodanikukaardi kasutuselevõtmisest, väljaandmisest ja kasutamisest". Reisidokumentide väljaandmist reguleerib „Dekreetseadus 97/2011".[25]

Portugali kodanikukaart on kodakondsust tõestav dokument. Tehnoloogilise lahendusena võimaldab see identifitseerida kasutajat arvutiteenustele ja autentida elektroonilisi dokumente kindla elektroonilise allkirjaga. Portugali kodanikukaart võimaldab avaliku halduse moderniseerimist dünaamilisemal viisil. See on praktiline dokument, mis kombineerib ja asendab maksumaksja kaarti, tervisekindlustuskaarti, sotsiaalkindlustuskaarti ja valijakaarti.

Seadus nr 7/2007 loob aluse kodanikukaardi kasutuselevõtmiseks ja reguleerib selle väljaandmist, asendamist, kasutamist ja tühistamist. Selle järgi tekib 6 aasta vanusest nii kohalikul kui välismaal asuval Portugali kodanikul dokumendikohustus, kui ta peab suhtlema avaliku sektoriga. Kodanikukaart on piisavaks identiteedi tunnistuseks iga avaliku asutuse või eraettevõtte jaoks. Isikutel käes olevad maksumaksja, tervisekindlustuse, sotsiaalkindlustuse ja valijakaardid jäävad kehtima nende kehtivusaja lõpuni. 2015. aasta 13. mail muudeti seaduses nr 7/2007 dokumendi kehtivusaega. Kodanikukaardi kehtivusajaks on sellest ajast viis aastat või kuni kaardile märgitud tähtpäevani. Kui kasutaja on kaardi välja andmise hetkeks saanud 65-aastaseks, kehtib kaart tema elu lõpuni.

Kodanikukaart ei sisalda infot kasutaja rahalise seisu, tervise või heaolu kohta. Isikuandmeid hoitakse endiselt eraldi andmebaasides. Kaart ei võimalda rekonstrueerida kasutajate elu üksikasju, tagab selle kasutaja privaatsuse ja ei võimalda ligipääsu isikuandmetele ilma kasutaja nõusolekuta.

Kodanikukaardi taotlemisel tuleb esitada ID-kaart, tervisekindlustuse kaart, maksumaksja kaart, sotsiaalkindlustuse kaart ja valijakaart. Juhul kui ei ole võimalust teha fotosid fotoboksis, peab taotleja esitama kaks fotot. Lisaks kantakse kaardikiibile ka kaks sõrmejäljekujutist. Enne andmete lõplikku sisestamist süsteemi kinnitab taotleja kõigi esitatud andmete õigsust.

Digitaalallkirja sertifikaat aktiveeritakse vastavat aktiveerimiskoodi kasutades hiljem. Selle saab aktiveerida ainult kasutaja, kui ta on vähemalt 16 aastat vana ja teovõimeline.

Autentimis- ja digitaalallkirja sertifikaadid on kasutamisvalmis hiljemalt 24 tunni möödudes kaardi kättesaamisest arvates. Viivitus on seotud tühistusnimekirjade uuendamise ajakavaga.

Portugalis on kasutusel viis liiki passe: Portugali e-pass, diplomaatiline pass, spetsiaalpass (ametipass), ajutine pass ja välisresidendi pass.

Tavapassi taotlemiseks peab isiklikult ilmuma taotlust esitama SEFi (Portugali Välismaalaste ja Piiriteenistusse), IRNi (Portugali Registrite ja Notarite Institutsiooni) või Assooride või Madeira valitsuste teenindusbüroodesse.

Passi taotlemise protseduur algab taotleja isikusamasuse kontrolliga esitatud ID- või kodanikukaardi alusel, ilma selle esitamiseta passi taotleda ei saa. ID-kaardil või kodanikukaardil olevat infot kontrollitakse vastavas andmebaasis oleva infoga. Pärast seda saadetakse taotleja hõivekioskisse,

[25] Rohkem infot Portugali isikut tõendavate dokumentide väljaandmist reguleerivate õigusaktide kohta: https://www.cartaodecidadao.pt/index.php_option=com_content&task=view&id=107&Itemid=26&lang=pt.html

kus tehakse fotod ning hõivatakse sõrmejäljekujutised ning allkirjakujutis, seejärel maksab taotleja riigilõivu ning valib passi väljastamise koha.

Uue passi kättesaamisel võetakse vana pass ära, va juhul, kui seal on viisa, mille kehtivusaeg õigustab vana passi kasutaja kätte jätmist.

B

Üldine andmekaitseseadus on "Seadus 67/98 isikuandmete kaitse kohta". Kasutajate isikuandmete kaitset elektroonilise side valdkonnas ja eraelu puutumatust reguleerivad "Dekreetseadus 7/2004" ja "Seadus 46/2012" (küpsised). Sätted soovimatute teadete ja otseturunduse kohta on kehtestatud "Seadusega 41/2004", mida muudab "Seadus 46/2012".

Isikuandmeid võib töödelda, kui tüüptingimused on täidetud. Praktikas kasutatakse tihti andmetöötluse seaduslikkuse põhjendamiseks õigustatud huvide elluviimise tingimust. Andmekaitseseadus sisaldab erandeid teatud tüüpi andmete töötlemiseks. Nt seaduse enamusi sätteid ei rakendata, kui füüsiline isik töötleb isikuandmeid isiklikel või majapidamise eesmärkidel.

Delikaatsete, sh biomeetriliste andmete kasutamisel tuleb peamist tähelepanu pöörata tasakaalustatusele. Delikaatsete isikuandmete töötlemine on lubatud, kui:

- kaitstakse andmesubjekti või teise isiku elulisi huvisid;
- töötlemine ei toimu tulu saamise eesmärgil ja andmesubjekt on andnud oma nõusoleku;
- töötlemine on seotud andmetega, mida on andmesubjekt ise avaldanud;
- töötlemine on vajalik õiguslike nõuete koostamiseks, esitamiseks või kaitsmiseks;
- töötlemine on seotud tervise- ja seksuaaleluga, sh geneetiliste andmetega; ja
- töötlemine on vajalik meditsiinilistel põhjustel.

AKA luba on vajalik kõikidel muudel juhtudel (sh ka juhul, kui andmesubjekt on andnud oma nõusoleku töötlemiseks). AKA annab loa ainult juhul, kui:

- töötlemine on vajalik vastutava töötleja juriidilise või seadusest tuleneva õiguse teostamiseks; või
- kui andmesubjekt on andnud oma selgesõnalise nõusoleku.

Ebaseadusliku tegevuse või kuriteoga seotud isikuandmete töötlemiseks on samuti vajalik luba.

Vastutav töötleja peab teavitama AKAd enne automatiseeritud andmetöötlusega alustamist. AKA eelnev luba on vajalik, et töödelda delikaatseid isikuandmeid, kui see töötlemine ei vasta töötlemise tingimustele. Luba antakse ainult juhul, kui:

- töötlemine toimub vastutava töötleja juriidilise või seadusliku õiguse teostamiseks või andmesubjekti nõusolekul;
- töödeldakse ebaseadusliku tegevuse või kuriteoga seotud isikuandmeid;
- töötlemine on seotud andmesubjekti krediidi- ja maksevõimega;
- isikuandmeid soovitakse kasutada muudel eesmärkidel, kui need, mis määrati nende kogumisel; ja
- kui töödeldavate andmete kombinatsiooni ei ole õigusaktides kirjeldatud.

Delikaatsete isikuandmete mitteautomatiseeritud andmetöötluse jaoks on samuti vajalik luba.

AKA võib lihtsustada/kehtestada erandeid, mis vabastavad teavitamise kohustusest, teatud andmekategooriates, kus andmesubjektide rikkumine on vähe tõenäoline. Nendeks on praegu:

- töötajate palkade ja hüvitiste andmete töötlemine;
- raamatukogude ja arhiivide kasutajate haldamine;
- arvete loomine ja kontaktid klientide, tarnijate ja teenuseosutajatega;
- töötajate ja teenuseosutajate haldusjuhtimine;
- sisse- ja väljapääsude kontroll hoonetes; ja
- liikmetasude kogumine ja kontaktid partneritega.

Teatamisest on vabastatud ka avalike registrite haldajad. Volitatud töötleja peab töödeldavate andmete kaitseks kasutama tehnilisi ja organisatsioonilisi turvameetmeid. Vastutava ja volitatud töötleja vahel peab olema siduv kohustus – leping või õigusakt, mis sisaldab volitatud töötleja tüüpkohustusi.

Andmekaitseseadus ei sisalda üldkohustust teavitada AKAd või andmesubjekte andmetega seotud rikkumisest. Elektroonilise side sektoris tegutsevad teenuseosutajad peavad teavitama valdkonna kõikidest isikuandmetega seotud rikkumistest vastavalt "Seadusele 46/2012" ja "Elektroonilise side seadusele" AKAd ja ka andmesubjekte, kui:

- neile võib rikkumisega kaasneda kahju, ja
- sobivaid tehnoloogilisi turvameetmeid, mis muudavad lekitud andmed loetamatuteks, ei kasutatud.

Isikuandmete edastamine on lubatud riikidesse, kus on piisav andmekaitse tase või kui on täidetud piiriülese edastamise tüüptingimused. Andmekaitse piisavuse üle otsustab AKA, ent 2004. aastal kuulutas AKA välja, et hakkab järgima kõiki Euroopa Komisjoni otsuseid/suuniseid, kui komisjon leiab, et piisav kaitse on tagatud.

AKAd tuleb teavitada kõikidest andmeedastustest. Samuti on vajalik loa saamine, v.a juhul, kui andmeid edastatakse riiki, mille isikuandmete kaitse taset on Euroopa Komisjon hinnanud piisavaks või töötlejad kasutatavad lepingu tüüptingimusi.

AKA ei kinnitanud siduvate ettevõtluseeskirjade kasutamist.

3.8. Rootsi

A

Rootsis reguleerib digitaalallkirjade kasutamist „Kvalifitseeritud elektrooniliste allkirjade seadus“. 1998. aastal võeti vastu uue „Rootsi isikuandmete seaduse“ – uus versioon asendas vana, 1973. aasta redaktsiooni. Passide väljaandmist reguleerib „Passiseadus“ ja „Passimäärus“, siseriiklike ID-kaartide väljaandmist reguleerib „ID-kaardi määrus“. Rootsis on ka eraõiguslikke ID-kaartide väljaandjaid. Selliste ID-kaartide välja andmine toimub tööstusharu tavareeglite järgi ilma riigivõimu vahelesegamiseta.

Rootsi Kuningriigis ei ole keskset identiteedihaldust, nende mõistes keskse andmete repositooriumi olemasolu ei ole veel identiteedihalduse ilming. Nii avaliku kui erasektori ametkonnad ja asutused (riigi institutsioonid ja pangad) vastutavad ise identiteedihalduse eest.

Rootsi rahvastikuandmed registreeritakse rahvastikuregistris (rootsi *Folkbokföringsregistret*). See sisaldab infot inimeste kohta kes ja kus Rootsis elavad. Rahvastikuregistri eest vastutab Rootsi maksuamet (rootsi *Skatteverket*).

Rahvastikuregistris hoitavad andmed on üldjuhul avalikud. Mõningatel juhtudel võib see tuua kaasa andmesubjekti jaoks ohu või ähvardused. Sellisel juhul võib maksuamet lisada isiku andmetele nn turvamärke. Õiguslikke reegleid selle kohta ei ole ega pole ka absoluutset salastamist, kuid püütakse avalikustamist piirata nii palju kui võimalik.

Biomeetrilise info töötlemist loetakse Rootsis eriti delikaatsete isikuandmete töötlemiseks. Seda reguleerivad reeglid on väga piiravad ja mõningal juhul, eriti erasektoris, vajatakse andmesubjekti luba. Avalikus sektoris toimuva isikuandmete töötlemise puhul tuleb seda aga harva ette.

Isikut tõendavate dokumentide ja kasutajate andmeid hoitakse vastavate ametkondade juures. Eraõiguslikud väljaandjad vastutavad oma poolt välja antavate dokumentide andmete säilitamise eest.

Erinevalt näo- ja allkirjakujutisest ei tohi passi või ID-kaardi taotlemisel hõivatud sõrmejälgi keskses andmebaasis säilitada. Dokumendi isikustamise järgselt sõrmejäljekujutised baasist kustutakse ja need säilitatakse ainult dokumendi kiibis. Muid biomeetrilisi andmeid kui sõrmejäljekujutised, Rootsis ei kasutata. Ka ei tohi andmeid erinevate registrite vahel seostada.

ID-kaarte annavad välja kolm avaliku sektori ametkonda – maksuamet, politsei ja transpordiamet. Politsei tohib dokumente välja anda ainult Rootsi kodanikele. Rootsi politseiamet annab välja rahvusvaheliselt tunnustatud Euroopa Liidu standardile vastavat ID-kaarti, mida saab kasutada Euroopas reisimiseks, ja Rootsi passe, mida tunnustatakse isikut tõendava dokumendina üle kogu maailma.

Transpordiamet annab välja juhilube, mis kehtivad Rootsis isikut tõendavate dokumentidena. Selle taotlemiseks peab juhil olema juhtimisõigus ning kindlasti mõni teine Rootsi isikut tõendav dokument või mõni lähedane sugulane, kes identiteeti kinnitab ja teda ennast saab tuvastada mõne teise isikut tõendava dokumendiga.

2009. aastast alates on maksuamet ID-kaarte välja andnud ja see on identiteedi tuvastamise protsessi lihtsustanud välismaiste passikasutajate jaoks. Siiski leidub identiteedi tuvastamise nõudeid, mis loovad takistusi eriti välismaalastele.

Rootsi identiteedihaldusstrateegia põhineb kesksel rahvastikuregistril ja riiklikul isikukoodil (rootsi *Personnummer*). Kui see 1947. aastal rakendati, oli see tõenäoliselt omasuguste hulgas kõige

esimene, mis kattis kogu riigi elanikkonna. Koodid, mida annab välja Rootsi maksuamet, on osa rahvastikuregistrist.

Kõigil residentidel ja kodanikel peab olema isikukood. Seda saab taotleda ka siis, kui taotlejal pole ID-kaarti. Rootsis on ID-kaardid täiesti vabatahtlikud ja kõigil pole neid vaja, kuna isikut tõendavad dokumendid nagu juhiluba on siseriiklikult aktsepteeritud. Rootsis on ainult vähemusel riiklik ID-kaart, sest enamusel on pass ja juhiluba ja neil pole rohkem dokumente vaja. Seaduse järgi ID-kaardi nõuet ei ole.

Välismaiste isikut tõendavate dokumentide tunnustamine Rootsis on piiratud. Teise riigi isikut tõendavate dokumentide tunnustamist paralleelselt Rootsi passide ja ID-kaartidega pole valitsuse poolt reguleeritud.

Elektroonilise identiteedi haldus tugineb tsentraalsele registreerimispoliitikale: STOd pöörduvad oma teenuste pakkumisel rahvastikuregistri poole. Rootsis ei ole riiklikku juursertifikaati. Et pangad on pikka aega pakkunud identiteedikinnitusi, siis vastavalt valitsuse ja hankemenetluse käigus väljavalitavate nelja firma vahel sõlmitavale lepingule luuakse taristu, mille kaudu pakutakse kodanikele avaliku võtme infrastruktuuri sertifikaate ja avaliku sektori asutustele valideerimisteenust. Pangad on väga usaldusväärsed.

Strateegia ei näe ette ühtainust sisselogimisvahendit, kuid kõik agentuurid aktsepteerivad nende firmade poolt väljastatud elektroonilisi kinnitusi ja kasutajatel on alati sama kasutajaliides sõltumata sellest, kes identifitseerimist nõuab.

Rootsis on eID juurutatud väga pragmaatilisel viisil. Valitsus on kehtestanud standardid ja kontrollib neid standardeid. eID vahendite turg on avatud. Kui keegi vastab nendele standarditele, saab ta süsteemiga ühineda. Faktiliselt domineerivad kasutuses pankade autentimised. Valitsus ei tahtnud tehnoloogiat enda peale võtta ja turg valmistati ette autentimisteenuste pakkumiseks, kui nende eest makstakse.

Kuigi pangalahendus ei katnud alguses täielikult kõiki eID aspekte, oli see praktiline ja võimaldas kiiret vastuvõttu. Nende jaoks, kes ei saanud varem eID võimalusi kasutada, leiti lahendus, kui eID funktsionaalsus lisati avalikule ID-kaardile. Selle otsusega lisati eID skeemile avalik kandja ja skeem muutus juriidilises mõttes segatud süsteemiks. Tegelikult käib enamik tehinguid läbi pankade. Rootsi aktsepteerib pankade välja antud eID-kaarte (tuntud kui *BankID*) valitsusasutustes sobiva identifitseerimisvahendina. *BankID* teeb võimalikuks Rootsi ametiasutustesse, ülikoolidesse ja pankadesse turvalise sisselogimise. *BankID* võib olla sertifikaadifailina andmekandjal, kaardil või nutitelefonis. Viimane (Rootsi BankID mobiiliteenus) ei too kasutajale kaasa täiendavat tasu ja teeb võimalikuks sisselogimise lauaarvuti veebiakna kaudu.

Strateegia toetab kaht kinnitust: tarkvaraline pääsmik[26] faili kujul, mida üksikisikud saavad oma arvutisse alla laadida ja riistvaraline, mis on tavaliselt kaardi kujul. Mõlemad võimaldavad kahe sertifikaadi kaudu autentimist ja e-allkirja. Tarkvaralist kinnitust kasutatakse peaaegu kõigis tehingutes. Riiklikes rakendustes on kasutusel ka teised e-autentimise vormid – kasutajanimi/salasõna või kaheteguriline autentimine (kasutajanimi/salasõna + SMS[27]). Iga teenusepakkuja otsustab ise, millist autentimislahendust ta kasutab.

[26] inglise keeles "*soft token*"

[27] tekstisõnum

Et andmete rahvastikuregistrisse kandmisel identifitseeritakse isikud personaalselt, siis see välistab mitmikidentiteetide tekkimise. Kui aga mingil põhjusel on see nii läinud, siis liidetakse need identiteedid kokku üheks.

Biomeetriliste andmete halduse kohta identiteedivahetuse puhuks Rootsis seadusi pole. Juhul kui kaitse all oleva isiku identiteet tuleb blokeerida, siis informatsiooni rahavastikuregistrist tema kohta kätte ei saa. Kui on vaja sellise inimesega sidet pidada, siis võib näiteks saata posti maksuametisse, kes siis tagab, et see isik osa posti kätte saab.

B

Rootsi oli esimene riik maailmas, mis rakendas riikliku andmekaitsealase seadusandluse, ja üks esimesi, kes rakendas rahvastikuregistri ja isikukoodide süsteemi.

Üldine andmekaitseseadus on "Rootsi isikuandmete seadus". Seaduse enamust sätteid ei pea järgima, kui töötlemine toimub kooskõlas õigusaktiga, mille nimetus on „Struktureerimata materjali reegel“ – see õigusakt rakendub, kui isikuandmeid töödeldakse automaatselt ning andmed on „struktureerimata” ehk ei too kaasa andmesubjekti puutumatuse rikkumist. Selliste andmete hulka kuuluvad nt internetis avaldatud tekstid ja helisalvestused.

AKA ülesanne on tagada, et ametiasutused, ettevõtted, organisatsioonid ja üksikisikud jälgiksid isikuandmete töötlemisel "Rootsi isikuandmete seadust", "Andmete seadust (1973)", "Võla sissenõudmise seadust (1974)", "Krediidiinfo seadust (1973)".

Kasutajate isikuandmete kaitset elektroonilise side valdkonnas ja eraelu puutumatust reguleerivad: "Turukaitseseadus", "Elektroonilise side seadus" ja "Kaamera jälitustegevuse seadus". Lisaks on Rootsis mitmeid reegleid eri otsuste ja määruste alusel, eri alade asutuste suhtes, näiteks tervishoiu sektoris ja ka finantsteenuste suhtes. Säärased reeglid täiendavad isikuandmete seadust ja muid seadusi.

Isikuandmeid võib töödelda, kui tüüptingimused on täidetud. Praktikas kasutatakse tihti andmetöötluse seaduslikkuse põhjendamiseks õigustatud huvide elluviimise tingimust.

Delikaatseid isikuandmeid võib töödelda, kui nende töötlemise tüüptingimused on täidetud. Andmeid õigusrikkumise kohta (mõne erandiga) võivad töödelda ainult avalik-õiguslikud asutused, va juhul kui AKA on andnud ka muule asutusele selleks loa. Kui isikukoodide töötlemiseks puudub andmesubjekti luba, võib neid töödelda ainult juhul, kui töötlemise eesmärk on selgelt määratletud, oluline on turvaline isikutuvastamine või muu märkimisväärse põhjuse olemasolul. Ükski eespool kirjeldatud piirangust ei kehti, kui isikuandmeid töödeldakse vastavalt "Struktureerimata materjali reeglile" (kirjeldatud eespool).

On olemas üldkohustus teavitada AKAd isikuandmete töötlemisest. Teavitamisega ei kaasne loa saamise kohustust. Teavitust tuleb esitada enne esimest andmetöötlust ja teavitamine on tasuta.

Teavitamise kohustus kohaldub andmete suhtes, mida töödeldakse täiesti või osaliselt automaatselt. Lisaks on olemas teavitamisest vabastamise tingimused, nt kui:

- andmesubjekt on andnud nõusoleku, et tema andmeid töödeldakse;
- vastutav töötleja on määranud ja registreerinud isikuandmete eest vastutavat isikut;
- isikuandmed ei ole delikaatsed ja puudutavaid isikuid, kellega on vastutaval töötlejal olemas seos (nt töötaja, organisatsiooni liige, klient), ning vastutav töötleja järgib töötlemise plaani, mis mh sisaldab infot, mida vastutav töötleja oleks teavitusse lisanud;
- töötlemine on kooskõlas "Struktureerimata materjali reegliga".

Volitatud töötleja peab töötlema isikuandmeid vastavalt kirjalikule lepingule, mis sisaldab volitatud töötleja tüüpkohustusi. See rakendub ka juhul, kui andmeid töödeldakse kooskõlas "Struktureerimata materjali reegliga".

Andmekaitseseadus sisaldab üldkohustust isikuandmete eest vastutaval isikul teavitada AKAd kõikidest kahtlusalustest rikkumistest. Elektroonilise side sektoris tegutsevad ettevõtted peavad teavitama isikuandmetega seotud rikkumistest vastavalt "Elektroonilise side seadusele".

Isikuandmete edastamine on lubatud riikidesse väljapoole Euroopa majanduspiirkonda, kus on tagatud andmete piisav kaitse või kui on täidetud piiriülese edastamise tüüptingimused. Vastutav töötleja võib ise hinnata, kas andmete tagatakse peale nende edastamist kolmandasse riiki piisav kaitse. See piirang ei kehti, kui isikuandmeid töödeldakse kooskõlas "Struktureerimata materjali reegliga".

Kui piiriülese edastamise tüüptingimused on täidetud, puudub AKA teavitamise kohustus, v.a siduvate ettevõtluseeskirjade kasutamise korral. Kuid AKA on sätestanud, et kui kasutatakse andmekaitsemeetmeid (nt lepingu tüüptingimusi), siis vastutav töötleja peab taotlema AKAlt vabastust edastamise keelust. Riigis puudub kohustus teavitada AKAd lepingu tüüptingimuste kasutuselevõtust või saada nende kasutamiseks luba.

Rootsis tunnustatakse siduvate ettevõtluseeskirjade kasutamist. Kuid AKA ei liitunud siduvate ettevõtluseeskirjade vastastikuse tunnustamise süsteemiga, mistõttu tuleb AKAle esitada eraldi taotlus.

3.9. Saksamaa

A

Saksamaal reguleerib passide väljaandmist „Passiseadus“ ja ID-kaartide väljaandmist „ID-kaardi ja elektroonilise identifitseerimise seadus“.

On olemas seadus suletud süsteemis kasutatavate elektronpostisõnumite kohta – „De-Maili seadus“. See seadus reguleerib niinimetatud *De-mail*i teenusepakkuja aktsepteerimist ja tööd – "elektroonilise kommunikatsiooniplatvormi teenused tagamaks turvalist, konfidentsiaalset ja tuvastatavat äri igaühele üle interneti." Teenusepakkujad peavad rahuldama kõrgeid andmeturbe ja -kaitsenõudeid ja peavad enne teenusepakkumisega alustamist läbima akrediteerimisprotsessi. Kasutajad autenditakse kindlalt enne konto aktiveerimist ja seejärel saab ta *De-maile* saata/vastu võtta. Identifitseerimisprotsessi jaoks saab kasutada Saksa ID-kaardi (*Personalausweis*) eID funktsiooni või identifitseerib kasutaja teenusepakkuja personal.

„Elektroonilise allkirja taristu seadus“ võeti vastu 2001. aasta 16. mail ja muudeti viimati 2013. aasta 7. augustil.

Saksamaal ei ole keskset identiteedihaldust. isikuidentiteetide andmebaasid on detsentraliseeritud. Föderaalne konstitutsioonikohus (*Bundesverfassungsgericht*) on langetanud otsuse, et isikuandmeid ei tohi seostada mitmes kohas samal eesmärgil kasutatava numbriga (kuulus 1983. aasta "rahvaloenduse kohtuasi"; BVerfG, 15.12.1983, 1 BvR 209). On oluline, et iga numbrit, mida ametkond on kodanikule andnud, tohib kasutada rangelt ainult selle konkreetse administratiivprotseduuri käigus. On harvad juhused, mil sellest reeglist võib kõrvale kalduda ja need on seaduses kirjas.

Identifitseerimissüsteemide haldamisega tegelevad:

- Isikut tõendavaid dokumente annavad välja ID- ja passiametid. Iga kohalik omavalitsus peab oma registrit ning nad peavad sidet omavahel ainult juhul, kui näiteks kodanikud kolivad ühest linnast teise. Väljaandjad peavad hoolitsema selle eest, et ühte ID-numbrit mitu korda välja ei anta.
- föderaalne keskmaksuamet haldab maksumaksja identifitseerimisnumbrite (*Steuerliche Identifikationsnummer* ehk *Steuer-Id Nr*) väljaandmist kõigile füüsilistele isikutele. Ka annab föderaalne keskmaksuamet organisatsioonidele välja majandusidentifitseerimisnumbreid (*Wirtschafts-Identifikationsnummer*).
- Föderaalne võrguamet (*Bundesnetzagentur*) on STO (Saksa Liitvabariigi tipmine sertifitseerija kvalifitseeritud allkirjade jaoks). Föderaalne võrguamet on vastutav ametkond vastavalt “Elektroonilise allkirja taristu seaduse” (SigG) §-le 3.
- Saksa Infoturbe Föderaalamet (*Bundesamt für Sicherheit in der Informationstechnik*) on elektrooniliste ID-kaartide, passide ja terminaalide STO.
- Saksa tervishoiuvõrk (*Deutsches GesundheitsNetz*) on STO – kvalifitseeritud ja täiustatud e-allkirjad[28] tervisespetsialistidele ja meditsiiniteenuste pakkujatele. Tervisekindlustusfirmad kasutavad sama tüüpi haiguskindlustusnumbreid (*Krankenversichertennummer*). Nende loomine toimub vastavalt „Sotsiaalseadustikule“, § 290 SGB V.
- ZDF (*Zweites Deutsches Fernsehen*) – Saksa televisioonifirma, STO – pakub sertifitseerimisteenuseid (suure jõudlusega PKI koos firmakaartidega).

[28] vastavalt Euroopa Parlamendi ja Nõukogu direktiivi 1999/93/EÜ artiklile 2.2

Saksamaal on identifitseerimisvahendite, kaasa arvatud elektroonilise identifitseerimise vahendite väljaandmine ainult avaliku sektori ülesanne.

Saksamaal pole põhiseaduse järgi lubatud isikukoodi kasutamine. Üksikisikuid tuvastatakse rea iseloomulike tunnuste alusel ja identifitseerimisnumbrid on sektorikohased. Seega põhineb Saksamaa strateegia kesksel registreerimispoliitikal, mis ei tugine unikaalsele identifikaatorile. Üksikisikuid identifitseeritakse selliste iseloomulike tunnuste kombinatsiooni alusel, nagu ees- ja perekonnanimed ning sünnikuupäev. Maksumaksja identifitseerimisnumbrid antakse füüsilistele isikutele, majandusidentifitseerimisnumbrid antakse organisatsioonidele; erilistel põhjustel antakse käibemaksu identifitseerimisnumbreid isikutele ja organisatsioonidele, kes peavad oma laekumilt käibemaksu maksma. Lisaks antakse kõigile sõjaväeteenistusse astujatele teenistusnumber. Ühtki neist numbritest ei kasutata mingil teisel eesmärgil, ka on selline (väär)kasutus seadusevastane. Saksa isikut tõendavad dokumendid ei sisalda ühtki neist numbritest, ainult dokumendinumbrit. Inimestelt ei oodata ametkondadega suhtlemisel oma numbrite teadmist, nii tuleb ette inimeste segiajamist.

Isikuandmetega ümberkäimist reguleeritakse ID-kaartide ja elektroonilise identifitseerimise seaduse §§ 14 – 20, Saksa kodanike identiteetide tuvastamine toimub kooskõlas „ID-kaardi ja elektroonilise identifitseerimise seaduse“ § 17-ga. Mittesaksa kodanike identiteetide tuvastamine toimub siseriiklike ja rahvusvaheliste andmebaaside kaudu nagu näiteks välismaalaste keskregister, Europoli infosüsteem (EIS) jt.

Saksamaa võttis elektroonilised ID-kaardid (*Personalausweis*) kasutusele 2010. aastal. Saksa strateegia ei näe ette ühtainsat sisselogimisviisi läbipaistvuse põhjusel (*online*-autentimistelt ei tohi isikuandmeid edastada kolmandatele isikutele). Kuid üheainsa sisselogimisega süsteemide pääsmikke võib kasutajale *online*-autentimise põhjal anda. Saksamaa ID-kaart on kontaktivaba liidesega ja samuti on välja töötatud mobiil-ID, kus mobiiltelefon talitleb kaardilugejana. ID-kaardisse on integreeritud protsessorikiip, mis toetab identiteedi elektroonilist tõendamist (e-äri ja e-identiteedi puhul, vaja läheb PINi ja autoriseerimissertifikaati) ja kvalifitseeritud elektroonilist allkirja (sertifikaadi saab hiljem kiibile laadida, seda ei anna välja riik, vaid selle saab turult).

Saksamaa valis otseselt avaliku eID, et jälgida privaatsust ja ohutust. Isikut tõendavate dokumentide tootmises osalevad erafirmad ja neid kontrollib valitsus.

Saksamaal pole lubatud mitmekordsed identiteedid. Vastavalt seadusele peab saksa kodanikul olema kaasas ID-kaart (või pass), mis võimaldab isikut üheselt tuvastada. Identiteedi võib siduda täiendavate tunnustega nagu pseudonüüm või lavanimi[29]. Siiski on biomeetriliste andmete töötlemine seotud isiku unikaalse identiteediga.

Volitatud esindaja ei saa ID-kaardi taotlust sisse anda passitaotleja või tema seadusliku esindaja eest (vt § 9 lõige 1 lause 3 ID-kaartide ja elektroonilise identifitseerimise seaduses). Iga identiteedi tuvastamine (loomine) – olgu siis ID-kaardi või passi puhul – algab isiku kohaletulekuga ID-kaardi/passiametisse.

B

Üldine andmekaitseseadus on „Saksamaa andmekaitse föderaalseadus". Saksamaa 16 liidumaal on liidumaa tasemel andmekaitseseadused. Need kehtivad avaliku sektori suhtes ainult sellel liidumaal. Isikuandmete kaitset online-turunduse (elektronpost, tekstisõnumid ehk SMS, multimeediasõnumid ehk MMS) puhul reguleerib "Kõlvatu konkurentsi seadus". Kasutajate isikuandmete kaitset

[29] Näiteks tuntud saksa laulja lavanimega Nina Hagen, kelle pärisnimi on Catharina Hagen

elektroonilise side valdkonnas ja eraelu puutumatust reguleerib "Saksamaa telekommunikatsiooniseadus". Seadus sisaldab ka majandusharuspetsiifilisi andmekaitse-meetmeid, mis kehtivad telemeedia teenusepakkujate suhtes nagu näiteks veebilehekülgede pakkujad. Andmetega seotud rikkumistest teavitamise kohustus tuleneb "Saksamaa telemeedia-seadusest" ja rakendub ainult telemeediateenuste osutajate suhtes. Seadus sisaldab samuti majandusharuspetsiifilisi andmekaitsemeetmeid, mis kehtivad telemeedia teenusepakkujate suhtes nagu näiteks veebilehekülgede, internetiühenduste ja WLAN kuumkohtade ligipääsuteenuse pakkujad.

Isikuandmeid võib töödelda, kui tüüptingimused on täidetud. Täiendavad reeglid rakenduvad järgmiste andmete suhtes:

- töötajate andmed;
- turunduse ja otseturustuse jaoks kasutatavad andmed;
- skoorimine; ja
- turu- ja arvamusuurigud.

Delikaatseid isikuandmeid võib töödelda, kui nende töötlemise tüüptingimused on täidetud.

Automatiseeritud töötlemise protseduure tuleb üldjuhul ette registreerida. Neid protseduure tuleb registreerida eeskätt juhul, kui vastutav töötleja salvestab isikuandmeid kaubanduslikel eesmärkidel, et edastada need kolmandatele isikutele või turu-uuringu läbiviimiseks. Registreerimine on igal juhul tasuta.

Registreerimine ei ole vajalik, kui:

- vastutav töötleja on määranud andmekaitse eest vastutavat isikut (mis on Saksamaal väga levinud) ; või
- enamasti on töötlemisse kaasatud kuni üheksa töötajat ja selleks kas saadakse andmesubjekti nõusolek või andmete kasutamine on vajalik andmesubjektiga lepingu sõlmimiseks, täitmiseks või lõpetamiseks.

Samuti pole vaja registreerida kui ei kohaldata erandeid.

Kui vastutav töötleja volitab andmetöötlust, peab ta sõlmima kirjaliku lepingu volitatud töötlejaga, mis peab sisaldama miinimumnõudeid, mis omakorda koosnevad volitatud töötleja tüüpkohustustest ja täiendavatest kohustustest, nt töötlemise objekti kirjeldus, töötlemise tähtajad, volitatud töötleja kohustus teavitama vastutavat töötlejat andmetega seotud rikkumistest. Vastutav töötleja vastutab, et volitatud töötleja tegutseks kooskõlas andmekaitseseadusega. Seetõttu peab vastutav töötleja tagama, et andmeid töödeldaks vastavalt tema juhistele.

Eraisikud peavad teavitama vastavat AKAd ja andmesubjekte andmetega seotud rikkumistest. Kui kõiki isikuid, keda võib rikkumine mõjutada, on raske teavitada rikkumisest otse, tuleb teade avaldada kahes päevalehes. Telemeedia sektoris tegutsevad ettevõtted peavad teavitama valdkonna kõikidest isikuandmetega seotud rikkumistest vastavalt "Saksamaa Telemeedia-seadusele".

Kui Saksamaa andmekaitseseaduses kehtestatud piiriülese edastamise tingimused on täidetud, siis on isikuandmete edastamine lubatud riikidesse väljapoole Euroopa majanduspiirkonda juhul, kui piiriülese edastamise tüüptingimused (EL) on ka täidetud.

Andmekaitseseadus ei sisalda kohustust teavitada AKAd juhul, kui isikuandmeid edastatakse väljapoole Euroopa majanduspiirkonda kasutades lepingu tüüptingimusi. Kuid mõni AKA nõuab

andmete edastajalt allkirjastatud lepingu tüüptingimuste esitamist teadmiseks. Pealegi, kui tüüptingimusi muudetakse, tuleb saada AKAlt täiendav luba.

Kui isikuandmeid edastatakse Saksamaalt välismaale, tuleb läbida kaheastmeline test. Esimene etapp – kas on olemas õiguslik alus isikuandmete kolmandale isikule edastamiseks (sh juhul, kui andmeid edastatakse rahvusvahelise kontserni siseselt). Teine etapp – kas andmetele tagatakse piisav kaitse riigis, kuhu neid edastatakse. Andmete edastamiseks kasutatakse ELi lepingu tüüptingimusi, rahvusvaheliste ettevõtete siseselt muutuvad üha levinumaks siduvad ettevõtluseeskirjad.

Saksamaa on liitunud siduvate ettevõtluseeskirjade vastastikuse tunnustamise süsteemiga, kuid ettevõtluseeskirjade kasutamise korral on AKA luba nende kasutamiseks ikkagi vajalik. Mõni Saksamaa AKA nõuab lisaks iga andmeedastuse eraldi kooskõlastamist.

3.10. Soome

A

Identiteedivaldkonna põhilised seadused on: „Rahvastikuandmete ja rahvastikuregistri tõendite seadus“, “ID-kaardi seadus”, “Passiseadus”, “Välismaalaste seadus”, “Turvalise elektroonilise autentimise ja elektrooniliste usaldusteenuste seadus”.

Identiteedihaldusstrateegia põhineb rahvastikuregistril ja isikukoodil.

Soomes identiteete kesksel ei hallata. Nii avalik kui erasektor (valitsusasutused, pangad, mobiilioperaatorid) on identiteedihalduse eest vastutavad. Soomes on pikaajaline traditsioon lubada oma eID süsteeme kasutada erasektori algatustel (eriti e-panganduse rakenduste puhul).

Soomes on kasutusel pooltsentraliseeritud digitaalse identiteedi ökosüsteem. Seal on mitu identiteedipakkujat (näiteks valitsusasutused, pangad, mobiilioperaatorid jt), mille vahel kodanikud saavad vabalt valida ja kasutada saadud kinnitusi laiale ringile teenustele ligipääsuks läbi identifitseerimiskeskkonna. Sellises ökosüsteemis mängivad erafirmad digitaalse identiteedi pakkuja rolli, kui valitsus on sellele andnud ametliku, alusdokumentidel (nagu näiteks sünni-tunnistused) põhineva toe.

Rahvastikuregister sisaldab isikuandmeid, mida hallatakse keskregistri ja kohalike harukontorite kaudu. Info isikut tõendavatest dokumentidest, sh. isikuandmed ja biomeetria, säilitatakse politsei hallatavas (passid ja ID-kaardid) ning migratsiooniameti hallatavas (elamisload) keskses infosüsteemis. Politsei väljastab isikut tõendavaid dokumente Soome kodanikele ja välismaalastest residentidele juhul, kui nendes registrites säilitatav info on usaldusväärselt kontrollitud.

Iga Soome kodanik saab sündimisel isikukoodi. Seaduse järgi saab isikukoodi ka iga välismaalane, kes elab Soomes kas alaliselt või kauem kui üks aasta. Et isikukood sisaldab sünniaega ja sootunnust, siis seda tohib kasutada ainult eriloa alusel. Soovitav on seda mitte avaldada, näiteks jälgivad tööandjad isikukoodi abil tihti töötajate palku. eID rakenduste pakkujad tohivad kasutada isikukoodi ainult juhtudel, mis on heaks kiidetud privaatsusombudsmani poolt ja kooskõlas isikuandmete seadusega. Teenusepakkujad kvalifitseeruvad isikukoodi kasutamiseks juhul, kui nad täidavad selle seaduse nõudeid. Isikukood kantakse nii kiibiga ID-kaardile, uuele ja vanale juhiloale kui ka passi. Juhiloa kasutamine isikut tõendava dokumendina väheneb väljastusprotsessi usaldusväärsuse vähenemise tõttu.

Soome rahvastiku infosüsteem on arvutiseeritud riiklik register, mis sisaldab Soome kodanike ja Soomes püsivalt elavate välismaalaste põhiinfot. Soome rahvastikuinfo on kõrge kvaliteedi poolest rahvusvaheliselt hinnatud. Infot sisestavad registrisse seadusega ette nähtud teatistega üksikisikud ja riigiasutused. Seal sisalduvat infot kasutatakse kogu Soome infoteenustes ja -halduses, sealhulgas avalikus halduses, valimistel, maksustamisel, justiitshalduses, uuringutel ja statistikas. Erafirmad ja muud eraõiguslikud organisatsioonid võivad samuti sellele infole ligipääsu saada. Süsteemis salvestatakse nimi, isikukood, aadress, kodakondsus ja emakeel, perekonnasuhted ja sünni- ning surmakuupäevad (kui on olemas).

Soome kodanikele antakse välja nii passe kui ID-kaarte. Vähemalt üks neist dokumentidest peab isikul olema, aga tal on vabadus valida, kumba ta eelistab. Nii passe kui ID-kaarte antakse välja ka alaealistele.

Soome oli esimene riik maailmas, kus ID-kaart kasutusele võeti. See põhineb vabatahtlikul rakendamisel ja kasutajad maksavad kinni kogu kaardi maksumuse. Soomes on ID-kaart vähemusel,

sest enamusel on siseriikliku isikut tõendava dokumendina tunnistatud pass või juhiluba ja nad ei vaja enamat.

Soome oli esimene riik Euroopas, kes eID projektiga (FIN-ID) 1999. aastal algust tegi.

Pakutakse ligipääsu nii avaliku kui erasektori teenustele.

Kõigis politsei väljastatavates ID-kaartides on kiip, va. vanemate/eestkostja nõusolekuta väljastatud ja ajutistes ID-kaartides. Politsei välja antud kiibiga kaartides on rahvastikuregistri (*Väestörekisterikeskus, VRK*) kodanikusertifikaat, mis võimaldab kasutajat e-teenustes autentida. Lisaks saab ID-kaardile kanda ka tervisekindlustusinfot, mis võimaldab seda kasutada ka tervisekindlustuskaardina. Selliste kaartide kehtivusaeg on viis aastat. Tervisekindlustusinfo kehtivuse määrab pensioniamet (*Kansaneläkelaitos, KELA*).

Soome eID-kaart põhineb rahvastikuinfosüsteemil ja avaliku võtme infrastruktuuril. Kiibil on kaks sertifikaati, üks autentimiseks ja teine kvalifitseeritud elektroonilise allkirja andmiseks. Kaarte annab välja ja administreerib Soome rahvastikuregister, mis haldab rahvastikuinfosüsteemi (*Väestötietojärjestelmä*), milles on kõigi Soome kodanike ja registreeritud püsielanike autentsete identiteeditunnuste võtmekomplekt. Kõik eID-kaardi autentimissertifikaadis salvestatud tunnused saadakse otse rahvastikuinfosüsteemist, välja arvatud kasutaja meiliaadress, mille saab lisada kasutaja soovil.

eID-kaart peab võistlema juba kasutusel olevate BankID-dega, mida pangad on välja andnud juba pikka aega. Kõik suuremad Soome pangad, nende hulgas Aktia, Osuuspankki, Nordea, Danske Bank ja S-Pankki, kasutavad kodumaist süsteemi TUPAS. TUPAS on Soome finantsteenuste liidu poolt välja töötatud tugeva digitaalse autentimise meetod ja see on *de facto* Soome digitaalse identifitseerimise standard. Pangad pakuvad TUPAS-tuvastust ka teistele internetis kättesaadavatele teenustele, sealhulgas avaliku sektori omadele, näiteks sisselogimiseks pensioniametisse või Soome maksuameti saidile *vero.fi*.

TUPAS baseerub „Turvalise elektroonilise autentimise ja elektrooniliste usaldusteenuste seadusele“. Vastavalt sellele seadusele peab turvaline identifitseerimismeetod sisaldama vähemalt kahte kolmest järgmisest identifitseerimismeetodist:

- salasõna või midagi, mida kasutaja teab;
- kiipkaart või midagi sarnast, mis on kasutajal olemas; ja/või
- sõrmejälg või midagi sarnast, mis on isiku puhul unikaalne. [elektroonilise autentimise ja elektrooniliste usaldusteenuste seadus]

Tavaliselt kasutatakse identifitseerimiseks salasõna ja ühekordseid paroole või paroolikalkulaatorit.

TUPAS-autentimine asendatakse lähemas tulevikus avaliku sektori rajatava teenusearhitektuuri (*Kansallinen palveluarkkitehtuuri*)[30] autentimisteenusega.

Mobiilioperaatorite pakutavad avaliku võtme infrastruktuuri eID lahendused pole eriti levinud, sest pangad on end selles sektoris tugevalt kindlustanud.

B

Üldine andmekaitseseadus on "Soome isikuandmete seadus". Lisaks "Soome isikuandmete seadusele" mõjutab isikuandmete kaitset ja sidet ka "Infoühiskonna seadus". Kasutajate

[30] põhineb Eesti X-tee lahendusel koostöös RIAga

isikuandmete kaitset elektroonilise side valdkonnas ja eraelu puutumatust reguleerib "Soome infoühiskonna koodeks". Isikuandmete kaitset mõjutavad ka erinevad valdkonnaspetsiifilised õigusaktid, nt "Tööelu puutumatuse kaitse seadus", "Valitsuse tegevuse avatuse seadus", "Patsientide staatuse ja õiguste seadus", "Biopankade seadus", "Taustakontrolli seadus", "Sotsiaalhoolekande klientide positsiooni ja õiguste seadus".

Isikuandmete töötlemise tingimused vastavad suures osas töötlemise tüüptingimustele. Töötlemise eesmärke, andmete allikaid ja salvestatud isikuandmete saajad tuleb määratleda enne töötlemist, kui andmeid plaanitakse salvestada registrisse või isiklikku andmefaili. Andmekaitseseadus sisaldab erandeid teatud tüüpi andmete töötlemiseks. Kui andmeid töödeldakse eriotstarbel (nt uuringu või statistika jaoks), siis enamikku selle seaduse sätetest ei rakendata.

Delikaatsete isikuandmete töötlemine on üldjuhul keelatud, kuid on olemas erandid. Põhimõtted vastavad suures osas delikaatsete isikuandmete töötlemise tüüptingimustele, mis on kehtestatud Andmekaitsedirektiiviga. Sh võib AKA lubada delikaatsete isikuandmete töötlemist, kui on olemas märkimisväärne avalik huvi. Luba antakse kindlaks ajaperioodiks või kindla juhu jaoks; see sisaldab andmesubjekti õiguste kaitsmise reegleid.

Vastavalt "Tööelu puutumatuse kaitse seadusele", mis reguleerib töötajate isikuandmete töötlemist, võib tööandja töödelda andmeid töötajate tervise kohta ainult juhul, kui need andmed saadi töötaja enda käest või tema nõusolekul, ja infot on vaja töödelda hindamaks töötaja töövõimet, puudumise põhjust või töötasu arvutamiseks.

Kui tegemist ei ole erandiga, peab vastutav töötleja teavitama AKAd automatiseeritud andmetöötlusest ja andmete edastamisest väljapoole Euroopa majanduspiirkonda, mis nõuab sellist teavitamist hiljemalt 30 päeva enne töötlemisega alustamist. Loa saamine ei ole vajalik ja teavitamine on tasuta. Lisaks teavitamise kohustusele, vastutav töötleja peab kirjeldama igat andmefaili koos töötlemise põhjuste ja põhimõtete kirjeldamisega. Andmefaili kirjeldus peab olema kättesaadav kõigile andmesubjektidele ülevaatamiseks.

Kõik vastutavad töötlejad peavad teavitama AKAd, kui ei kehti vähemalt üks eranditest, sh, kui mitte ainult:

- andmesubjekt on andnud oma ühemõttelise nõusoleku töötlemiseks;
- andmesubjekt on andnud töötlemise ülesande või töötlemine on vajalik andmesubjektiga lepingu sõlmimiseks või täitmiseks;
- töötlemine on vajalik andmesubjekti eluliste huvide kaitsmiseks konkreetses juhtumis;
- on olemas seaduslik alus töötlemiseks;
- on olemas asjakohane seos vastutava töötleja ja andmesubjekti vahel, nt andmesubjekt on klient või organisatsiooni liige;
- isikuandmed puudutavad kontserni vm majandusliku ühenduse kliente või töötajaid ja andmeid töödeldakse selle ühenduse siseselt; või
- juhatus on andnud loa töötlemiseks.

Lisaks võib kehtestada erandeid dekreediga, kui muutub selgeks, et isikuandmete töötlemine ei riku andmesubjekti vabadusi või õigust eraelu puutumatusele.

Volitatud töötleja peab enne töötlemisega alustamist rakendama turvameetmeid ja kindlustama andmete kaitset. Neid meetmeid ja garantiisid soovitatakse kirjeldada lepingus vastutava ja volitatud töötleja vahel. Töötlemise käigus saadud infot teiste isikute omaduste, isiklike asjaolude või majandusliku olukorra kohta ei tohi avaldada kolmandatele isikutele.

Andmekaitseseadus ei sisalda kohustust teavitada AKAd andmetega seotud rikkumistest. Elektroonilise side sektoris tegutsevad ettevõtted peavad teavitama valdkonna isikuandmetega seotud rikkumistest vastavalt "Infoühiskonna seadusele".

Isikuandmete edastamine kolmandatesse riikidesse on lubatud, kui vastutav töötleja täidab piiriülese edastamise tüüptingimusi. Alternatiivina võib isikuandmeid edastada väljapoole Euroopa majanduspiirkonda, kui:

- kõnealune riik tagab nende piisava kaitse; või
- kasutatakse lepingu tüüptingimuste modifitseeritud versiooni.

AKA loa saamine ei ole vajalik, kui kasutatakse muutmata lepingu tüüptingimusi. AKAd on vaja teavitada, kui:

- andmeedastusleping ei vasta lepingu tüüptingimustele;
- andmeedastus põhineb vastutava töötleja enda hinnangule kõnealuse riigi andmekaitse piisavuse kohta;
- andmeid edastatakse teatud registrist, mille kohta kehtivad eraldi reeglid või
- kui Euroopa Komisjon on leidnud, et vastutav töötleja ei taga andmete piisavat kaitset.

Siduvate ettevõtluseeskirjade kasutamine rahvusvahelise kontserni siseselt on lubatud, kui AKA on eelnevalt siduvad ettevõtluseeskirjad kooskõlastanud ja kui kontserni kõik firmad jälgivad neid eeskirju. AKA ei kinnitanud veel siduvate ettevõtluseeskirjade laialdast kasutamist, kuid on teinud seda nende firmade suhtes, kes esitasid vastava taotluse Soomes ning kellele oli teise liikmesriigi AKA juba lubanud siduvate ettevõtluseeskirjade kasutamist.

3.11. Suurbritannia

A

2006. aastal võeti vastu „ID-kaardi seadus“. „Isikut tõendavate dokumentide seadus“ on pärit 2010. aastast.

Suurbritannias ei ole keskset identiteedihaldust. Igal avaliku või erasektori osal on oma identiteedihalduse süsteem.

2006. aastal vastuvõetud ID-kaardi seadus nägi ette riiklikku identiteediregistrit sisaldava ID-kaardi skeemi. Esimesed kaardid anti välja 2009/2010. aastal ja kokku anti välja umbes 15 000 kaarti.

2010. aastal toimusid Suurbritannias üldvalimised. Nende tulemusena ametisse asunud valitsuse korraldusel lõpetati “Isikut tõendavate dokumentide seadusega” igasugune tsentraliseeritud identiteedihaldus Suurbritannias, hävitati riiklik identiteediregister, katkestati ID-kaardi ja identiteediregistri projektid ning tühistati juba välja antud ID-kaardid. Sama seadusega kehtestati kriminaalvastutus võltsitud dokumentide omamise eest, selle alla kuulub ka teise isiku ehtsate dokumentide enda käes hoidmine ilma mõistliku põhjenduseta ja võltsitud dokumentide valmistamiseks loodud või kohandatud seadmete valdamine.

Identiteedi loomine baseerub biograafilisel ja biomeetrilisel[31] informatsioonil. Biograafiline info on põhiliselt isiku sotsiaalne jalajälg, kus identiteedi loomisel tehakse päringud erinevatesse allikatesse nagu elektri- ja gaasivarustuse firmad, pangad, aga ka Facebook, Twitter, LinkedIn jt. Biomeetrilise passi taotlemisel hõivatakse lisaks ka sõrmejäljekujutisi, mis toimub Suurbritannia postiteenistuse büroodes. Passi taotlemisel esitatakse samuti sotsiaalset identiteeti kinnitav info, lisaks on vaja veel, et ka mõnes ametis olev isik formaalselt kinnitaks, et ta on subjekti üle kahe aasta tundnud või oleks mõni ametiisik. Sellist varianti kasutab ka nt Validate UK, kus tuleb oma isikuandmeid[32] sisaldavale avaldusele lisada tunnistaja[33] poolt kinnitatud kaks fotot. Dokumentide taotlemisel GOV.UK Verify kaudu on tunnistaja kinnitus üldjuhul nõutav. Passi taotlemise menetlusse kuulub ka isikuintervjuu, kus isiku identiteeti süvitsi kontrollitakse.

Aitamaks riiklikele teenustele üle võrgu ligipääsu, on valitsuse digiteenuste (ingl. *Government Digital Service*) loodud GOV.UK Verify teenus, mis käivitati 2016. aasta mais.

GOV.UK Verify teenust pakub erafirmade liit, see kasutab identiteedi kinnitamiseks kommertsiaalselt ja avalikult kättesaadavaid allikaid. Valitsus on andnud neile ligipääsu passi- ja juhiloasüsteemidele, et aidata neid nende dokumentide ehtsuse kinnitamisel. Selleks polnud vaja mingeid täiendavaid õigusakte vastu võtta.

Selle kaudu saab ligipääsu kolmeteistkümnele[34] (13) riiklikule teenusele ja kasutaja identiteedi kinnitamine on pandud eraõiguslikele sertifitseeritud firmadele[35]:

---

[31] ei kasutata nt GOV.UK Verify ja Validate UK poolt, need kasutavad sotsiaalse identiteedi põhist identiteediloomet

[32] nimi, aadress, sünnikuupäev, meiliaadress ja telefoninumber

[33] aktsepteeritavate ametikohtade loetelu on kättesaadav: https://validateuk.co.uk/official-UK-ID-Card/acceptable-referees

[34] 2016. aasta 25. aprilliseisuga. Osa nendest teenustest on avalikus beetatestimises ja uusi teenuseid on ka lisandumas. (https://identityassurance.blog.gov.uk/2016/05/25/government-services-using-gov-uk-verify-may-2016-update/)

[35] materjal Internetist (https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify) andmetel, mis on avaldatud 2014. aasta 17. septembril.

- Barclays;
- CitizenSafe;
- Digidentity;
- Experian;
- Post Office;
- Royal Mail; ja
- SecureIdentity.

GOV.UK Verify hub (mis teeb võimalikuks ühenduse kasutaja, sertifitseeritud firma ja GOV.UK teenuse vahel) aitab kasutajatel valida sertifitseeritud firma, mis suurima tõenäosusega on võimeline nende identiteeti kinnitama. Kasutavad selleks "*Open Identity Exchange*". Mõned neist sertifitseeritud firmadest on nüüd suutelised kinnitama ka selliste kasutajate identiteeti, kellel pole Suurbritannia passi ega juhiluba. Paljud inimesed suudavad end avaliku sektori teenustele täisdigitaalselt identifitseerida umbes 10 minuti jooksul.

GOV.UK kasutab erinevaid tegevusajaloo allikaid selleks, et teha kindlaks kes inimesed on, kui nad seda väidavad. Identiteedi kontrollimisel on viis erinevat elementi ja valitud sertifitseeritud firma peab igas neist saavutama teatava lävendi enne, kui nad kasutaja identiteeti kinnitada saavad. Kasutaja valitud sertifitseeritud firma küsib esmakordsel registreerimisel teatavat infot ja viib läbi mõned kontrollid, et teataval tagatistasemel[36] väita, et kasutaja on see, kes ta väidab end olevat. Kui see kord on läbi tehtud, annab sertifitseeritud firma kasutajale kinnituse, mida saab kasutada avalikele teenustele ligipääsuks.

- Element A – hõivata tõendid, et identiteet eksisteerib. Tõenditel on kolm kategooriat – kodakondsus, raha ja elamine.
- Element B – tõendite valideerimine. Sertifitseeritud firma peab kindlaks tegema, et pakutud identiteet on kehtiv, ehtne või mõlemat, sõltuvalt nõutavast tagatistasemest.
- Element C – isiku ja identiteedi vahelise seose kehtestamine. Üks tavaliselt kasutatav meetod hõlmab isikult küsimuste küsimist, millele tõenäoliselt ainult tema oskab vastata. Need võivad käia info kohta, mis on ainult sertifitseeritud firmal olemas, või ka mõnelt teiselt teenusepakkujalt või krediidiinfo agentuurilt saadud.
- Element D – pettustevastane ristkontroll. Sertifitseeritud firma peab kindlaks tegema, et identiteet pole teadaolevalt ega tõenäoliselt võltsitud või varastatud.
- Element E – tegevusajalugu. Sertifitseeritud firma peab kindlaks tegema, et identiteet on olnud teatava ajavahemiku jooksul aktiivne.

Teiste Euroopa Liidu liikmesriikide ja mitte-liikmesriikide identiteetide tuvastamine toimub nende riikide poolt välja antud dokumentide alusel.

Elektroonilise identiteedina saab käsitleda ainult GOV.UK. Verify teenust, mis pakub riiklike digitaalteenuste kasutamisel lihtsat digitaalset viisi oma identiteeti tõendada. See kasutab olemasolevat infot ning siin puudub keskne identiteedi andmebaas, Suurbritannia kodanikele ei anta välja ka ID-kaarte.

GOV.UK Verify põhineb avalikult publitseeritud standarditel ning hea praktika juhistel (*Good Practice Guides (GPG's)*), mis on välja töötatud koos ministeeriumitega (*Governmental*

[36] eIDAS mõiste "Level of Assurance" tõlge eesti keelde

Departments), Riikliku Tehnilise Infoturbeameti (*The National Technical Authority for Information Assurance*) ja tööstuspartneritega. Siseministeerium on välja andnud juhised, mis pigem selgitavad standardeid, millele sertifitseeritud firma peab vastama ja kuidas nad neid nõudeid täita saavad, kui määratlevad tehnoloogiat või protsesse.

Valitsus on kehtestanud erinevad tagatistasemete standardid erinevate tehingute riskitasemete puhuks. Nõuded, mis tuleb mingite tagatistasemete saavutamiseks täita, on standardites kirjas. Iga ministeerium otsustab ise, milline tagatistase on nõutav tema teenuste kasutamiseks.

GOV.UK Verify pakub praegu identiteedi tagamist tasemel kaks, mis tähendab, et tõenäoliselt on kasutaja see, kes ta väidab end olevat. See annab kasutajatele identiteedikinnituse, mis on piisav vaikimisi enamiku digitaalsete teenuste kasutamiseks. Lähemalt on selgitatud, mida hõlmab kellegi esmakordne identiteedi kontrollimine sertifitseeritud firma poolt.

GOV.UK Verify teenus on kasutatav alates 20-aastaselt.

Enne GOV.UK Verify käikuminekut ei olnud kellelgi võimalik ainult veebis oma identiteeti tõendada 2. tagatistasemel, mida on vaja paljude keerulisemate või tundlike digitaalteenuste kasutamisel (ilma vajaduseta saata või saada asju posti teel või külastada isiklikult letiteenindust).

Neid standardeid saab rakendada ka väljaspool keskvalitsuse sfääri, näiteks kohalike omavalitsuste ja erasektori teenuste puhul nagu pangandus, mobiiltelefoni ja rahvusvahelise turismi valdkonnas. Näiteks 2. tagatistaseme identiteeditagatist võib kasutada, et täita pankade kohustusi "Tunne oma klienti"-nõuete rahuldamiseks.

Iga üksus annab igale isikule tavaliselt välja ainult ühe identiteedi isiku kohta. Suurbritannias ei liideta tavaliselt identiteete ja keskne identiteetide andmebaas puudub. Iga üksus haldab oma identiteetide andmebaasi ja infot vahetatakse juhtumipõhiselt.

2016. aasta augustis avaldas Suurbritannia Siseministeerium juhised nimevahetuseks ja järjekindla kogu ministeeriumit hõlmava lähenemise nimetaotluste menetlemiseks ametlikes dokumentides nagu Briti pass, siseministeeriumi reisidokumendid ja biomeetrilised elamisload. Kui isik otsib võimalust identiteeti vahetada, siis peab ta esitama selgitavad dokumendid, et seda identiteeti kasutatakse kõigil formaalsetel eesmärkidel.

Kui on vaja kaitsta isikuid kahju eest, on võimalik lubada ühel isikul kasutada mitut identiteeti kõigil kasutusjuhtudel. See hõlmab kaitsetuid kuritööohvreid (nt koduvägivalla ja jälitamise ohvrid) ja tunnistajaid. Kui kaitsetu ohver või tunnistaja soovib enda kaitseks oma nime muuta, peab tema taotlus olema toetatud asjaomase ametkonna poolt, nagu politsei, pagulasteenistus või mõni muu akrediteeritud organisatsioon. Nende üksikisikute kirjed on kaitse all ja iga infopäringut käsitlevad vastava ametkonna spetsialistid.

Kui nimevahetus toob kaasa passivahetuse, kus esitatakse nimevahetuse üksikasjad, säilitatakse info, mis seob isiku tema eelmise nimega, st täisnime nagu eesnimi, keskmine nimi/nimed ja perekonnanimi, et kindlustada seos varasema ja hilisema nime vahel. See info on vajalik, et vältida eelmise nimega deklareerimata passide käibelolekut. Põhjuseks on kuritegude ennetamine ja tuvastamine, kuna nimevahetust saab kasutada pettuse eesmärgil või avastamise vältimiseks, luues puhta identiteedi. Kodanikukaitse vaatepunktist vaadatuna aitab see tagada identiteedi tuvastamise piiriületusel ja kõrvaldab riskid, et isikud reisivad riikide vahel erinevate passidega.

Identiteedihaldusega tegelevad erafirmad, kes väljastavad kaarte, mille puhul on põhiliselt tegemist vanuse tõestamiseks mõeldud "dokumentidega". Siin on heaks näiteks VALIDATE UK - üks eraõiguslikke identiteedipakkujaid, nende poolt välja antud kaardid on ikkagi kasutaja vanuse tõestamiseks sobivad, ei rohkemat.

B

Üldine andmekaitseseadus on "Andmekaitse seadus 1998". Kasutajate isikuandmete kaitset elektroonilise side valdkonnas ja eraelu puutumatust reguleerib "Eraelu puutumatuse ja elektroonilise side (EÜ direktiivi) määrustik 2003". Määrus reguleerib elektroonilist otseturustust, küpsiste ja sarnaste tehnoloogiate kasutamist ning samuti andmetega seotud rikkumistest teavitamist. Teavitamise kohustus kohaldub vaid avalike elektrooniliste sideteenuste osutajate suhtes.

Reguleeritavatel organisatsioonidel finantsteenuste sektoris on eraldi kohustus korraldada oma äritegevust "piisava vilumuse, ettevaatuse ja hoolikusega" ning "mõistlikul viisil korraldada ja kontrollida [oma] asju vastutustundlikult ja tõhusalt rakendades riskijuhtimise süsteeme". Need nõuded toovad vastutavatele töötlejatele kaasa täiendavaid andmekaitse kohustusi finantsteenuste valdkonnas.

Isikuandmeid võib töödelda kui tüüptingimused on täidetud. Praktikas kasutatakse tihti andmetöötluse seaduslikkuse põhjendamiseks õigustatud huvide elluviimise tingimust. Andmekaitseseadus sisaldab erandeid teatud tüüpi andmete töötlemiseks. Nt seaduse enamikku sätteid ei rakendata, kui füüsiline isik töötleb isikuandmeid majapidamise eesmärkidel.

Delikaatseid isikuandmeid võib töödelda kui nende töötlemise tüüptingimused on täidetud. Täiendavad töötlemise tingimused on lisaks sätestatud andmekaitseseaduses ja selle juurde kuuluvas korralduses, sellisteks tingimusteks on nt juurdlus, uuringute läbiviimine, poliitiline tegevus.

Isikuandmeid ei tohi töödelda, kui vastutav töötleja ei teavitanud sellest AKAd või kui tegemist ei ole erandiga. Loa saamine ei ole vajalik. Teavitamine peab eelnema töötlemisega alustamisele.

Kõik vastutavad töötlejad peavad teavitama AKAd, va juhul, kui on täidetud üks vabastamise tingimustest:

- personalihaldus;
- vastutava töötleja äritegevuse reklaamimine ja turundus;
- töödeldakse vastutava töötleja enda või tema klientide/tarnija andmeid;
- töödeldakse teatud andmekategooriaid, mis on seotud mittetulundusühingutega; ja
- hallatakse avalikku registrit.

Volitatud töötleja peab töötlema isikuandmeid vastavalt kirjalikule lepingule, mis sisaldab volitatud töötleja tüüpkohustusi.

Andmekaitseseadus ei sisalda kohustust teavitama AKAd või andmesubjekte andmetega seotud rikkumistest. Kuid AKA avaldas suunise, kus ta soovitab informeerida teda tõsistest turvalisuse rikkumistest vabatahtlikult. Elektroonilise side sektoris tegutsevad ettevõtted peavad teavitama isikuandmetega seotud rikkumistest vastavalt "Eraelu puutumatuse ja elektroonilise side (EÜ direktiivi) määrustikule". Lisaks võivad teatud valdkondade teenuseosutajad (nt finantsteenuste osutajad) olla kohustatud teavitama oma valdkonna järelevalveasutust vastavatest rikkumistest.

Suurbritannia andmekaitseseadus kehtestab piiranguid piiriülesele andmeedastusele. Andmeid võib edastada, kui on täidetud piiriülese andmeedastuse tüüptingimused. Alternatiivina võib volitatud töötleja toetuda oma hinnangule, kas isikuandmetele tagatakse piisav kaitse peale nende edastamist väljapoole Euroopa majanduspiirkonda.

Piiriülene andmeedastus ega lepingu tüüptingimuste kasutamine ei nõua AKA teavitamist ega loa saamist.

Suurbritannia on kinnitanud siduvate ettevõtluseeskirjade kasutamist ning on liitunud siduvate ettevõtluseeskirjade vastastikuse tunnustamise süsteemiga.

3.12. Šveits

A

ID-kaardi ja passi väljaandmise õiguslik alus on „Šveitsi kodanike isikut tõendavate dokumentide[37] föderaalseadus“ ja „Šveitsi kodanike isikut tõendavate dokumentide määrus“. Muudatused nimetatud õigusaktidesse tehti föderaalpolitsei määrusega 2010. aasta 16. veebruarist, selle viimane redaktsioon on 2014. aasta 31. detsembrist.

Šveitsis antakse välja kahte tüüpi isikut tõendavaid dokumente – passe ja ID-kaarte. Neid koos taotledes saab tellimuse esitada kas Internetis või telefoni teel passibüroost. Kui isik soovib saada ainult ID-kaarti, siis saab seda sõltuvalt kantonist taotleda kas kohalikust omavalitsusest, kantoni passibüroost või Šveitsi välisesindusest.

Šveitsi e-passis, mida antakse välja alates 2010. aastast, on isikuandmed, näokujutis ning kiibis lisaks nendele ka digitaalallkiri ja kaks sõrmejälge.

ID-kaartide väljaandmiseks vajalikku registrit peab Šveitsi Föderaalpolitseiamet. Sellesse infosüsteemi võivad teha kandeid:

- Föderaalpolitseiamet;
- ID-kaardi väljaandja; ja
- väljastuskoha personal.

Oma põhikirjajärgsete ülesannete täitmiseks võivad ID-kaartide infosüsteemi poole pöörduda:

- Föderaalpolitseiamet;
- väljaandjad;
- piirivalve, ainult isikute tuvastamiseks;
- föderaal- ja kantonipolitseijaoskonnad, ainult isikute tuvastamiseks;
- selleks volitatud kantonipolitseijasokonnad kadunud isikute arvelevõtmiseks; ja
- selleks määratud föderaalpolitseijaoskonnad rahvusvaheliste identiteedipäringutele vastamiseks.

Identiteedi kontrolli õigsuse eest vastutavad kantonites paiknevad passibürood.

Interneti kaudu tellides täidab taotleja ekraanil talle esitatud lahtrid nime, eesnime(de), sünnikuupäeva, sünnikoha ja kodulinna nimega, aadressi ja võimalusel eelmis(t)e dokumendi (dokumentide) andmetega, edasine suhtlemine toimub elektronposti teel. Samas saab ka foto üles laadida. Elulisuse kontrolliks kasutatakse *Captcha*t. Taotlejale saadetakse aeg, millal tulla intervjuule ja kus teda informeeritakse täiendavate dokumentide esitamise vajadusest.

Nii ID-kaart kui pass kehtivad üldjuhul 10 aastat. Kiir-/hädaabipass kehtib kuni 12 kuud.

Šveitsi Föderaalpolitseil on muuhulgas järgmised kohustused:

- korraldab järelevalvet isikut tõendavate dokumentide väljaandmise üle – taotlejate isikute tuvastamine ja dokumentide korrektsus, väljaandjate vastavus protsessinõuetele;
- jälgib, et saladuste hoidmise ja andmekaitsenõuded oleksid täidetud, informatsioon ja juhised Šveitsi ID-kaardi kohta vastaksid sise- ja välisriikide organisatsioonide nõuetele;

[37] Siin tuleb tõlkida mõiste "Ausweis" kui isikut tõendav dokument, sest määrus hõlmab nii passe kui ID-kaarte

- jälgib, et saladuste hoidmise ja andmekaitsenõuded oleksid täidetud Šveitsi ID-kaartide taotlemisel ja nende väljastamisel;
- väljastab infot ja juhiseid väljaandmiskohtadele ja peatöövõtjatele ning jälgib nõuetele vastavust;
- jälgib isikut tõendavate dokumentide ülemaailmset arengut ning vastutab rahvusvaheliste standardite kasutuselevõtmise eest;
- haldab Šveitsi isikut tõendavate dokumentide jaoks avaliku võtme infrastruktuuri.

Šveitsis on sarnaselt Eestile erasektor, eriti aga mobiilifirmad, mänginud võtmerolli siseriikliku identiteedisüsteemi ja autentimistarkvara loomisel ning vabastanud digitaalse identiteedi potentsiaali majanduse jaoks, kasutades täies mahus olemasolevaid vahendeid ja äriprotsesse.

"*Trägerverein SuisseID*" loodi 2010. aasta 10. novembril. Assotsiatsiooni eesmärk on "*SuisseID*" juurutamine ja arendus. Asutajateks on Majanduse riigisekretäriaat (Majandusministeerium), Informaatika ja telekommunikatsiooni Föderaalamet BIT, QuoVadis Trust Link Switzerland AG, Swiss Post / SwissSign AG ja Swisscom (Switzerland AG).

"S*uisseID*" on Šveitsi turvalise autentimise ja elektroonilise allkirja standard. 2010. aastast alates on "*SuisseID*"-d kodanikele väljastatud neljast volitatud eraõiguslikust usalduskeskusest ja sel on nüüdseks riigi, st. föderaalpolitsei toetus. Tegemist on kahetegurilise autentimislahendusega, mis sobib *online* teenuste jaoks – elektrooniline identifitseerimine, autentimine ja allkirjastamine nii avalikus kui erakeskkonnas. "*SuisseID*" on Šveitsi kodanikele vabatahtlik ning lisandus riiklikule eID-kaardile. "*SuisseID*" on tasuline ja praegu väljastavad neid kaks ametlikku tarnijat – Quo Vadis Trustlink Schweiz AG ja Schweizerische Post/SwissSign AG.

"*SuisseID*" tootmine vastab "Šveitsi elektroonilise allkirja föderaalseadusele", "Elektroonilise allkirja valdkonna sertifitseerimisteenuste määrusele" ja "Raamatupidamisseadusele". Sertifikaadid on salvestatud krüptoprotsessorisse ja ligipääs võtmeoperatsioonidele on kaitstud PIN-koodiga. Pärast kolme korda vale PIN-i sisestamist protsessor blokeerub jäädavalt, PUK-koode ei kasutata.

2014. aasta kevadel toimus föderaalpolitsei eestvedamisel nõupidamine, kus arutluse all oli kolm võimalikku lahendust ja otsustati võtta kasutusele Eesti mudel. "*SuisseID*" on samuti unikaalse võtme funktsionaalsusega, kus ühe kaardiga saab sisse kõigisse süsteemiga liitunud teenustesse. Samuti on "*SuisseID*"-ga antud elektrooniline allkiri õiguslikult siduv nagu Eestiski. Erinevalt Eestist säilitatakse usaldusteenuse pakkuja juures laiendatud isikuandmete komplekti, milles sisalduvat informatsiooni kaardikasutaja nõusolekul automaatselt teenusepakkujale edastatakse. Krüpteerimisfunktsiooni "*SuisseID*"l ei ole.

Veel on erinevus Eestiga - kui Eestis on eraisikul eID funktsionaalsus kaardil ja firmade digitempel USB mälupulgal, siis Šveitsis seda vahet ei tehta ning "*SuisseID*" on saadaval mõlema jaoks nii kaardi kui mälupulga vormis.

Ülevaate "*SuisseID*"ga ligipääsetavatest teenustest leiab "*SuisseID*" koduleheküljelt[38].

B

Üldine andmekaitseseadus on "Šveitsi andmekaitse föderaalseadus". Seepärast on Euroopa Komisjon leidnud, et Šveits tagab andmekaitse piisava taseme (Euroopa Komisjoni otsus 2000/518/EC) ja ELi liikmesriigid võivad andmeid Šveitsiga vahetada. Praegu on otsus ülevaatamisel.

[38]http://suisseid.ch/de/anwendungen

Igas Šveitsi kantonis on olemas omad andmekaitsealased põhikirjad, mis puudutavad andmete töötlemist kantoni ametiasutustes. Šveitsi pangasaladus ja vastavad suunised mõjutavad andmekaitset panga kliendi andmete töötlemisel. Isikuandmete kaitset mõjutab ka Šveitsi kriminaalkoodeks, mis sisaldab saladuse hoidmise kohustust (nt patsiendi tervise andmete puhul).

Alates 2012. aasta 1. aprillist ei luba "Kõlvatu konkurentsi seaduse" uus säte helistada numbritele, mis on Šveitsi kataloogides tähistatud standardiseeritud telemarketingist loobumise deklaratsiooniga, va juhtudel, kui isik on ettevõtte klient või on muul viisil andnud nõusoleku reklaamisisuga e-mailide saamiseks.

Isikuandmeid võib töödelda kui see:

- ei riku andmesubjekti puutumatust; või
- rikub andmesubjekti puutumatust, kuid rikkumist õigustab andmesubjekti nõusolek, ülekaalukas ühiskondlik või isiklik huvi või Šveitsi seadusest tulenev seaduslik alus.

Andmekaitseseadus sisaldab mitteammendavat loetelu tingimustest, mis vastavad märkimisväärse avaliku huvi kriteeriumile, nt:

- andmesubjektiga lepingu sõlmimine/täitmine;
- konkurentide kohta info töötlemine; või
- andmete töötlemine mitteisiklikel eesmärkidel.

Kuigi andmekaitseseadus kasutab pisut erinevat sõnastust, siiski on isikuandmete põhimõtted sarnased tüüptingimustega ja andmeid võib töödelda, kui tüüptingimused on täidetud.

Delikaatseid isikuandmeid (ja isiklikke profiile) ei tohi avaldada kolmandatele isikutele, va juhul kui on täidetud üks kriteeriumitest, sh, kuid mitte ainult:

- andmesubjekti nõusolek;
- märkimisväärne avalik või isiklik huvi; või
- seaduslik alus.

Enamasti võib delikaatseid isikuandmeid töödelda kui on täidetud tüüptingimused.

Kui delikaatseid isikuandmeid või isiklikke profiile kogutakse (süstemaatiliselt), tuleb andmesubjekti sellest teavitada, ning taoliste andmete töötlemist tuleb registreerida AKAs.

Vastutavad töötlejad, kes töötlevad delikaatseid isikuandmeid või isiklikke profiile regulaarselt või avaldavad isikuandmeid kolmandatele isikutele regulaarselt peavad registreerima töötlemist AKAs. Registreering ei nõua AKA nõusolekut ning on teavitamise eesmärgil. Registreerimine peab toimuma enne töötlemisega alustamist ja on tasuta. Register on interneti kaudu avalik kättesaadav.

Registreerimine ei ole vajalik, kui:

- töötlemise kohustus tuleneb Šveitsi seadusest;
- asutus on määranud andmekaitse eest vastutavat isikut, kes kontrollib sõltumatult andmekaitsereeglite täitmist ja haldab andmetöötluse loetelu. Vastutav isik peab vastama andmekaitseseaduse nõuetele ja isiku määramisest tuleb teavitada AKAd;
- vastutaval töötlejal on sertifitseerimise käigus olemas andmekaitse kvaliteedimärgi ning teavitanud sellest AKAd;
- toimetatud andmeid avaldatakse perioodilises väljaandes ja ei avaldata neid kolmandatele isikutele ilma andmesubjekti nõusolekuta;
- isikuandmeid töötlevad ajakirjanikud, kes kasutavad andmeid ainult isiklikus töös; või

- kehtib üks täiendavatest eranditest (nt avalikud admekogumised, kliendi ja tarnija andmete, mis ei ole delikaatsed, töötlemine ja töötlemine raamatupidamislikel eesmärkidel).

Isikuandmete töötlemist võib volitada kui:

- vastutav töötleja tagab, et andmeid töödeldakse lubatud eesmärkidel ja määral; ja
- puudub seaduslik või lepinguline konfidentsiaalsuskohustus.

Vastutav töötleja peab tagama, et volitatud töötleja vastab üldistele turvanõuetele. Volitatud töötleja õigustatud huvide kinnitamiseks sõlmib vastutav töötleja temaga tavaliselt lepingut.

AKA ei kohusta teavitama andmetega seotud rikkumisest. Kuid põhinõue töödelda isikuandmeid heas usus võib eeldada andmesubjektide või kolmandate isikute teavitamise vajadust või muid meetmeid. Rikkumisest ei pea teavitama AKAd, kuid tõsiste rikkumiste korral soovitatakse AKAd teavitada. Teatud valdkondade teenuseosutajad võivad olla kohustatud teavitama oma valdkonna järelevalveasutust vastavatest rikkumistest.

Isikuandmete edastamine on lubatud riikidesse, kus on piisav andmekaitse tase (ELi liikmesriigid, Euroopa Majanduspiirkonna riigid; USA; riigid valges nimekirjas). Kui andmeid edastatakse riiki, kus ei ole tagatud andmete piisavat kaitset, peab olema täidetud üks eeldustest:

- on olemas rahvusvahelise andmeedastusleping või kasutusel on muud meetmed andmete kaitseks välismaal;
- kui andmeid edastatakse rahvusvahelise kontserni siseselt – piisavad lepingu tüüptingimused;
- on olemas andmesubjekti nõusolek;
- andmeedastus on vajalik andmesubjektiga sõlmitud lepingu täitmiseks;
- andmeedastus on vajalik vastavalt korrale oluliste riiklike ja avalike huvide kaitseks või on vajalik kohtuvaidluses;
- andmeedastus on vajalik andmesubjekti elu ja tervise kaitseks; või
- andmeedastus puudutab andmeid, mida andmesubjekt on ise avaldanud ja ei ole keelanud avalikult nende kasutamist.

Seega, riigis kehtivad piiriülese andmeedastuse tüüptingimused mõningate erinevustega (nt puudub nõue kasutada lepingu tüüptingimusi rahvusvahelistes andmeedastuslepingutes).

AKA on oma internetileheküljel avaldanud lihtsaid lepingu tüüptingimusi, mis on kohandatud Šveitsi seadusandluse jaoks; kuid enamikel juhtudel on lubatud kasutada ka keerulisemaid tüüptingimusi. Kuni "*Safe Harbor*" raamistiku tühistamiseni peeti seda ka piisavaks andmekaitsemeetmeks, kuigi AKA ei tunnistanud seda otseselt.

Vastutavad töötlejad peavad teavitama AKAd, kui nad kasutavad andmeedastuslepinguid, siduvaid ettevõtluseeskirju vm meetmeid edastatavate andmete kaitseks riigis, kuhu andmeid edastatakse. AKA loa saamise kohustus puudub. Siiski kommenteerib AKA tavaliselt 30 päeva jooksul, kas ta peab antud meetmeid piisavateks. Kui vastutavad töötlejad kasutavad AKA heakskiidetud meetmeid (milleks on praegu lepingu tüüptingimused, Šveitsi lepingu tüüptingimus, Euroopa komisjoni lepingu tüüptingimus ning kuni tühistamise hetkeni ka USA ja ELi vaheline Atlandi-üleseid andmevoogusid reguleerinud andmekaitseraamistiku "*Safe Harbor*" Šveitsi adapteeritud versioon).

Šveits aktsepteerib siduvate ettevõtluseeskirjade kasutamist. Spetsiifilised formaalsed nõuded sellele puuduvad. AKA loa saamine ei ole vajalik – ainult teavitamine.

3.13. Teema lühikokkuvõte

Identiteedihalduse strateegiad ei soovita ühtset või globaalselt täiesti interoperatiivset identiteedisüsteemi, vaid piirduvad teatud rahvusvahaliste standardite rakendamisega. Riikidel on erinevad reeglid identiteedi suhtes, mis tihti põhinevad traditsioonidel, mis on teatud ulatuses viidud kooskõlasse moodsa tehnoloogiaga, aga siiski põhinevad varasematel kultuurilistel ja ajaloolistel alustel. Oluline on **piisav rahvusvaheline tehniline interoperatiivsus**, et saaks dokumente piiriüleselt kasutada. See vajadus kasvab, kuna inimesed liiguvad rohkem üle piiride.

Teatud regionaalsetel projektidel (näiteks EU STORK) on (oli) eesmärgiks tihedam koostöö ja/või rohkem ühtlustatud reeglid. Elektrooniline kaubandus ja e-valitsemine on toonud kaasa vajaduse enam ühtlustada identiteediga seotud küsimusi, kuna rohkem isikuid võivad eri viisil puutuda kokku teiste riikide reeglite ja süsteemidega – seda ka füüsiliselt teises riigis viibimata.

2014. aastal vastu võetud eIDAS määrus muudab mitmed e-identiteedi ja digitaalallkirja kasutamisega seotud reeglid liikmesriikide vahel ühtlasemaks. See loob ühise aluse turvalisele elektroonilisele suhtlusele kodanike, ettevõtjate ja ametiasutuste vahel, suurendades sellega avaliku ja erasektori internetipõhiste teenuste, e-äri ja e-kaubanduse tõhusust liidus.

Samas võib välja tuua uue paralleelse suundumise – riigid kehtestavad identiteedihaldamise kohta eriseadusi. Seni valitsenud tava, et ühtset reguleerimist ei ole vaja ja piisab eriseadustes sätestatust, on ajale jalgu jäänud.

Mitmetasemeliste identiteetide kasutamist ja seaduslike topeltidentiteetide uuritud riikidest ei selgunud. Saksamaa võimaldab ka lavanime ja pseudonüümi kasutavaid identiteete, mis on seotud põhiidentiteediga. Ka anti vastustega vähe infot biomeetria kasutamise kohta, kuigi väljasaadetud küsimustikes oli biomeetria eraldi ära mainitud.

Andmekaitse on ELi õiguses olnud kogu aeg oluline, aga detailides on liikmesriigid rakendanud Andmekaitsedirektiivi eeskirju erinevalt. See on üks põhjuseid, miks andmekaitse on ELis hetkel killustatud ja ebaühtlane. See olukord peaks muutuma alates 2018. aastast, kui jõustub ELi uus andmekaitsemäärus nr 2016/679.

Kuigi andmekaitse reeglite üksikasjad erinevad eri liikmesriigiti, saab ühise joonena välja tuua selle, et igas riigis on olemas AKA – sõltumatu riiklik andmekaitseasutus, mis tegeleb nii järelevalvega *ex officio* kui ka kaebustega. Samuti jaotatakse kõigis riikides isikuandmeid delikaatseteks ja mittedelikaatseteks. Biomeetrilise info töötlemist loetakse delikaatsete isikuandmete töötlemiseks ning sellise töötlemise suhtes rakendatakse rangemaid reegleid.

Erinev on järelevalve tase isikuandmete töötlemise üle andmekaitseasutuste töös. Rangema andmekaitsepoliitikaga riikides on olnud juhtumeid, kus suured rahvusvahelised ettevõtted on saanud tõsiseid trahve andmekaitseseaduse rikkumise eest[39] ja suured tarkvaraettevõtted nagu Google või WhatsApp pidid isegi muutma oma tarkvara, et jätkata tegutsemist antud riigi turul[40].

Delikaatsete, sh biomeetriliste isikuandmete töötlemine avaliku sektori menetlustes on enamasti keelatud, välja arvatud juhul kui töötlemine on vajalik seadusest tuleneva kohustuse täitmiseks, nt

[39]Nt Lidl kontsern sai Saksamaal 2009. aastal 1,5 mln eurose trahvi Saksamaa poodides salajaste kaamerate kasutamise eest: https://iapp.org/media/pdf/publications/July-Aug09_Advisor.pdf. Hollandi regulatsioon näeb andmekaitse reeglite rikkumise eest trahvi suuruses kuni 810, 000 eurot või 10% firma aastakäibest

[40] Vt nt https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-whatsapp-non-users-better-protected või https://autoriteitpersoonsgegevens.nl/en/news/privacy-campaign-google-following-possible-sanction-dutch-dpa

biomeetriliste isikut tõendavate dokumentide väljaandmiseks. Andmetöötluse eesmärk peab olema selgelt defineeritud ja töötlemine on lubatud ainult defineeritud eesmärgil. Delikaatsete, sh biomeetriliste andmete töötlemist reguleerivad reeglid on väga piiravad. Nt Rootsis ja Saksamaal eemaldatakse biomeetrilise dokumendi jaoks hõivatud sõrmejäljed kõikidest andmebaasidest kohe pärast dokumendi isikustamist. Teatud riikides, sh Eestis, biomeetrilisi andmeid, sh sõrmejälgi, ristkasutatakse erinevates avaliku sektori menetlustes väga harvadel juhtudel ja rangelt määratletud protseduuride puhul – nt mõnes kriminaalmenetluses ja isikut tõendava dokumendi taotleja isikusamasuse kontrollimiseks.

Erasektoris toimuva biomeetriliste andmete kogumise ja töötlemise kohta eraldi regulatsioone enamasti ei ole, kõigi suhtes kehtivad samad seadused. Siin rakendatakse põhilisi reegleid – kuna andmesubjekt on andmete omanik, siis on vajalik sellise andmetöötluse jaoks tema luba. Samuti peab andmetöötluse eesmärk olema selgelt defineeritud.

Enamasti tohib isikuandmeid edastada kolmandatesse riikidesse, kus on tagatud andmekaitse piisav tase. Võimaldamaks isikuandmete edastamist riikidesse kus ei ole tagatud piisavat andmekaitset, ja samal ajal kaitsmaks edastatavaid isikuandmeid, on enamik riike kinnitanud ettevõtetele nn lepingu tüüptingimusi – andmeedastuslepinguid isikuandmete vastutava ja vastutava töötleja vahel, mille alusel ebapiisava andmekaitse tasemega välisriigis asuv andmete vastuvõtja tagab, et täidab Andmekaitsedirektiivis kehtestatud isikuandmete kaitse nõudeid.

Enamik riike on kinnitanud ettevõtetele ka siduvaid ettevõtluseeskirju, mis võimaldavad kaitsta isikuandmeid, kui need edastatakse rahvusvahelise kontserni siseselt. Siduvate ettevõtluseeskirjade kasutamine ei tulene seadusest – kontsernid koostavad ja järgivad neid vabatahtlikult, tagamaks isikuandmete nõuetekohast kaitset andmete edastamisel oma äriühingute vahel, mis kuuluvad samasse kontserni ja mis on omavahel seotud asjaomaste eeskirjadega.

2016. aastal vastu võetud isikuandmete kaitse üldmäärus tugevdab ja ühtlustab isikuandmete töötlemise ja andmekaitse reegleid EL-is ning reguleerib isikuandmete edastamist väljapoole ELi. Kuna määrus sai vastu võetud 2016. aasta mais, siis uuringu tulemusena ilmnes, et valdavas osas on riigid hakanud planeerima üleminekut, kuid detailne arusaam kaasnevatest muudatustest ei ole veel selge. Siiski on üksikud riigid üles näidanud edusamme ja on võtnud osa sätetest ennetähtaegselt üle. Näiteks sisaldavad mõne riigi regulatsioonid kohustust teavitada AKAd ja/või võimalikke ohvreid andmetega seotud rikkumisest. Suurbritannia AKA aga avaldas suunise, kus ta soovitab töötlejatele informeerida AKAd tõsistest turvalisuse rikkumistest vabatahtlikult, kuna andmekaitseseadus ei sisalda seda kohustust.

4. Euroopa kohtute praktika: näited teemakohastest kohtulahenditest

Näited on toodud eriti kohtupraktikatest, peamiselt seoses Euroopa Liidu (EL) määrusega (EÜ) nr 2252/2004 biomeetriliste passide kohta. Kuna nii ELi andmekaitse kui ka elektroonilise identiteedi reeglistik on hiljuti muudetud ja uute määruste rakendusperiood veel kestab, ei ole nende määruste suhtes huvitavaid kohtulahendeid. Määrust 2252/2004 puudutavad kohtuotsused on kahte eri tüüpi: liikmesriikide kohustuste täitmise kohta ning eelotsused, milles liikmesriikide kohtud küsivad Euroopa Liidu kohtult ELi õigusaktide tõlgenduse kohta. Eriti eelotsused on huvitavad õigusaktide sisu paremaks põhimõtteliseks arusaamiseks.

Lühidalt selgitades ühte liikmesriikide vastast kohtuotsust võib nimetada kaasust C-139/13 *Komisjon versus Belgia* liikmesriigi väidetavate kohustuste rikkumise kohta väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite suhtes. Küsimus oli riigi poolt sõrmejälgede kasutuselevõtu nõude täitmata jätmine. Selles ja sarnastes kohtuasjades on tegemist sellega, kas riik on tähtaja jooksul täitnud kohustusi või on neil õigustatud põhjusi seda mitte teha. Määruses sätestatud standardid on kohustuslikud ja liikmesriikidel on ainult võimalik selles ulatuses, mida määrus ise lubab, otsustada kuidas neid nõudeid täita.

Privaatsusega tegelevad kaasused vaatavad kas piirangud inimõigustes (nagu näiteks privaatsuses) on tehtud õigustatud eesmärkidel, proportsionaalselt ja seaduse alusel. Neid kriteeriume on loonud Euroopa Inimõiguste Kohus ja ka EL rakendab samu põhimõtteid. Antud juhtumites on tegemist küsimusega kas nõue määruses 2252/2004 anda biomeetrilisi andmeid on ebaproportsionaalne privaatsuse piirang. Isikute privaatsust käsitlevate kaasuste hulgast võib nimetada liidetud kohtuasju C-446/12-C-449/12 *W. P. Willems jt versus Burgemeester van Nuth jt*, mis käsitleb kohustust anda biomeetrilisi andmeid, eelkõige sõrmejälgi. Küsimuse all oli ka kogutud andmete kasutamine muul eesmärgil kui passide ja reisidokumentide väljastamiseks, biomeetrilisi andmeid sisaldavate andmebaaside loomine ja kasutamine ning selle seadusega tagatus. Lisaks määrusele oli õiguslik alus EL põhiõiguste harta artiklid 7 ja 8 (privaatsuse ning isikuandmete kaitse) ning Direktiiv 95/46/EÜ andmekaitse kohta.

Willems jt. Hollandi kodanikud keeldusid andmast sõrmejälgi ja ei saanud sellepärast passe ega muid isikudokumente. Nad olid mures, et nende andmeid hoitakse ebaturvaliselt ja et on ebaselge, kas neid saaks ka muudel eesmärkidel (kui reisidokumendi jaoks) kasutada. Hollandi kohtul oli eelotsuseks kaks küsimust. Esiteks: kas määrus kehtib ka teatud isikut tõendavate dokumentide suhtes mis ei ole passid, aga mida saab teatud määral kasutada reisidokumentidena. Vastus oli, et määrus ei tegele sääraste dokumentidega (mis tähendab, et liikmesriigid otsustavad ise niisuguste dokumentide kohta). Teiseks oli küsimus, kuidas tõlgendada andmekaitse reegleid biomeetriliste andmete muu kasutuse suhtes, kui neid oli algselt kogutud passide jaoks. Euroopa Kohus vastas, et määruse sisuks on määruses ettenähtud eesmärkidel (st reisidokumentide jaoks) kogutud andmed ja andmed, mida muudel eesmärkidel kogutakse või kasutatakse, reguleeritakse liikmesriikide seadustega[41]. See tähendab, et määrus ei piira neid eesmärke, millel liikmesriigid võivad koguda biomeetrilisi andmeid, vaid sätestab ainult reegleid teatud spetsiifilise olukorra jaoks. Siseriiklik seadus või ka Euroopa Inimõiguste Konventsioon võivad piirata andmete kogumist ja kasutamist.

Kohtuasjas C-291/12 *Michael Schwarz versus Stadt Bochum* leidis kohus, et määrus oli kehtiv kahest eri vaatevinklist. Sellel on õiguslik alus, kuna EL võib võtta vastu õigusakte piirikontrolli suhtes, ning

[41]Madalamaade biomeetriliste andmete andmebaasi toimimine peatati 2011. aastal, kuna ei saanud selle turvalisust privaatsuse vaatevinklist ning biomeetriliste tehnoloogia usaldusväärsust tagada.

privaatsuse piirangud on proportsionaalsed, kuna on oluline kindlaks teha passi omanike identiteeti ning seega passide kehtivust.

Võib tsiteerida (lõiku 43), kus kohus mainib: „Selles osas tuleb siiski nentida, et see, et nimetatud meetod ei ole täielikult usaldusväärne, ei ole otsustav. Nimelt ühelt poolt, isegi kui see meetod ei välista täielikult luba mitteomavate isikute aktsepteerimist, piisab sellest, kui see vähendab märkimisväärselt niisuguste aktsepteerimiste riski, mis esineks siis, kui seda meetodit ei kasutataks." Teiste sõnadega: ei saa nõuda, et meetod koguda või säilitada andmeid oleks täiuslikult usaldusväärne, kuna säärane nõue oleks ebareaalne, aga kui tase on piisav ja see kasu, mida teatud andmete kogumisest saadakse on küllalt suur, siis see kaalub üles võimalikud negatiivsed küljed. Seda võib ka nii tõlgendada, et kohus oletab, et seadusandja on määrust vastu võttes kaalunud olulisi aspekte privaatsuse ja andmekaitse suhtes, ning kohus pigem kontrollib proportsionaalsust ning et protsess on olnud korrektne, kui alustab otsast peale biomeetriliste andmete kogumise adekvaatsuse hindamisega.

Kohtuotsused pigem näitavad, et õiguslik olukord biomeetriliste andmete kogumise ja kasutamise suhtes Euroopa Liidus ei ole veel selge[42]. Määruse 2252/2004 nõuded reisidokumentide suhtes on õigustatud, aga see määrus ei anna vastuseid laiemalt biomeetriliste andmete suhtes. Kohus on ka (eriti kaasuses Williams) tõlgendanud määruse sisu ja selle kaudu ka enda kompetentsi kui väga kitsast.

Euroopa Inimõiguste Kohus on ka tegelenud biomeetriliste (ja geneetiliste) andmetega. Juba 2008. aastal otsuses *S. and Marper versus UK.* Küsimuse all oli kui tundlikud on DNA profiilid ja muu biomeetriline ja geneetiline teave ning kas sääraste andmete kogumine ja hoidmine riivab privaatsust ka siis, kui neid andmeid ei kasutata. Inimõiguste kohus küll nõustus väitega, et võitlus kuritegevuse ja eriti organiseeritud kuritegevuse ja terrorismi vastu on tänapäeva Euroopa riikide üks suurimaid väljakutseid ja et nüüdisaegne tehnika saab olla suureks abiks selles võitluses. Samas on just kiire tehniline areng säärane, et on võimalik, et edaspidi kasutatakse andmeid viisidel või eesmärkidel, mida tänapäeval ei saa aimata. Just sellepärast peab rangelt vaatama andmete kogumise proportsionaalsust ja vajalikkust. Isegi kui tänapäeval neid andmeid ei kasutata siis nende kogumine võib igal juhul riivata privaatsust.

Veidi teine järeldus tehti kaasuses *Christine Goodwin versus UK* (2002), mis küll ei tegelenud biomeetriaga, aga mille tulemust saaks sarnaselt kasutada biomeetriliste andmete kohta. Kohus leidis et asjaolu, et Christine Goodwin muutis sugu sünnitunnistuses pärast soomuudatuse operatsiooni oli vajalik ja proportsionaalne. Puudusid põhjused seda keelata ja kui ei oleks olnud võimalik muudatusi teha, oleks see toonud kaasa isikule ebamugavusi ja raskusi.

[42]ELi kohtupraktikast on huvitav ära märkida, et kohus on teadlik ja aktsepteerib, et biomeetrilised meetodid ei pea olema täiuslikud. See aga ei tähenda, et neid ei saa kasutada, kui kaitse on piisav ja/või tuvastamise vea tõenäosus on väike. Oluline on proportsionaalsus – mis riskid on ja mis eelised on teatud tehnoloogia kasutamisel? Kui see vahekord on sobiv, saab kasutada uusi meetodeid isikuandmete kogumiseks, vahetamiseks ja säilitamiseks.

5. Kokkuvõtvaid märkusi ja soovitusi

Kokkuvõtvad märkused ja soovitused (kommentaar ja sellele vastav soovitus) on koostatud – tuginedes varem kogutud informatsioonile – ajurünnaku käigus ja selle koostamisel ei ole kasutatud eraldi metoodikat. Osa kommentaare ja soovitusi on mõeldud abiks identiteedihalduse strateegia struktuuri või teemade kindlaksmääramisel. Kommentaarid ja soovitused on toodud sellises järjekorras, nagu nad teema loogilisel käsitlemisel üles kerkisid.[43]

Antud soovitusi saab kasutada sisendiks detailanalüüsile, mis käsitleks iga analüüsitava riigi menetlusakte ja õigusaktide tõlgendamist ja praktilist rakendamist ning annaks soovitusi rakendusaktide kehtestamiseks Eesti Vabariigis.

1. Eesti e-riigi eduloo üks nurgakive on tugev tsentraliseeritud identiteedihaldus. Eesti on üles ehitanud usaldusväärse identiteedihalduse, millele tuginevad identiteediskeemid (eID, mID). Riigi poolt välja arendatud identiteedihaldus, mille tehnilised lahendused on välja arendatud koostöös erasektoriga, on majanduslikult efektiivne kogu ühiskonnale.
   Soovitus: Jätkata Eestis seni edu garanteerinud tsentraliseeritud identiteedihalduse mudeliga.

2. Järjest rohkem riike, sh Eesti, on võtnud kasutusele mudeli, kus isikuandmete põhikomplekti haldaja ning vastutav andmete kvaliteedi ja aktuaalsuse eest on rahvastikuregister (registri nimi võib olla erinev).
   Soovitus: Jätkata Eestis identiteedihalduse mudeliga, kus rahvastikuregister on isikuandmete põhikomplekti haldaja ning andmete kvaliteedi ja aktuaalsuse eest vastutaja.

3. Nüüdisaegseid edukaid identiteedihalduse mudeleid iseloomustab usaldusväärsete tehnoloogiate kasutamine. Valdavalt kasutatakse avaliku võtme infrastruktuuril põhinevaid identiteediskeeme[44]. Euroopas on sellisteks riikideks lisaks Eestile näiteks Belgia, Portugal, Soome, Taani, Šveits, Austria jt.
   Soovitus: Jätkata Eestis PKI-l või teistel usaldusväärsetel tehnoloogiatel tuginevate identiteediskeemide kasutamist.

4. Avaliku võtme infrastruktuuril põhinevad identiteediskeemid jagunevad kaheks, erinedes selle poolest kuidas privaatvõtmeid hoitakse. Detsentraliseeritud skeemi puhul on privaatvõti tema omaniku täieliku kontrolli all ja ta ise vastutab selle turvalise hoidmise eest. Selline mudel on kasutusel Eestis (privaatvõti on kas isikutunnistuse kiibis või SIM-kaardil). Näiteks Taanis ja Austrias on tegemist tsentraalse privaatvõtmete haldusega, kus tsentraalne teenuseosutaja vastutab privaatvõtmete hoidmise eest.
   Soovitus: Jätkata Eestis detsentraliseeritud privaatvõtme haldust sisaldavate identiteediskeemide kasutamist, mille puhul täielik kontroll ja vastutus privaatvõtme hoidmise üle on inimese enda käes.

---

[43] E-Riigi Akadeemia poolt SMi tellimusel 2013. aastal läbi viidud uuringus "ID-1 formaadis dokumentide funktsionaalsuse uuring" on samuti tehtud mitmeid identiteedihaldusega seotud ettepanekuid, mida käesolevas uuringus korratud ei ole, v.a juhul, kui samalaadne ettepanek uuringu läbi viimise käigus uuesti esile kerkis.

[44] Järjest rohkem viiakse läbi uuringuid blockchain'i võimaliku kasutamise kohta paljudes valdkondades. e-Riigi Akadeemia on 2014. aastal läbi viinud uuringu „Krüptoraha – võimalused, ohud, riskid".

5. Identiteedihalduses on edukad riigid, kus on kasutusel (inimestele omistatud) unikaalne tunnus, mida näiteks Eestis nimetatakse isikukoodiks. Saab välja tuua otsese seose infoühiskonna taseme ja unikaalse tunnuse kasutamise vahel. Unikaalne tunnus on vajalik isikuga seotud teiste tunnuste sidumiseks ning e-teenuste osutamiseks vajaliku andmete ristkasutuse ja andmevahetuse automatiseerimise jaoks. Näiteks ei ole Suurbritannia ja Saksamaa võtnud kasutusele unikaalset tunnust, mille tõttu nendes riikides puudub riigi tasemel ühtne (usaldusväärne) identiteedihaldus ja infoühiskond kui selline. Osades riikides on unikaalne tunnus küll kasutusele võetud, aga selle kasutamist piiratakse seadusega, mistõttu seda ei saa kasutada laiemapõhjaliseks e-riigi arendamiseks. Põhiline diskussioon on praegu maailmas suunatud unikaalse tunnuse vormile: kas see peaks/võiks omada tähendust nagu Eesti isikukood näitab inimese sugu ja sünniaega. Riikides, kus numbrilise ja/või tähendusliku unikaalse tunnuse kasutamine ei ole leidnud toetust, omistatakse inimestele juhuvalikuga moodustatud unikaalseid tunnuseid.
   Soovitus: Jätkata Eestis unikaalse tunnuse – isikukoodi – kasutamist senisel viisil.

6. Euroopa Liitu sisserände suurenemisel võib juhtuda, et residentsuse taotlejate ehk võimalike isikukoodide saajate hulgas on sama sünnipäevaga isikuid rohkem kui ühe päeva kohta isikukoode välja saab anda. Näiteks panevad Lähis-Ida riikidest, kus rahvastikuregistri pidamine pole veel väga arenenud, pärit inimesed oma sünnipäevaks sageli rahvuslikke tähtpäevi (nt 21. märts, sest sel kuupäeval tähistatakse nii Afganistanis kui Iraanis Pärsia uut aastat). Nii juhtus Rootsis, kus maksuamet oli sunnitud kasutusele võtma 2561 libasünnipäeva[45].
   Soovitus: Viia läbi riskianalüüs ja töötada välja varuvariant olukorraks, kus isikukoodid ühe päeva lõikes võivad „otsa saada“.

7. E-residentsus, mis on e-riigi maine seisukohalt Eestile suurt tunnustust toonud, on seadnud Eesti identiteedihalduse tugevuse küsimärgi alla. Sisuliselt oleme sisse toonud Suurbritannia või Saksamaa mudeli, kus välisriikide kodanikke tuvastatakse põhiliselt reisidokumendi alusel. Reisidokumentide usaldusväärsuse hindamiseks vajalikud teadmised klienditeenindajatel puuduvad.
   Soovitus: Tugeva identiteedihalduse tagamiseks ja abiks klienditeenindajatele tuleks taastada reisidokumentide hindamise keskus.

8. Näiteks on Portugali isikutunnistusel kasutusel *Match-on-Card (MoC)* tehnoloogia[46]. Ka passides ehk reisidokumentides olevat näo- ja sõrmejäljekujutisi saab kasutada ainult võrdluseks inimese

---

[45]Postimees (7.04.2016) „Rootsis said isikukoodid otsa“. http://maailm.postimees.ee/3647037/rootsis-said-isikukoodid-otsa, 2.10.2016

[46] Sõrmejälgede biomeetria valdkonnas on laialdast levikut leidnud *Match-on-Card* (MoC) kontseptsioon. MoC on sõrmejälgede kaartidel hoidmise ja võrdlemise kontseptsioon, mis tõendab kaardiomaniku füüsilist kohalolekut ja tagab selle abil turvalise isikutuvastuse. MoC on mitmete riikide rahvuslikel isikutunnistustel kasutusele võetud. MoC kasutusele võtmise tagajärjel hoiab USA Riigidepartemang aastas ühe kasutaja kohta kokku 200 USD, kuna enam ei ole vaja käigus hoida salasõnade haldamise, sh uuendamise süsteemi, sest 30% kasutajatoe mahust oli salasõnadega seotud abi (http://www.matchoncard.com/references/case-studies/employee-id.).

MoC tehnoloogia kasutamise poolt räägivad järgmised asjaolud: 1. MoC võimaldab spetsiaalse lugeja vahendusel tuvastada kaardiomaniku füüsilist kohalolekut ja tagab isiku tõsimeelset tuvastamist, mille kaudu a) väheneb identiteedivarguste ja -pettuste hulk; b) suureneb turvalisus; c) tekitatakse jälg ja auditeeritavus; d) suureneb

endaga. Vastavalt Nõukogu määrusele 2252/2004 kasutatakse biomeetrilisi tunnuseid passides ja reisidokumentides üksnes dokumendi ehtsuse kontrollimiseks ja kasutaja isikusamasuse kontrollimiseks otseselt kättesaadavate võrreldavate tunnuse abil kui passi või muu reisidokumendi esitamine on seadusega nõutav.
Soovitus: Kaaluda *Match-on-Card* lahenduse kasutamist järgmise põlvkonna isikutunnistustel.

9. Sõrmejälgi saab kasutada kahel moel: sõrmejälgedena ja mallina. Viimast meetodit on vaja vähem kaitsta, sest mallist ei saa n-ö tagasi sõrmejälge tekitada. ISO standarditega on malli tegemise algoritmid kindlaks määratud. Väära aktsepteerimise ja väära tõrjumise taseme viga ükskõik millise biomeetrilise tunnuse üksikult kasutamisel on oluliselt suurem kui unikaalse tunnuse kasutamise puhul, seepärast on vaja identifitseerimisel kasutada informatsiooni liiasuse põhimõtet.
Soovitus: Otseste biomeetriliste andmete kasutamisele eelistada alati biomeetriliste andmete malli kasutamist.

10. Identiteedihalduse organisatoorne korraldus on riikides üldjuhul lihtsalt välja kujunenud ja kajastub osadena mitmetes õigusaktides. Eestis vastutab SM rahvastiku arvestuse ja isikut tõendavate dokumentide sh digitaalsete dokumentide poliitika eest. RIA (MKMi alluvuses) vastutab kokkuleppeliselt elektroonilise dokumendi kandja ning dokumendikeskkonna kasutatavuse ja turvalisuse eest. MKM vastutab eIDAS[47] rakendamise sh usaldusteenuste osutamise eest. Riigi koostööpartneriteks on Swedbank, SEB, Telia, Sertifitseerimiskeskus, TRÜB Baltic jne. Registreerimisasutus on PPA ning sertifitseerimisteenust osutab SK.
Soovitus: Kirjeldada Eestis väljakujunenud identiteedihalduse alane tööjaotus ühes dokumendis.

11. Isikutuvastamine ei ole riikides üldjuhul seaduse tasandil reguleeritud ja kasutusel olev semantika on väga erinev. Ka Eestis ei ole isikutuvastamise põhimõtted hierarhiliselt reguleeritud.
Soovitus: Reguleerida isikutuvastamise üldpõhimõtted seaduse ja alamate õigusaktide süsteemina. Koostada isikutuvastamise head tavad. Koostada identiteedihalduse seletav sõnaraamat (eesti-inglise-vene ehk menetlustes kasutatavates keeltes, täiendada *Google translate* keskkonda).

---

kuluefektiivsus; e) säilitatakse kasutaja privaatsust; f) suureneb kasutajamugavus. 2. MoC ei vaja reaalajas ühendust ühegi andmebaasiga ehk on mõeldud kasutamiseks offline. Sõrmejäljekujutisi säilitatakse turvaliselt kiibis. 3. Sellise lahenduse kasutuselevõtmine on vajalik kõrgemat autentimistaset nõudvate teenuseosutajate (pangad, telekommunikatsiooniettevõtted jt) jaoks.

MoC tehnoloogia rakendamisega seotud riskid on: 1. Vajadus spetsiaalsete lugejate järele, mis vähendavad kasutajamugavust ja ei ole odavad (keskmine risk, maandamismeetmed: kõrgemat autentimistaset nõudvad teenuseosutajad võimaldavad klientidele lugejaid tasuta või kasutatakse neid teenuseosutaja juures kohapeal). 2. Kohe ei ole palju kasutusvõimalusi (kõrge risk, maandamismeetmeks rakendamine ainult digitaalsel isikutunnistusel).

[47] EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) nr 910/2014, 23. juuli 2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ

12. E-identimise ja e-tehingute usaldusteenuste seaduse kolmas lugemine toimus riigikogus 2016. aasta 12.oktoobril.[48]. Vastava eelnõu § 2 nimetab eIDAS määrust rakendavad pädevad asutused. Näiteks täidab eelnõu kohaselt Euroopa Parlamendi ja Nõukogu määruse (EL) nr 910/2014 artiklitest 9 ja 12 tulenevaid liikmesriikidevahelise koostöö ühtse kontaktpunkti ülesandeid valitsuse volitatud riigiasutus. Ka isikutuvastusandmete piiriülese kinnitamise võimaluse tagamist vastavalt Euroopa Parlamendi ja Nõukogu määruse (EL) nr 910/2014 artikli 7 punktile f korraldab valitsuse volitatud riigiasutus.
    Soovitus: Käsitleda Euroopa Liidu e-identimise koostöövõrgustikku kuuluvaid Eesti kontaktpunkte Eesti identiteedihalduse osana.

13. ICAO viib läbi identiteedihalduse auditeerimisi. ICAO kontrollib vastavust tema poolt antud soovitustele „ICAO guide for assessing security of handling and issuance of travel documents“. Soovitustes on toodud vajalike tegevuste loetelu ja audiitor hindab, kas ja millisel määral vajalikud tegevused riikides on läbi viidud.
    Soovitus: Viia Eestis läbi enesehindamine vastavalt „ICAO guide for assessing security of handling and issuance of travel documents“ ver 4, 2016[49].

14. Seaduslikud topeltidentiteedid on siseriiklik kompetents. Riigi julgeoleku seisukohalt ei avaldata neid andmeid. Mõnes riigis teeb parlament järelevalvet topeltidentiteetide üle. Näiteks Rootsis tuleb üks kord aastas anda parlamendile ülevaade olukorrast, sama kord kehtib teadaolevalt Suurbritannias.
    Soovitus: Analüüsida, kas järelevalvesüsteem topeltidentiteetide kasutamise üle on Eestis piisavalt reguleeritud.

15. Isikutunnistuse digitaalse vormi kohustuslikkus (valikuvabaduse puudumine erinevat liiki isikutunnistuste vahel) on toonud edu infoühiskonna arendamisel.
    Soovitus: Jätkata isikut tõendavate dokumentide poliitikat, mille nurgakiviks on ühe riiklikult välja antava elektroonilise funktsionaalsusega isikutunnistuse kohustuslikkus. Sertifikaatide peatamise funktsionaalsusest piisab valikuvabaduse realiseerimiseks.

16. Et mobiiltelefonidest kaovad lähitulevikus ära eraldatavad SIM-kaardid (SIM-kaart muutub telefoni osaks), siis tuleb leida uusi lahendusi mobiil-ID jaoks. Üks arenguvõimalusi on kontaktivaba autentimislahendust võimaldava tehnoloogia NFC *(Near Field Communication)* liidese kasutusele võtmine isikutunnistustel, mille abil saab isikutunnistust ja mobiiltelefoni koos autentimisel ja digitaalallkirjastamisel kasutada.

---

[48] eIDAS määruse rakendamine ei ole käesoleva uuringu skoobis. Uuringu skoobis on identiteedihalduse korraldus erinevates riikides, sh Eestis. Komisjoni rakendusotsus (EL) 2015/296, 24. veebruar 2015, kehtestas menetluskorra liikmesriikide vaheliseks koostööks e-identimise valdkonnas vastavalt Euroopa Parlamendi ja Nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 12 lõikele 7. Rakendusotsuse artikliga 3 “Ühtsed kontaktpunktid” on kehtestatud, et: 1) Määruse (EL) nr 910/2014 artikli 12 lõigetes 5 ja 6 ettenähtud liikmesriikidevahelise koostöö hõlbustamiseks määrab iga liikmesriik ühtse kontaktpunkti; 2) Iga liikmesriik esitab teistele liikmesriikidele ja komisjonile teabe ühtse kontaktpunkti kohta. Komisjon avaldab ühtsete kontaktpunktide loetelu internetis. Ühtsed kontaktpunktid on kahtlemata Euroopa Liidu liikmesriikide identiteedihalduse osa.

[49] TAG/TRIP/1-WP/25Appendix B

Soovitus: Kaaluda NFC liidese kasutusele võtmist järgmise põlvkonna isikutunnistustel, mis looks ühe võimaliku aluse uut tüüpi mobiil-ID arendamiseks.

17. Eestis on seni kasutusel väga otstarbekaks ja turvaliseks osutunud mudel, kus autentimine (tuvastatakse isik) ja autoriseerimine (tuvastatakse tema volitused) on kaks erinevat protsessi. Näiteks toimub X-Tee andmevahetuskeskkonnas autentimine tsentraalselt, aga volituste andmine ja kontroll on teenuse osutaja ülesanne.
    Mitmetes riikides jätkub diskussioon tsentraalse autoriseerimislahenduse loomise ja rollisertifikaatide[50] (sertifikaadi väljastamisel saab inimene teatavad õigused või rolli) kasutamise ulatuse üle. Kuna inimese volitused on pidevas (lausa igapäevases) muutumises, siis on nii tsentraalne autoriseerimislahendus kui ka rollisertifikaatides inimese volituste aktuaalsena hoidmine üsna keeruline ja kallis lahendus.
    Soovitus: Jätkata Eestis seni kasutusel olevat mudelit, kus autentimine ja autoriseerimine on kaks erinevat protsessi.

18. Arvestades Euroopa Liidus praegu toimuvat andmekaitsereformi ja seda, et 2018. aasta on vähemalt kahe andmekaitse määruse rakendamise tähtaeg, on soovituslik hakata planeerima nende rakendamise strateegiaid ja tutvustama tulevaid määrusi ja muudatusi avalikkusele ja eelkõige isikuandmete töötlemisega kokku puutuvatele isikutele, et suurendada ühest küljest avaliku ja erasektori e-teenuste ja e-äri tõhusust ning turvalisust ja teisest küljest residentide ja e-residentide usaldust e-teenuste ja e-riigi vastu.
    Soovitus: Eesti identiteedihaldus peab olema vastavuses EL andmekaitsereformiga loodava keskkonnaga. Oluline on dialoog proportsionaalsuse üle, rakendades turvaliseks identiteedihalduseks vajalikke kaasaegseid tehnoloogilisi lahendusi ühelt poolt ning kaitstes inimeste privaatsust ja vältides andmete mistahes väärkasutamist teiselt poolt.

Soovitavalt võiks uuringuperiood sarnaste uuringute Euroopa riikides läbiviimiseks ehk eelkõige uuringu alusandmete kogumiseks mitte sisaldada juuli- ja augustikuud.

[50] Kasutatakse ka atribuutsertifikaadi terminit.

Lisa 1. Küsimustikud

1. Põhiküsimustik

1) What national legal acts, codes of conduct, procedures and policy documents (hereinafter *Legal acts*) regulate your country's identity management policy?
2) Are personal identities managed centrally (yes/no)? By whom are/is the identification system/s driven (responsible authority)?
3) Which data is personal identity creation based on in public and private sectors? How is the identity creation managed? Whether/how is the creation and use of multiple identities prevented?
4) How the personal data protection is managed? Are there any national legal acts or rules regulating the identity management procedures to be followed by the public and private sectors? Do private entities have access to national databases/opportunity to make queries in order to verify someone's identity? If yes, which databases and what are the corresponding legal acts?
5) In which civil[51] proceedings and under what conditions it is allowed to process the personal identity data, especially biometric data?
6) Do private entities have within private proceedings right to collect, store and transfer to third parties personal identity data, incl. biometric data? If so – to what extent and under what conditions?
7) Whether and – if so – under which conditions it is allowed to cross-use the personal identity data, incl. biometric data, which have been collected within different **civil** proceedings, in **other civil** proceedings (publicvs. public)?
8) Whether and – if so – under what conditions it is allowed to use the personal identity data, incl. biometric data, which have been collected within different **private** proceedings, in **civil** proceedings (private vs. public)?
9) Whether and – if so – under what conditions it is allowed to send the personal identity data, incl. biometric data, which have been collected within different **civil** proceedings, **to private** entities? (publicvs. private)?
10) Whether and – if so – under what conditions it is allowed to send the personal identity data, incl. biometric data, which have been collected within different **civil** proceedings, to **other countries and EU institutions/international organizations**?
11) Whether and – if so – how the verification of identities determined by other EU Member States and non-EU Member States is managed in your country?
12) Whether and – if so – which national legal acts and practices regulate the transfer of personal data between different countries within criminal and civil proceedings (mutual legal assistance)?

[51]In the context of the current Research a term ***civil proceeding*** means any kinds of proceedings by public sector authorities or on their behalf; a ***private proceeding*** means a proceeding held by private sector bodies, persons or authorities.

13) How are persons identified and authenticated in electronic communications? Is there electronic identity (digital identity document) in use in the country? If so – is electronic identity based on physical identity and how it is assured (a personal identification number – PIN, password, special chip card, digital signature, SMS, mobile-ID, …)?
14) How are derivative (multi-level, when a person has multiple identities issued by one or different entities) identities managed? How are they linked to each other, what are their rules and usage areas?
15) How the legal pseudonymising – changing of identities (i.e. of individuals under witness protection programs, police agents, etc.) is managed and disclosure of their overlapping with real identities avoided during biometric data processing? Is there a specific legislation (public or classified) on that?
16) The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) EU directive, adopted on 27.04.2016 and entering into force on 25.05.2018, intends to strengthen and unify data protection for individuals within the European Union (EU) and replace the current data protection directive (Directive 95/46/EC).
    a. **Question to non-EU Member States**: The GDPR extends the scope of the EU data protection law to all foreign companies processing data of EU residents. Whether and – if so – how this will influence the legislation of your country? Have any initiatives on education in data protection and privacy/increase of awareness been taken or planned? Has there been the EU directive adaptation plan developed?
    b. **Question to EU Member States**: how and when is the EU directive planned to be implemented? Has there been developed an implementation plan (incl. education in data protection and privacy, increase of awareness) and what are the expected implementation deadlines? Will there a „big bang“ or step-by-step adaptation of the directive?

2. Lisaküsimustik

1) Please provide definition of the term 'delicate personal data' applicable in your country. Is there any additional (stricter) rules concerning biometric data and its processing apart from other personal data (i.e. name, gender, etc.)?
2) Please explain how is biometrics used in establishing a person's identity, how biometric data is processed in civil sector (please refer to the definition of 'civil' in the initial Questionnaire), what are restrictions to storage and usage of this data and is cross-processing allowed in your country? For example, in Sweden and Germany enrolled personal data is destroyed after the document of the holder is personalised. In Estonia all enrolled data including facial and fingerprint images is stored in the informations system database and in case of strictly defined procedures it is allowed to use – for example, in some criminal proceedings and for raising level of assurance in establishing identity of the applicant while applying for a new identity document.
3) Are there additional rules and restrictions to enrollment and collection of especially biometric data in private proceedings?
4) Are there additional rules and restrictions to cross-usage of especially biometric data between civil-civil, civil-private, private-civil and private-private proceedings?
5) Are such processes as for example fingerprint login to a smartphone or using voice and selfie biometrics in banking considered as processing of delicate personal data in your country? For example, Lloyds Banking Group has become the latest UK banking group to enable selfie face recognition technology for the opening of new accounts. À la "Though there are no legal acts to regulate this clearly there exist A and B private services where users' delicate personal data is processed."
6) Is other biometrics apart from fingerprints – iris, veins, voice, gait etc. – used in your country in personal data processing? If yes, are there any differences in requirements to biometric data management in comparison to facial and fingerprint images?
7) Please provide definition of the term 'standard conditions for data processing are met applicable in your country. Please describe the differences from the requirements in the 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016'.

Lisa 2. Küsimustikule vastajate loetelu

1. Küsimustikule vastajate loetelu

Nr	Riik	Vastaja nimi	Positsioon	Kontaktandmed
1.	DE	Vincent Rosahl	Referat IT I 4 - Identifizierungssysteme; Pass- und Ausweiswesen Bundesministerium des Innern	ITI4@bmi.bund.de
2.	DE	Peter Büttgen	Federal Commissioner for Data Protection and Freedom of Information Germany	referat21@bfdi.bund.de
3.	DE	Dr. Sabine Sosna	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Referat 21	referat21@bfdi.bund.de
4.	FI	Mika Hansson	Program Manager, Finnish Country Signing Certificate Authority (CSCA), National Police Board	mika.hansson@poliisi.fi
5.	LV	Inguss Treiguts	Current: Partner at Treiguts Consulting, former: Director of Identity Documents Department, Office of Citizenship and Migration Affairs, Ministry of the Interior	padd@pmlp.gov.lv; +37129479474
6.	NL	Diana van Driel	Coordinator Travel document Policy, Ministry of the Interior and Kingdom relations	Diana.driel@minbzk.nl; +650738468
7.	NO	Jan-Petter Mathisen	Sales Director | Citizen Access & Identity | Norway, Oberthur Technologies Norway AS	jp.mathisen@oberthur.com
8.	SE	Lars Bjöhle	Passport Legal Advisor, Superintendent / Head of travel document organization, Department of Legal Affairs, Swedish Police Authority	lars.bjohle@polisen.se; +46105639419, +46708951687
9.	UK	Kevin Burt	Identity Security, Home Office	kevin.burt@homeoffice.gsi.gov.uk
10.	UK	Calum Bunney	eID Solutions Architect, Nexus Group	calum.bunney@nexusgroup.com; +46739501347

2. Küsimustiku saajate loetelu (mittevastanud/edastanud/keeldunud isikud)

Nr	Riik	Küsimustiku saaja nimi	Kontaktandmed

1.	International	Silvia Pogolsha (OSCE – Organization for Security and Co-operation in Europe)	silvia.pogolsa@osce.org
2.	International	Stephanie de Labriolle (SIA – Secure Identity Alliance)	stephanie.delabriolle@secureidentityalliance.com
3.	AT	Florian Humplik	humplik@staatsdruckerei.at
4.	AT	Erwin Madebacher	erwin.maderbacher@gmx.at
5.	CH	Andreas Lussy	andreas.lussy@for-zh.ch
6.	CH	Michel Baetscher	michel.baetscher@gmail.com
7.	DE	Georg Hasse	georg.hasse@secunet.de
8.	DE	Achim Hildebrandt	achim.hildebrandt@bmi.bund.de
9.	FI	Sakari Arvela	sakari.arvela@poliisi.fi
10.	NL	Ronald Belser	belser@belser.nl
11.	NL	Jasper Mutsaers	jasper.mutsaers@rvig.nl
12.	NL	Jeen DeSwart	jdeswart@xs4all.nl
13.	NO	Arne Isak Tveitan	arne.isak.tveitan@nidsenter.no
14.	NO	Jon Olnes	jon.olnes@unibridge.no
15.	NO	Pal Kristiansen	pal.kristiansen@unibridge.no
16.	NO	Roger Johnsen	roger@norsis.no
17.	NO	Kjell Olav Skogen	kos@commfides.no
18.	NO	Atle Årnes	atle.arnes@datatilsynet.no
19.	NO	Pål Müller	pal.muller@buypass.no
20.	NO	Norunn Elin Saure	norunn.elin.saure@helsedirektoratet.no
21.	NO	Tor Alvik	tor.alvik@difi.no
22.	NO	Annar Bohlin-Hansen	annar.hansen@lifi.no
23.	PT	Luisa Maia Gonçalves	luisa.goncalves@sef.pt
24.	PT	Marina Portugal	marina.portugal@sef.pt
25.	PT	Octávio Rodrigues	octavio.rodrigues@sef.pt
26.	SE	Staffan Tilling	staffan.tilling@polisen.se
27.	SE	Stefan Danielsson	stefan.danielsson@polisen.se

28.	UK	Frank Smith	frank.55@btinternet.com
29.	UK	Margaret-Mary Wilmot	margaret-mary.wilmot2@homeoffice.gsi.gov.uk
30.	UK	Tony Dean	tony.dean2@uk.delarue.com

Lisa 3. Olulisi õigusakte

Lisa kirjeldab valdkonna olulisi õigusakte, mida on kehtestatud nii ELi kui eraldi riikide tasemel.

1. Euroopa Liit

Nr	Õigusakt	Kehtivus	Õigusakti kirjeldus
1.	Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta	Kehtiv kuni 25.05.2018	Direktiiviga kehtestatakse reguleeriv raamistik, et saavutada tasakaal üksikisiku privaatsuse kõrgetasemelise kaitse ja isikuandmete vaba liikumise vahel Euroopa Liidus (EL). Seetõttu on direktiiviga kehtestatud ranged piirangud isikuandmete kogumise ja kasutamise suhtes ning iga ELi liikmesriik peab asutama sõltumatu riikliku andmekaitseasutuse, kes tegeleb kõigi isikuandmete töötlemisega seotud tegevuste järelevalvega.
2.	Euroopa Parlamendi ja Nõukogu direktiiv 96/9/EÜ andmebaaside õiguskaitse kohta	Kehtiv	Direktiiv käsitleb ükskõik millises vormis andmebaaside õiguskaitset
3.	Euroopa Parlamendi ja Nõukogu direktiiv 2002/22/EÜ universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja –teenuste puhul **(=universaalteenuse direktiiv)**	Kehtiv	Direktiivis sätestatakse eeskirjad elektrooniliste sideteenuste osutamiseks ELis: kohustused teatud kohustuslike teenuste (universaalteenuste) osutamiseks ja lõppkasutajate õigused ning üldkasutatavate elektrooniliste sidevõrkude ja -teenuste pakkujate vastavad kohustused
4.	Euroopa Parlamendi ja Nõukogu direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris **(=eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv)**	Kehtiv	Direktiivi eesmärk on direktiivi 95/46/EÜ täiendades kaitsta füüsiliste isikute põhiõigusi, eelkõige nende õigust eraelu puutumatusele, ja juriidiliste isikute õigustatud huve
5.	Euroopa Parlamendi ja Nõukogu direktiiv 2009/136/EÜ, millega muudetakse direktiivi 2002/22/EÜ universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul, direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris, ning määrust (EÜ) nr 2006/2004 tarbijakaitseseaduse jõustamise eest vastutavate siseriiklike asutuste vahelise koostöö kohta	Kehtiv	Direktiivi eesmärk on tagada tulemusliku konkurentsi ja valikuvabaduse abil kogu ühenduses hea kvaliteediga üldkasutatavate teenuste kättesaadavus ning käsitleda asjaolusid, mille puhul turg ei rahulda tulemuslikult lõppkasutajate vajadusi. Käesolev direktiiv sisaldab samuti sätteid lõppseadmete teatud aspektide kohta, sealhulgas sätteid, mille eesmärk on hõlbustada puuetega lõppkasutajate juurdepääsu nendele.
6.	Euroopa Parlamendi ja Nõukogu direktiiv 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete	Ülevõtmise tähtaeg on 06.05.2018 pärast ca 2-	Direktiivis sätestatakse õigusnormid, mis käsitlevad füüsiliste isikute kaitset isikuandmete töötlemisel pädevate asutuste poolt süütegude tõkestamiseks, uurimiseks, avastamiseks, nende eest vastutusele

	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 **(=politseidirektiiv)**	aastast üleminekuperioodi (14.04.2016-6.05.2018)	võtmiseks või kriminaalkaristuste täitmisele pööramiseks, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmiseks ja nende ennetamiseks. Direktiiv asendab varasemat raamotsust
7.	Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2016/681 broneeringuinfo (PNR) kasutamise kohta terroriaktide ja raskete kuritegude ennetamiseks, avastamiseks, uurimiseks ja nende eest vastutusele võtmiseks **(=broneeringuinfo direktiiv)**	Ülevõtmise tähtaeg on 25.05.2018 pärast ca 2-aastast üleminekuperioodi (27.04.2016-25.05.2018)	Uute reeglite kohaselt peavad lennufirmad väljastpoolt Euroopa Liitu ELi suunduvate lennureiside kohta reisijate broneeringuinfot jagama. Iga liikmesriik saab ise otsustada, kas kasutada samu reegleid ka Euroopa Liidu siseste lendude puhul. Tegemist on vastuolulise õigusaktiga, mida on kritiseerinud nii Euroopa andmekaitseinspektor, Euroopa Parlamendi Roheliste fraktsioon kui ka mitmed vabaühendused.
8.	Euroopa Parlamendi Ja Nõukogu määrus (EÜ) 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta	Kehtiv	Kodanike eraelu puutumatuse tagamiseks luuakse määrusega Euroopa Andmekaitseinspektori institutsioon
9.	Nõukogu määrus (EÜ) 1030/2002, millega kehtestatakse ühtne elamisloa vorm kolmandate riikide kodanike jaoks, ja eelnimetatud määruse muudatused	Kehtiv	Elamisloakaardi vormi tehnilised nõuded
10.	Euroopa Parlamendi ja Nõukogu määrus (EÜ) 2006/2004 tarbijakaitseseaduse jõustamise eest vastutavate siseriiklike asutuste vahelise koostöö kohta **(=tarbijakaitsealase koostöö määrus)**	Kehtiv	Määrusega rajati võrgustik pädevatest asutustest, kes vastutavad tarbijakaitsealaste õigusaktide täitmise järelevalve eest. Määrust kohaldatakse üksnes ELis toime pandud rikkumiste suhtes
11.	Nõukogu määrus (EÜ) 2252/2004 liikmesriikide poolt väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta ja eelnimetatud määruse muudatused	Kehtiv	Reisidokumentide tehnilised nõuded
12.	Euroopa Parlamendi ja Nõukogu määrus (EL) 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ ja selle rakendusmäärused	Kehtiv, ülevõtmisel (2 ülevõtmise tähtaega -	eIDAS määrus ühtlustab Euroopa Liidu elektroonilise identiteedi ja digitaalallkirja kasutamise põhimõtteid. Määruse eesmärk on suurendada usaldust elektrooniliste tehingute vastu siseturul, luues ühise aluse turvalisele elektroonilisele suhtlusele kodanike, ettevõtjate ja ametiasutuste vahel, suurendades sellega avaliku ja erasektori internetipõhiste teenuste, e-äri ja e-kaubanduse tõhusust liidus. Määruse eesmärk on tagada, et

		1.07.2016 ja 28.09.2018).[52]	juurdepääsul liikmesriikide pakutavatele piiriülestele internetipõhistele teenustele oleks võimalik turvaline e-identimine ja e-autentimine.
13.	Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta **(=isikuandmete kaitse üldmäärus)**	Ülevõtmise tähtaeg on 25.05.2018 peale ca 2-aastast üleminekuperioodi (27.04.2016-25.05.2018)	Määruse eesmärk on tugevdada ja ühtlustada andmekaitse EL-is ning reguleerida isikuandmete edastamist väljapoole EL-i. GDPR-i põhieesmärke on anda elanikele tagasi kontrolli nende isikuandmete üle ja lihtsustada regulatiivset keskkonda rahvusvahelise äri jaoks ühtlustades vastavat õiguslikku regulatsiooni EL-is. GDPR sisaldab erandeid töötajate isikuandmete töötlemise ja riigi julgeoleku tagamiseks töötlemise jaoks - neid valdkondi võib endiselt reguleerida riigi tasemel

2. Austria

- „Austria e-valitsuse seadus“
- „E-riigi seadus“ (jõustus 1.03.2004)
- "Föderaalseadus isikuandmete kaitse kohta" (ingl. *Federal Act concerning the Protection of Personal Data*, saksa k. *Bundesgesetz über den Schutz personenbezogener Daten või Datenschutzgesetz*) (vastu võetud 17.08.1999, jõustus 1.01.2000)
- „Pangandusseadus“ (ingl. *Banking Act*)
- "Telekommunikatsiooniseadus 2003" (ingl. *Telecommunications Act 2003*)
- "Töönõukogu põhiseadus" (ingl. *Works Council Constitution Act*, saksa k. *Arbeitsverfassungsgesetz*)

3. Eesti

- "Elektroonilise side seadus" (vastu võetud 8.12.2004, jõustus 1.01.2005)
- "Isikuandmete kaitse seadus" (vastu võetud 15.02.2007, jõustus 1.01.2008)
- "Infoühiskonna seadus" (vastu võetud 14.04.2004, jõustus 1.05.2004)
- „Isikut tõendavate dokumentide seadus“ (vastu võetud 15.02.1999, jõustus 1.01.2000)
- „Rahvastikuregistri seadus“ (vastu võetud 31.05.2000, jõustus 1.08.2000)
- „Välismaalasele rahvusvahelise kaitse andmise seadus“ (vastu võetud 14.12.2005, jõustus 1.07.2006)
- „Välismaalaste seadus“ (vastu võetud 9.12.2009, jõustus 1.10.2010)

4. Holland

- "Andmetega seotud rikkumisest teavitamise seadus" (ingl. *Breach Notification Law*, holl. *Wet Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp*) (vastu võetud 26.05.2015, jõustus 1.01.2016)

[52]Liikmesriikide asutused peavad digitaalallkirju vastastikku tunnustama hakkama 1.07.2016. aastal ja elektroonilist identiteeti 28.09.2018. aastal. Liikmesriigid võivad teiste liikmesriikide elektroonilist identiteeti vastastikku tunnustada ka juba varem. Rakenduseelnõu oli Eestis kavandatud jõustuma samaaegselt eIDAS määruse jõustumisajaga Euroopa Liidus ehk 1.07.2016, kuid on 23.08 seisuga läbinud vaid 1. lugemise)

- "Hollandi isikuandmete kaitse seadus" (ingl. *Dutch Data Protection Act*, holl.k. *Wet bescherming persoonsgegevens*) (jõustus 1.09.2001)
- "Hollandi passiseadus" (ingl. *Dutch Passport Law*, holl. *Paspoortwet*)
- „Kohalike omavalitsuste isikukirjete andmebaasi seadus“
- “Otsus erandite kohta” (ingl. *Exemption Decree Data Protection Act*, holl. *Vrijstellingsbesluit Wbp*)
- Seadus küpsiste kohta (holl. *Wet van 4 februari 2015 tot wijziging van de Telecommunicatiewet*)
- "Telekommunikatsiooniseadus" (ingl. *Telecommunications Act*)

5. Läti

- „Biomeetriliste andmete töötlemise süsteemi seadus“ (ingl. Biometric Data Processing System Act)
- „e-identifitseerimise seadus“ (ingl. *Electronic Identification Act*)
- "Elektroonilise side seadus" (ingl. *Electronic Communications Law*)
- "Füüsiliste isikute andmete kaitse seadus" (ingl*. Law on Protection of Personal Data of Natural Persons*) (vastu võetud 23.03.2000, jõustus 20.04.2000)
- "Infoühiskonna teenuste seadus" (ingl. *Law on Information Society Services*)
- "Isikut tõendavate dokumentide seadus" (ingl. *Personal Identification Documents Law*)
- „Isikute erikaitse seadus“ (ingl. *Individuals Special Protection Act*)
- „Perekonnaseisudokumentide registreerimise seadus“ (ingl. *Law on the Registration of Civil Status Documents*)
- „Rahvastikuregistri seadus“ (ingl. *Population Register Law*)

6. Norra

- "Biopankade seadus" (ingl. *Biobanks Act*)
- „e-Kaubanduse seadus" (ingl. *Ecommerce Act*) (küpsised) ja seda rakendav "e-Kaubanduse määrus" (ingl. *Ecommerce Regulation*)
- "Isiklike terviseandmete kogumissüsteemi seadus" (ingl. *Personal Health Data Filing System Act*) (vastu võetud 20.06.2014)
- "Isikuandmete seadus" (ingl. *Personal Data Act*) (vastu võetud 14.04.2000, jõustus 1.01.2001) ja seda rakendav "Isikuandmete määrus" (vastu võetud 15.12.2000, jõustus 1.01.2001)
- "Patsiendiandmete seadus" (ingl. *Act on Patient Records*) (vastu võetud 20.06.2014)
- "Schengeni infosüsteemide seadus" (ingl. *Schengen Information Systems Act*)
- "Terviseuuringute seadus" (ingl. *Health Research Act*)
- "Turustamise kontrolli seadus" (ingl. *Marketing Control Act*) (vastu võetud 9.01.2009, jõustus 1.06.2009)
- "Valuuta vahetamise registri seadus" (ingl. *Currency Exchange Register Act*)

7. Portugal

- "Dekreetseadus 7/2004" (ingl. *Decree-Law No. 7/2004*, port. *Decreto-Ley 7/2004*) (vastu võetud 7.01.2004)

- „Dekreetseadus 97/2011“ (ingl. *Decree-Law No. 97/2011*, port. *Decreto-Ley 97/2011*) (vastu võetud 20.09.2011)
- “Seadus 7/2007 kodanikukaardi kasutuselevõtmisest, väljaandmisest ja kasutamisest” (ingl. *Law 7/2007*, port. *Lei 7/2007*) (vastu võetud 4.02.2007)
- "Seadus 41/2004" (ingl. *Law 41/2004*), mida muudab "Seadus 46/2012" (ingl. *Law 46/2012*)
- "Seadus 46/2012" (ingl. *Law 46/2012*) (vastu võetud 29.08.2012) (küpsised)
- "Seadus 67/98 isikuandmete kaitse kohta" (ingl. *Law 67/98 on personal data protection*) (vastu võetud 26.10.1998, jõustus 1.11.1998)

8. Rootsi

- "Andmete seadus (1973)" (ingl. *Data Act (1973)*)
- "Elektroonilise side seadus" (ingl. *Electronic Communications Act*, rootsi k. *Lagen om elektronisk kommunikation (2003:389)*)
- "Kaamera jälitustegevuse seadus" (ingl. *Camera Surveillance Act*)
- "Krediidiinfo seadus (1973)" (ingl. *Credit Information Act (1973)*)
- „Passiseadus“ ning seda rakendavad „Passimäärus“ ja „ID-kaardi määrus“
- "Rootsi isikuandmete seadus" (ingl. *Swedish Personal Data Act*, rootsi k. *Personuppgiftslagen (1998:204)*) (jõustus osaliselt 24.10.1998 ja täismahus 1.10.2001)
- „Struktureerimata materjali reegel“ (ingl. *Unstructured Material Rule*) (jõustus 1.01.2007)
- "Turukaitseseadus" (ingl. *Marketing Act*)
- "Võla sissenõudmise seadus (1974)" (ingl. *Debt Recovery Act (1974)*)

9. Saksamaa

- „De-Maili seadus“ (saksa *De-Mail-Gesetz*)
- „Elektroonilise allkirja taristu seadus“ (vastu võetud 16.05.2001)
- „ID-kaardi ja elektroonilise identifitseerimise seadus“ (ingl. *Act on Identity Cards and Electronic Identification*, saksa *Personalausweisgesetz, PAuswG*)
- "Kõlvatu konkurentsi seadus" (ingl. *Unfair Competition Act*, saksa k. *Gesetz gegen den unlauteren Wettbewerb*)
- „Passiseadus“ (ingl. *Federal Act on Passports*, saksa *Passgesetz*)
- „Saksamaa andmekaitse föderaalseadus" (ingl. *German Federal Data Protection Act*, saksa k. *Bundesdatenschutzgesetz*) (jõustus 23.05.2001)
- "Saksamaa telekommunikatsiooniseadus" (ingl. *German Telecommunications Act*, saksa k. *Telekommunikationsgesetz*)
- "Saksamaa telemeediaseadus" (ingl. *German Telemedia Act*, saksa k. *Telemediengesetz*)
- „Sotsiaalseadustik“

10. Soome

- "Biopankade seadus" (ingl. *Act on Bio Banks* (688/2012)
- “ID-kaardi seadus” (ingl. *Identity Card Act*, soome *Henkilökorttilaki*)
- "Infoühiskonna seadus" (ingl. *Information Society Act* (917/2014)) (jõustus 1.01.2015)
- “Passiseadus” (ingl. *Passport Act*, soome *Passilaki*)
- "Patsientide staatuse ja õiguste seadus" (ingl. *Act on the Status and Rights of Patients* (785/1992)),

- „Rahvastikuandmete ja rahvastikuregistri tõendite seadus“ (ingl. *Population Information System Act,* soome *Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista*)
- "Soome infoühiskonna koodeks" (ingl. *Finnish Information Society Code*, soome k. *Tietoyhteiskuntakaari 2014/917*) (vastu võetud 7.11.2014, jõustus 1.01.2015)
- "Soome isikuandmete seadus" (ingl. *Finnish Personal Data Act*, soome k. *Henkilötietolaki* 1999/523) (vastu võetud 22.04.1999, jõustus 1.06.1999)
- "Sotsiaalhoolekande klientide positsiooni ja õiguste seadus" (ingl. *Act on the Position and Rights of Clients of Social Welfare* (812/2000))
- "Taustakontrolli seadus" (ingl. *Act on Background Checks* (726/2014))
- “Turvalise elektroonilise autentimise ja elektrooniliste usaldusteenuste seadus” (ingl. *Digital Signature Act*, soome *Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista*)
- "Tööelu puutumatuse kaitse seadus" (ingl. *Act on the Protection of Privacy in Working Life* (759/2004)) (töötajate andmete kaitse)
- "Valitsuse tegevuse avatuse seadus" (ingl. *Act on the Openness of Government Activities (621/1999)*)
- “Välismaalaste seadus” (ingl. *Foreigner Act*, soome *Ulkomaalaislaki*)

11. Suurbritannia

- "Andmekaitse seadus 1998" (ingl. *Data Protection Act 1998*) (enamik sätteid jõustus 1.03.2000)
- "Eraelu puutumatuse ja elektroonilise side (EÜ direktiivi) määrustik 2003" (ingl. *Privacy and Electronic Communications (EC Directive) Regulations 2003*) (jõustus 11.12.2003)
- „ID-kaardi seadus 2006“ (vastu võetud 2006. aastal)
- „Isikut tõendavate dokumentide seadus 2010“ (vastu võetud 2010. aastal)

12. Šveits

- "Elektroonilise allkirja valdkonna sertifitseerimisteenuste määrus"
- "Kõlvatu konkurentsi seadus" (ingl. *Swiss Unfair Competition Act*)
- Raamatupidamisseadus"
- "Šveitsi andmekaitse föderaalseadus" (ingl. *Swiss Federal Data Protection Act*) (vastu võetud 19.06.1992, jõustus 1.07.1993)
- "Šveitsi elektroonilise allkirja föderaalseadus"
- „Šveitsi kodanike isikut tõendavate dokumentide föderaalseadus“
- „Šveitsi kodanike isikut tõendavate dokumentide määrus“

Lisa 4. Soovitatav kirjandus

1. DLA Piper (2016). Data Protection Laws of the World. Kättesaadav: https://www.dlapiperdataprotection.com, 1.10.2016.
2. Kindt, Els J. (2013). Privacy and Data Protection Issues of Biometric Applications, a Comparative Legal Analysis. Springer.
3. Campisi, Patrizio (2013). Security and Privacy in Biometrics. Springer.
4. OECD (2011), National Strategies and Policies for Digital Identity Management in OECD Countries, OECD Digital Economy Papers, No. 177, OECD Publishing. Kättesaadav: http://dx.doi.org/10.1787/5kgdzvn5rfs2-en, 28.08.2016
5. GSMA (2016). Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. Secure Identity Alliance Discussion Paper. Kättesaadav: http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf. 1.10.2016
6. Article 29 Data Protection Working Party (2012). Opinion 3/2012 on developments in biometric technologies. Kättesaadav: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf. 1.10.2016
7. Eurosmart (2015). The Future Digital Identity Landscape in Europe. Kättesaadav: http://www.eurosmart.com/news-publications/policy-papers/158-the-future-digital-identity-landscape-in-europe.html. 1.10.2016
8. ICAO Guide for Assessing Security of Handling and Issuance of Travel Documents. Version 4, 2016. Kättesaadav: http://www.icao.int/Security/mrtd/Pages/Assessment-Guide.aspx. 3.10.2016
9. European Union (2013). Feasibility Study on an Electronic Identification, Authentication and Signature Policy (IAS) – Stork 2.0. Kättesaadav: http://ec.europa.eu/information_society/newsroom/cf/dae/itemdetail.cfm?item_id=12030. 3.10.2016
10. Dutch Ministry of the Interior and Kingdom Relations (2015). International Comparison eID Means. Report. Kättesaadav: https://www.government.nl/documents/reports/2015/05/13/international-comparison-eid-means. 3.10.2016
11. Datatilsynet (2016). Tracking in Public Spaces: The use of WiFi, Bluetooth, beacons and intelligent videoanalytics. Kättesaadav: https://www.datatilsynet.no/globalassets/global/04_planer_rapporter/sporing-i-det-offentlige-rom_eng_web.pdf. 3.10.2016
12. UK Government Office for Science (2013). Future Identities: Changing identities in the UK – the next 10 years. DR 19: Identity Related Crime in the UK. Kättesaadav: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275784/13-521-identity-related-crime-uk.pdf