Avaandmete kasutuspotentsiaali uuring

15. juuli 2014

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti tuleviku heaks

Dokumendi andmed	
ID:	**A-001**
Nimetus:	**Avaandmete kasutuspotentsiaali uuring**
Teema lühitutvustus:	**Millised on õiguslikud aspektid – piirangud ja võimalused (nt EL direktiiv --- 1999/93/EC, Eesti seadusandlus) avaandmete kasutamisel autentimisprotsessis? Kuidas on jagatud vastutus CRL---s sisalduva informatsiooni osas sertifitseerimisasutuse ja tema poolt väljastatud CRL---l baseeruva autentimisteenuse osutajale? Millised delikaatsete isikuandmete kaitsega seotud küsimused seejuures võivad kerkida?**
Staatus	**VER.0.1**
Kategooria:	**A1-T**
Dokumendi number:	**CBTS0004-12**
Organisatsioon:	**Cross Borders Trust Services OÜ**
Koostas:	**Liisi Jürgen**
Alusdokument:	**Hankedokument – Avaandmete (Open Data) kasutuspotentsiaali uuringu lähteülessanne;** **Cross Borders Trust Services OÜ Pakkumine – Avaandmete (Open Data) kasutuspotentsiaali uuring**
Seotud dokumendi:	
Allikad:	**Kehtivad õigusaktid:** **Isikuandmete kaitse seadus (RT I 2007, 24, 127)** **Direktiiv 1999/93/EU** **Direktiiv 95/46/EU** **Muu** **Isikuandmete kaitse seaduse seletuskiri (kättesaadav: h kaitse/oigusaktid)** **Kohtupraktika** **Riigikohtu lahend nr 3-3-1-57-03 (http://www.riigikohus 1-57-03)** **Riigikohtu lahend nr 3-3-1-46-10 http://www.riigikohus.ee/?id=11&tekst=RK/3-3-1-46-10** **Riigikohtu lahend nr 3-3-1-70-11 http://www.riigikohus.ee/?id=11&tekst=RK/3-3-1-70-11**

1. Dokumendi ajalugu

Versioon	Koostas	Muudatus	Aeg
0.1	Liisi Jürgen	Dokumendi algversioon	15.07.2014

Uuringu teostamine on kaasrahastatud EASi toel Euroopa Regionaalarengu Fondist.

1. Autentimisprotsess - õiguslikud aspektid – piirangud ja võimalused avaandmete kasutamisel autentimisprotsessis?

1.1. Kohaldatav õigus

EU õigus ei ole siiani toetanud aktiivselt piiriüleseid e-teenuseid ja e-teenuseid toetavaid toiminguid nagu näiteks e-autentimine.[1] EU seadusandja ei ole (selgelt) defineerinud mitmeid olulisi mõisteid ning sätestanud (vajalikke) ühtlustavaid nõudeid.

Direktiiv 1999/93/EC ei kasuta mõistet "autentimine" ja/või "autentimisprotsess". Eesti digitaalallkirja seadus baseerub direktiivil 1999/93/EC ning sellest tulenevalt ei kasuta ka Eesti seadusandja digitaalallkirja seaduses nimetatud mõistet. Samuti ei kasuta direktiiv 95/46/EU mõistet "autentimine" ja/või "autentimisprotsess".

Üldtuntud käsitluse kohaselt on autentimisprotsess kellegi või millegi autentsuse kontroll ehk isiku puhul isiku autentsuse (identiteedi) kontrollimine ja tõestamine. Kuna autentimise eesmärk on teatud andmete töötlemise tagajärel teha kindlaks isik, siis autentimisprotsessi juures tuleb tähelepanu pöörata isikuandmete kaitse seadusele (edaspidi IKS). IKS reguleerib isikuandmete töötlemise tingimusi ja korda. Seaduse üldine kohaldavus ei sõltu töötlemise viisist k.a automatiseeritud juhtudel.

Samuti ei kasuta direktiiv 1999/93 mõistet "avaandmed". Avaandmete mõiste sisutamisel lähtub Analüüsi autor Hanke kutses toodud käsitlusest, mille kohaselt **avaandmete** *(open data) all mõistame kõigile avalikult vabalt kasutamiseks antud, veebist kättesaadavaid, masinloetavas formaadis andmeid ilma kasutamis-, patentide- ja levitamispiiranguteta. Üldjuhul, kui seaduses ei ole andmete hankimise eest ette nähtud tasu, saab avaandmeid kätte tasuta ja ilma ligipääsupiiranguteta*.

1.2. Isikuandmed ja avaandmed

Direktiivi 95/46/EÜ artikkel 2 sätestab legaaldefinitsioonid. Punkt a kohaselt on isikuandmed igasugune teave tuvastatud või tuvastatava füüsilise isiku (edaspidi "andmesubjekt") kohta. Tuvastatav isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige isikukoodi põhjal või ühe või mitme tema füüsilisele, füsioloogilisele, vaimsele, majanduslikule, kultuurilisele või sotsiaalsele identsusele omase joone põhjal.

Punkt b sätestab, et isikuandmete töötlemine (edaspidi "töötlemine") – 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.

[1] EU edaspidi kehtima hakkavate õigusaktide projektid lubavad arvata, et üsna varsti olukord muutub, normid defineerivad ühesemalt nõuded ja tingimused.

IKS § 4 lg 1 sätestab, et *isikuandmed on mistahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on*. IKS seletuskiri selgitab, et ei ole olemas füüsilise isiku kohta käivaid andmeid, mis ei ole IKS tähenduses isikuandmed.[2] EU õigus läbi direktiivi 95/46/EU sätestab kohustuse kaitsta mistahes isikuandmeid.

Isiku tuvastatavuse hindamisel tuleb igal üksikjuhtumil arvesse võtta kõiki vahendeid, mida andmete töötleja võib andmesubjekti[3] tuvastamiseks tõenäoliselt kasutada. IKS regulatsiooni laienemiseks ei ole oluline, kas andmesubjekt on tuvastatav otse või kaudselt (üldiste tunnuste või omaduste põhjal või andmete kasutamise kontekstist tulenevalt). Isikuandmeteks IKS tähenduses ei ole füüsiliste isikute kohta käivad andmed, mille puhul ei ole andmesubjekt otse ega kaudselt tuvastatav. Seega ei pea IKS-s ettenähtud nõudeid rakendama anonüümsete andmete töötlemisel, kui andmesubjekti ei ole ka muul viisil võimalik tuvastada.[4]

Avaandmed kui sellised on andmete kogum, mis ei oma IKS tähenduses ainult siis tähendust, kui ükski andmesubjekt ei ole avaandmete hulka kuuluvate andmete juhul tuvastatav. Andmesubjekt ei tohi olla tuvastatav ei otse ega kaudselt. Kui avaandmete hulka kuulub andmeid, mille tagajärjel on võimalik andmesubjekt ehk isik tuvastada, kas otseselt või kaudselt, siis kohaldub IKS.

Samas on autentimise eesmärk isiku kindlaks tegemine. Konkreetse autentimise eesmärk ei pruugi olla isiku täielik tuvastamine, tehes kindlaks isiku nimi, isikukood vms. Autentimise eesmärk võib olla ka isiku osaline tuvastamine või pseudonüümi tuvastamine. Igal juhul on tegu nö kaudse isikutuvastamisega, mis kuulub IKS reguleerimisalasse.

1.3. Kui kohaldub IKS?

IKS sätestab nõuded andmetega töötlemisele. IKS § 5 sätestab isikuandmete töötlemise definitsiooni, mille kohaselt *isikuandmete töötlemine on iga isikuandmetega tehtav toiming, sealhulgas isikuandmete kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, ristkasutamine, ühendamine, sulgemine, kustutamine või hävitamine, või mitu eelnimetatud toimingut, sõltumata toimingute teostamise viisist ja kasutatavatest vahenditest*.

Töötlemine hõlmab igasuguseid isikuandmetega tehtavaid toiminguid. Põhimõtteliselt kõik toimingud isikuandmetega on IKS tähenduses isikuandmete töötlemine.

IKS sätestab §-s 6 isikuandmete töötlemise põhimõtted, millele peab isikuandmete töötlemine vastama. **Isikuandmete töötleja on kohustatud isikuandmete töötlemisel järgima järgmisi põhimõtteid:**

- **seaduslikkuse põhimõte – isikuandmeid võib koguda vaid ausal ja seaduslikul teel**;

[2] IKS Seletuskiri § 4 selgitus teine taane.
[3] IKS § 8 kohaselt on andmesubjekt isik, kelle isikuandmeid töödeldakse.
[4] IKS Seletuskiri § 4 selgitus teine taane.

IKS seletuskiri selgitab, et andmete töötlemise õigluse huvides peab andmesubjektil olema võimalik saada töötlemisest teada ja juhul, kui andmeid kogutakse tema enda käest, tuleb teda täpselt ja täies ulatuses teavitada andmete kogumise asjaoludest.

- **<u>eesmärgikohasuse põhimõte</u> – isikuandmeid võib koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning neid ei või töödelda viisil, mis ei ole andmetöötluse eesmärkidega kooskõlas**;

IKS selgitab, et andmetöötluse eesmärk peab olema kindlaks määratud enne andmete kogumist ja sama eesmärgiga peab seonduma ka järgnev andmete töötlemine. See ei tähenda siiski, et eesmärgi hilisem muutmine oleks täielikult välistatud, kuid üldjuhul tuleb igal uuel eesmärgil töötlemiseks saada andmesubjekti selgelt väljendatud nõusolek. Isikuandmete eesmärgikohase töötlemisega ei peeta siiski vastuolus olevaks andmete töötlemist teadusuuringu või statistika vajadusteks.

Töötlemise eesmärgikohasuse põhimõttega seondub ka kohustus töödelda andmesubjekti tuvastamist võimaldavaid isikuandmeid üksnes niikaua, kui see on vajalik seoses andmete kogumise või hilisema töötlemise eesmärkidega; erand kehtib vaid teaduse ja statistika vajadustest lähtudes.

- **<u>minimaalsuse põhimõte</u> – isikuandmeid võib koguda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks**;

Direktiiv 95/46/EÜ artikkel 6 lg 1 p b kohaselt võib isikuandmeid koguda üksnes ulatuses, mis on vältimatult vajalik andmetöötluse eesmärgi saavutamiseks.

- **<u>kasutuse piiramise põhimõte</u> – isikuandmeid võib muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal**;

Enne andmete kogumist määratletud töötlemiseesmärkidest on võimalik hiljem kõrvale kalduda üldjuhul vaid andmesubjekti nõusolekul; erand kehtib vaid teaduse ja statistika vajadustest lähtudes (põhimõte tuleneb direktiivi artikli 6 lõike 1 punktist b, vt direktiivi preambuli punktid 29, 34).

- **<u>andmete kvaliteedi põhimõte</u> – isikuandmed peavad olema ajakohased, täielikud ning vajalikud seatud andmetöötluse eesmärgi saavutamiseks**;

See punkt hõlmab endas seletuskirja kohaselt kahte eesmärki. Esiteks, kui isikuandmeid juba töödeldakse, siis tuleks seda teha korrektselt, põhjendamatu isiku eraellu sekkumiseta, eeldusel, et kogutud andmete ebapiisavuse või nende ebatäpsuse või mitteajakohasuse tõttu jääks saavutamata see oluline töötlemise eesmärk, mis sellist isiku privaatsfääri sekkumist õigustas. Teiseks piirab see põhimõte aga isikuandmete kogumist suuremas ulatuses, kui on vältimatult vajalik andmetöötluse eesmärgi saavutamiseks. IKS teotub direktiivi 95/46/EÜ artikel 6 lõike 1 punktidele c ja d.

Andmete kvaliteedi põhimõte sisaldab ka kohustust töödelda andmesubjekti tuvastamist võimaldavaid isikuandmeid üksnes juhul, kui see on vajalik seoses andmete kogumise või hilisema töötlemise eesmärkidega (põhineb direktiivi 95/46/EÜ artiklil 6 lõike 1 punkt e). Erandi saab siiski teha teaduse ja statistika vajadusi silmas pidades.

- **<u>turvalisuse põhimõte</u> – isikuandmete kaitseks tuleb rakendada turvameetmeid, et kaitsta neid tahtmatu või volitamata töötlemise, avalikukstuleku või hävimise eest;**

Isikuandmete töötlemisel andmesubjektide õiguste ja vabaduste kaitsmise vajadus eeldab, et nii andmetöötlussüsteemi kavandamise kui ka andmete töötlemise ajal tuleb rakendada vajalikke tehnilisi ja korralduslikke meetmeid, et tagada andmete turvalisus ja eelkõige välistada andmete omavolilise töötlemise võimalus.

Andmete töötlemisel tuleb igal ajal andmete tagada selline turvalisuse tase, mis on võimalik saavutada parimat, mõistlike kulutustega kättesaadavat, tehnoloogiat kasutades. Tuleb arvestada konkreetse töötlemisviisiga seotud riske ja kaitstavate andmete laadi. Mida delikaatsemat laadi andmed ning suurem tahtmatu või volitamata töötlemise oht, seda tõhusamad peavad olema ka rakendatavad turvameetmed.

See säte (IKS § 6 p 7) kaitseb isikuandmete töötlejat selliselt, et andmekaitse järelevalveasutus võib nõuda isikuandmete töötlejalt ebaproportsionaalsete turvameetmete rakendamist.

(Direktiiv 95/46/EÜ artikkel 17 lg 1; vt preambuli punkti 46).

- **<u>individuaalse osaluse põhimõte</u> – andmesubjekti tuleb teavitada tema kohta kogutavatest andmetest, talle tuleb võimaldada juurdepääs tema kohta käivatele andmetele ja tal on õigus nõuda ebatäpsete või eksitavate andmete parandamist**.

tulenevalt individuaalse osaluse põhimõttest peab andmesubjektidele olema andmete töötlemise õigluse huvides tagatud võimalus saada teada oma andmete töötlemisest, töötlejatest ja töötlemise eesmärkidest, samuti üldjuhul otsustada enda kohta käivate andmete töötlemiseks nõusoleku andmise või mitteandmise üle (v.a erandid ja piirangud).

Andmesubjektil peab olema ka võimalik esitada vastuväiteid tema andmete töötlemisele ning andmete ebatäpsuse või mittetäielikkuse korral ning nõuda oma isikuandmete parandamist. Tähelepanu tuleb pöörata, et nimetatud individuaalse osaluse põhimõte laieneb ka surnud isiku andmete töötlemisele, sellisel juhul realiseerivad andmesubjekti õigusi surnu pärijad. (IKS põhimõte tuleneb direktiiv 95/46/EÜ artiklitest 10–14 ning preambuli punktidest 38–43)

1.4. Isikuandmete töötlemise lubatavus

IKS § 10 lg 1 sätestab, et *isikuandmete töötlemine on lubatud üksnes andmesubjekti nõusolekul, kui seadus ei sätesta teisiti*. Nagu juba säte ise reguleerib, siis andmesubjekti nõusolekuta tohib andmeid töödelda vaid seaduses ettenähtud juhtudel.

IKS § 10 lg 2 sätestab erisuse haldusorganile, mille kohaselt *haldusorgan võib isikuandmeid töödelda üksnes avaliku ülesande täitmise käigus seaduse, välislepingu või Euroopa Liidu Nõukogu või Euroopa Komisjoni otsekohalduva õigusaktiga ettenähtud kohustuse täitmiseks*.

Seega võib haldusorgan töödelda isikuandmeid täites kohustusi, mis tulenevad seadustes või muust kõrgemast õigusaktist, kui see on seotud avalike ülesannete täitmisega.

1.5. Kokkuvõte

Avaandmed, mis sisaldavad andmeid, mis lubavad isegi kaudselt isiku tuvastamist on isikuandmete töötlemine IKS tähenduses ja seega peab isikuandmete töötleja oma tegevuse kooskõlastama IKS-st ja direktiivist 95/46/EÜ tulenevate nõuete ja põhimõtetega. Direktiivi puhul tuleb arvestada, et direktiiv ei kohaldu otse vaid liikmesriik on kohustatud direktiivi üle võtma siseriiklikku õigussüsteemi. Seega peab Eestis isikuandmeid töötlev isik oma tegevuses olema kooskõlas Eesti siseriikliku õigusega.

IKS § 7 lg 1 sätestab, et isikuandmete töötleja on füüsiline või juriidiline isik, välismaa äriühingu filiaal või riigi- või kohaliku omavalitsuse asutus, kes töötleb või kelle ülesandel töödeldakse isikuandmeid.

IKS § 7 lg 2 sätestab, et isikuandmete töötleja määrab kindlaks:

(i) isikuandmete töötlemise eesmärgid;

(ii) töödeldavate isikuandmete koosseisu;

(iii) isikuandmete töötlemise korra ja viisi;

(iv) isikuandmete kolmandatele isikutele edastamise lubamise.

Need on põhilised kohustused, samas lasub isikuandmete töötlejal IKS alusel veel kohustusi ja nõue kinni pidada IKS-s sätestatud andmete töötlemise põhimõtetest.

Kasutajat peab teavitama, et teenuse kasutamisel tema isikuandmeid töödeldakse. Kasutajal peab jääma õigus keelduda, et tema isikuandmeid töödeldakse. Teenuseosutaja ei pea sellisel juhul teenust osutama.

2. Vastutus

2.1. Vastutus direktiivi 1999/93 alusel

Direktiiv 1999/93 ei kasuta mõistet sertifitseerimisasutus. Direktiiv 1999/93 artikkel 2 p 11 sätestab, et *sertifitseerimisteenuste osutaja on üksus või juriidiline või füüsiline isik, kes väljastab sertifikaate või osutab muid elektrooniliste allkirjadega seotud teenuseid*. Kuna küsimuses on viidatud direktiivile 1999/93, siis käesoleva Analüüsi autor toob välja direktiivis 1999/93 käsitletud vastutuse käsitluse.

Direktiiv 1999/93 sätestab artiklis 6 vastuse sätet. Artikkel 6 lg 1 sätestab, et liikmesriigid tagavad vähemalt, et sertifitseerimisteenuste osutaja, kes väljastab üldsusele sertifikaadi nõuetekohase sertifikaadina või annab üldsusele sellise sertifikaadi kohta tagatise, vastutab üksusele või juriidilisele või füüsilisele isikule, kes põhjendatult tugineb sellele sertifikaadile, põhjustatud kahju eest seoses järgmiste asjaoludega:

a) nõuetekohases sertifikaadis selle väljastamise ajal sisalduva teabe õigsus ja see, et sertifikaat sisaldab kõiki nõuetekohasele sertifikaadile ettenähtud andmeid;

b) kindlus selles, et sertifikaadi väljastamise ajal olid nõuetekohases sertifikaadis määratletud allakirjutaja valduses allkirja andmiseks vajalikud andmed, mis vastavad sertifikaadis esitatud või määratletud allkirja ehtsuse tõendamiseks vajalikele andmetele;

c) kindlus selles, et allkirja andmiseks ja selle ehtsuse tõendamiseks vajalikke andmeid saab kasutada teineteist täiendaval viisil juhtudel, kui sertifitseerimisteenuste osutaja on loonud need mõlemad,

välja arvatud juhul, kui sertifitseerimisteenuste osutaja tõestab, et ta ei ole tegutsenud ettevaatamatult.

Sertifitseerimisteenuste osutajal on õigus vastutust piirata. Nimelt artikkel 6 lg 4 sätestab, et liikmesriigid tagavad, et sertifitseerimisteenuste osutaja võib märkida nõuetekohasele sertifikaadile nende tehingute väärtuse ülemmäära, milleks sertifikaati saab kasutada, tingimusel et see ülemmäär on kolmandatele isikutele arusaadav. Sertifitseerimisteenuste osutaja ei vastuta kahju eest, mis tuleneb selle ülemmäära ületamisest.

Direktiiv näeb ette, et nende suhtes, kes osutavad sertifitseerimisteenuseid üldsusele, kehtivad siseriiklikud vastutust käsitlevad normid, see tähendab, et sertifitseerimisteenuse osutaja vastutab kahju tekitamisel Eesti siseriikliku õiguse alusel.

2.2. Vastutus IKS alusel

IKS § 7 lg 3 sätestab, et *isikuandmete töötleja (edaspidi vastutav töötleja) võib haldusakti või lepinguga volitada isikuandmeid töötlema teist isikut või asutust (edaspidi volitatud töötleja), kui seadusest või määrusest ei tulene teisiti*.

IKS § 7 lg 4 sätestab, et vastutav töötleja annab volitatud töötlejale kohustuslikke juhiseid isikuandmete töötlemiseks ja vastutab selle eest, et volitatud töötleja täidab isikuandmete töötlemise nõudeid. Seaduses sätestatud nõuded määrab volitatud töötleja jaoks kindlaks vastutav töötleja.

IKS § 7 lg 5 sätestab, et volitatud töötleja võib isikuandmete töötlemist edasi volitada üksnes vastutava töötleja kirjalikul nõusolekul ning tingimusel, et ei ületata volitatud töötleja volituste mahtu. Volitatud töötleja määramise õigus on vastutavale töötlejale, kellel lasub vastutus töötlemise nõuetekohase korraldamise eest ja kes peab saama vajaduse korral volitatud töötlejalt ka töötlemisõiguse ära võtta. Kui vastutav töötleja on haldusorgan, siis võib volitatud töötleja määramiseks anda haldusakti või sõlmida halduslepingu. Seejuures tuleb halduslepingu sõlmimisel muu hulgas lähtuda halduskoostöö seadusest. Legaliteedi põhimõttest lähtuvalt peab haldusorganite tegevus olema alati tagasiviidav seaduse sättele, mis tähendab, et igasugune

isikuandmete töötlemine, kui seda teeb avaliku võimu kandja, peab toimuma seaduse või määruse alusel (isikuandmete töötlemine peab olema vajalik asutusele pandud ülesannete täitmiseks).

Vastutav töötleja ei vabane vastutusest nende isikuandmete töötlemise eest, mida töötleb volitatud töötleja. Üldjuhul on kõik isikuandmete töötlejad vastutavad töötlejad. Isikuandmete töötlejateks on kõik isikud ja asutused, kes isikuandmeid töötlevad. Eraõiguslike isikuandmete töötlejatel on kohustus, et isikuandmete töötlemiseks nõusoleku küsimisel peab isikuandmete töötleja teavitama andmesubjekte ka tema andmete töötlemisest volitatud töötleja poolt (IKS § 12 lg 2 p 3). Andmesubjektil peab olema ülevaade, kes tema kohta käivaid andmeid töötleb. Seega on kohustus teavitada andemesubjekti mh volitatud töötlejast.

2.3. Kokkuvõte

Ükski isik sh haldusorgan ei vastuta direktiiv 1999/93 alusel, kui nad ei väljasta sertifikaate direktiivi 1999/93 tähenduses.

IKS alusel vastutab isikuandmete töötleja. Vastutab nii vastutav kui ka volitatud isikuandmetega töötleja.

3. Delikaatsete isikuandmete kaitse (Millised delikaatsete isikuandmete kaitsega seotud küsimused seejuures võivad kerkida?)

3.1. Delikaatsed isikuandmed

Eestis õigusruumis defineerib mõisted isikuandmed ja delikaatsed isikuandmed isikuandmete kaitse seadus. Nimetatud seaduse § 4 lg 1 sätestab, et isikuandmed on mistahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on.

Sama seaduse sama paragrahvi lg 2 sätestab delikaatsete isikuandmete mõiste, mille kohaselt delikaatsed isikuandmed on

(i) poliitilised vaated,

(ii) usulisi ja maailmavaatelisi veendumusi kirjeldavad andmed, välja arvatud andmed seadusega ettenähtud korras registreeritud eraõiguslike juriidiliste isikute liikmeks olemise kohta,

(iii) etnilist päritolu ja rassilist kuuluvust kirjeldavad andmed;

(iv) andmed terviseseisundi või puude kohta;

(v) andmed pärilikkuse informatsiooni kohta;

(vi) biomeetrilised andmed (eelkõige sõrmejälje-, peopesajälje- ja silmaiirisekujutis ning geeniandmed);

(vii) andmed seksuaalelu kohta;

(viii) andmed ametiühingu liikmelisuse kohta;

(ix) andmed süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist.

3.2. Delikaatsete isikuandmete töötlemine

Isikuandmete tööltemise seaduse § 5 sätestab, et isikuandmete töötlemine on iga isikuandmetega tehtav toiming, sealhulgas isikuandmete kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, ristkasutamine, ühendamine, sulgemine, kustutamine või hävitamine, või mitu eelnimetatud toimingut, sõltumata toimingute teostamise viisist ja kasutatavatest vahenditest.

IKS § 12 lg 4 *delikaatsete isikuandmete töötlemiseks tuleb isikule selgitada, et tegemist on delikaatsete isikuandmetega ning võtta selle kohta kirjalikku taasesitamist võimaldav nõusolek*. IKS § 14 lg 1 p 4 kohaselt isikuandmete töötlemine on lubatud andmesubjekti nõusolekuta, kui isikuandmeid töödeldakse andmesubjektiga sõlmitud lepingu täitmiseks või lepingu täitmise tagamiseks, välja arvatud delikaatsete isikuandmete töötlemine.

Riigikohtu praktika on vastavalt IKS muudatustele muutunud. Nimelt Riigikohtu lahendis nr 3-3-1-57-03 selgitatakse, et 1. oktoobrini 2003 kehtinud IAKS § 8 lg 1 p 5 lubas mittedelikaatsete isikuandmete töötlemist ilma isiku nõusolekuta, kui töötlemise eesmärk on kolmanda isiku, kellele andmed üle antakse, õigustatud huvide arvestamine, kui andmesubjekti huvid ei ole olulisemad. 2011. aastal muutis Riigikohus oma seisukohta lähtudes IKS uuest redaktsioonist. Riigikohus selgitab kohtuotsuses nr 3-3-1-70-11, et kui krediidivõimelisuse hindamise või muul samasugusel eesmärgil töödeldavate andmete edastamine on IKS § 11 lg 7 alusel välistatud, tuleb kooskõlas IKS § 6 p-s 2 sätestatud eesmärgikohasuse põhimõttega lõpetada nende igasugune töötlemine IKS § 11 lg 6 alusel.

Riigikohus nr 3-3-1-46-10 sedastab, et IKS § 21 lg 2 p 3 välistab sõnaselgelt andmesubjekti õiguse nõuda tema kohta kogutud isikuandmete kustutamist või sulgemist, kui andmed on kogutud seaduse alusel. Kuna kinnipeeturegistrisse kogutud andmed on kogutud seaduse alusel (VangS § 51 koostoimes põhimäärusega), ei ole kinnipeetaval õigust nõuda tema kohta kogutud isikuandmete kustutamist või sulgemist.

Kinnipeetaval ei ole õigust pääseda kinnipeeturegistris tema kohta olevate andmete juurde, sest kinnipeeturegistrile on piiratud juurdepääs ja andmeid väljastatakse isikule, kellel on seadusest tulenevalt asutusesiseseks tunnistatud teabele juurdepääsuõigus. Kuna andmete parandamise nõudmine eeldab, et kinnipeetaval oleks juurdepääs tema kohta tehtud kandele, ei saa ta nõuda nende andmete parandamist, mis pole talle saanud õiguspäraselt teatavaks.

Analoogia põhjal saab öelda, et see kehtib ka muudele registritele, aga alus peab tulema seadusest. Ainult seadus tohib reguleerida registri tähtsust. Avaandmete töötlemisest andmesubjekti nõudel ei saa keelduda, kuna avaandmed ei ole seaduse alusel loodud register, mille andmeid on kogutud, et

täita seadusest tulevaid kohustusi ja nõudeid. Seega on andmete töötlejal, kes töötleb avaandmeid, kohustus muuta neid andmesubjekti nõusolekul.

IKS § 27 sätestab delikaatsete isikuandmete töötlemise registreerimise kohustuse. Delikaatsete isikuandmete töötlemine on keelatud, kui Andmekaitse Inspektsioon ei ole delikaatsete isikuandmete töötlemist registreerinud, välja arvatud, kui isikuandmete töötleja ei ole määranud kindlaks IKS §-s 30 sätestatud isikuandmete kaitse eest vastutavat isikut.

Andmekaitse Inspektsioon keeldub delikaatsete isikuandmete töötlemise registreerimisest, kui:

(i) töötlemiseks puudub seaduslik alus;

(ii) töötlemise tingimus ei vasta käesolevas seaduses, muus seaduses või selle alusel kehtestatud õigusaktis sätestatud nõudele;

(iii) rakendatud isikuandmete organisatsioonilised, füüsilised ja infotehnilised turvameetmed ei taga IKS-s sätestatud nõudeid.

IKS § 42 sätestab, et delikaatsete isikuandmete töötlemise registreerimiskohustuse, isikuandmete kaitse turvameetmete või isikuandmete töötlemise muude nõuete eiramise eest karistatakse rahatrahviga kuni 300 trahviühikut ning sama teo eest, kui selle on toime pannud juriidiline isik, karistatakse rahatrahviga kuni 32 000 eurot.

3.3. Kokkuvõte

IKS defineerib väga selgelt, millised andmed kvalifitseeruvad delikaatseteks isikuandmeteks.

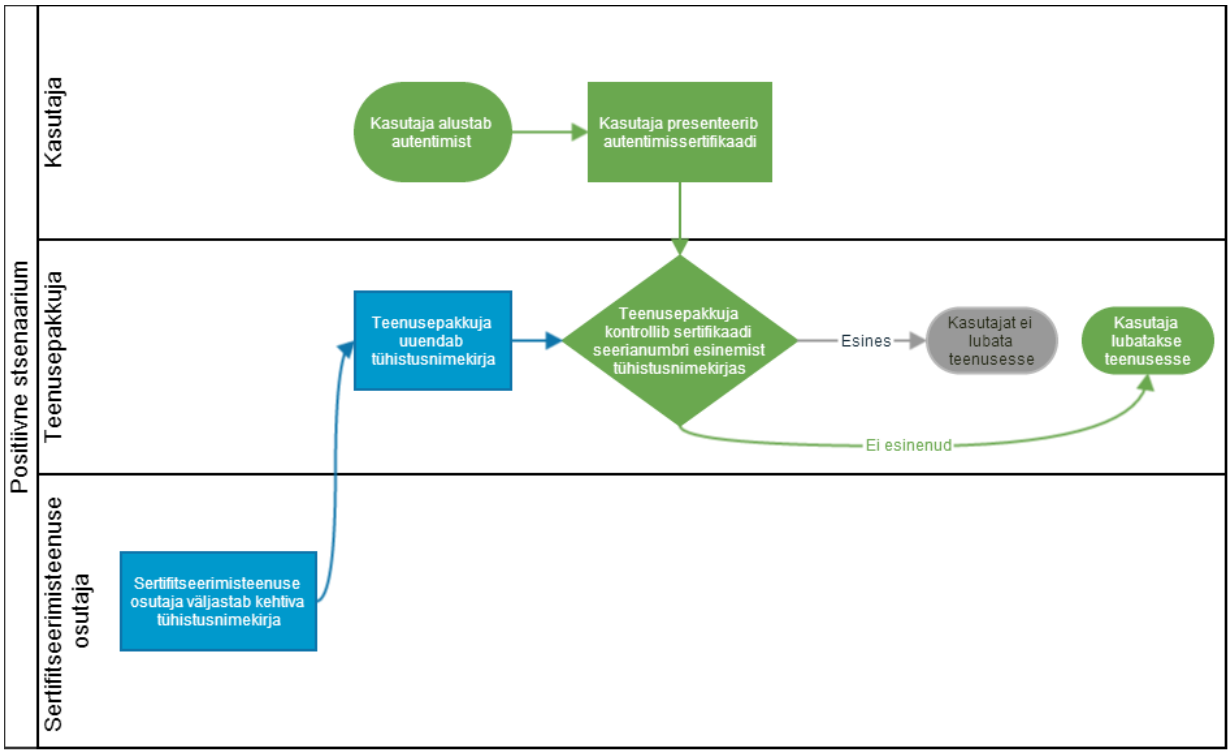
IKS sätestab piirangud ja nõuded delikaatsete isikuandmete töötlemisele. Samuti näeb seadusandja ette, et juriidilist isikut karistatakse delikaatse isikuandmete töötlemise registreerimiskohustuse rikkumise ja/või isikuandmete töötlemisel ettenähtud turvanõuete rikkumisel rahatrahviga kuni 32 000 eurot.

CRL-i abil autentimise stsenaariumid

CRL (Certificate Revocation List) ehk tühistusnimekiri on CA (Certification Authority) ehk sertifitseerimisteenuse osutaja poolt sertifitseerimisahela salajase võtmega signeeritud tühistatud sertifikaatide seerianumbrite nimekiri. CRL ise ei sisalda isikuandmeid, vaid ainult tühistatud sertifikaatide seerianumbreid.

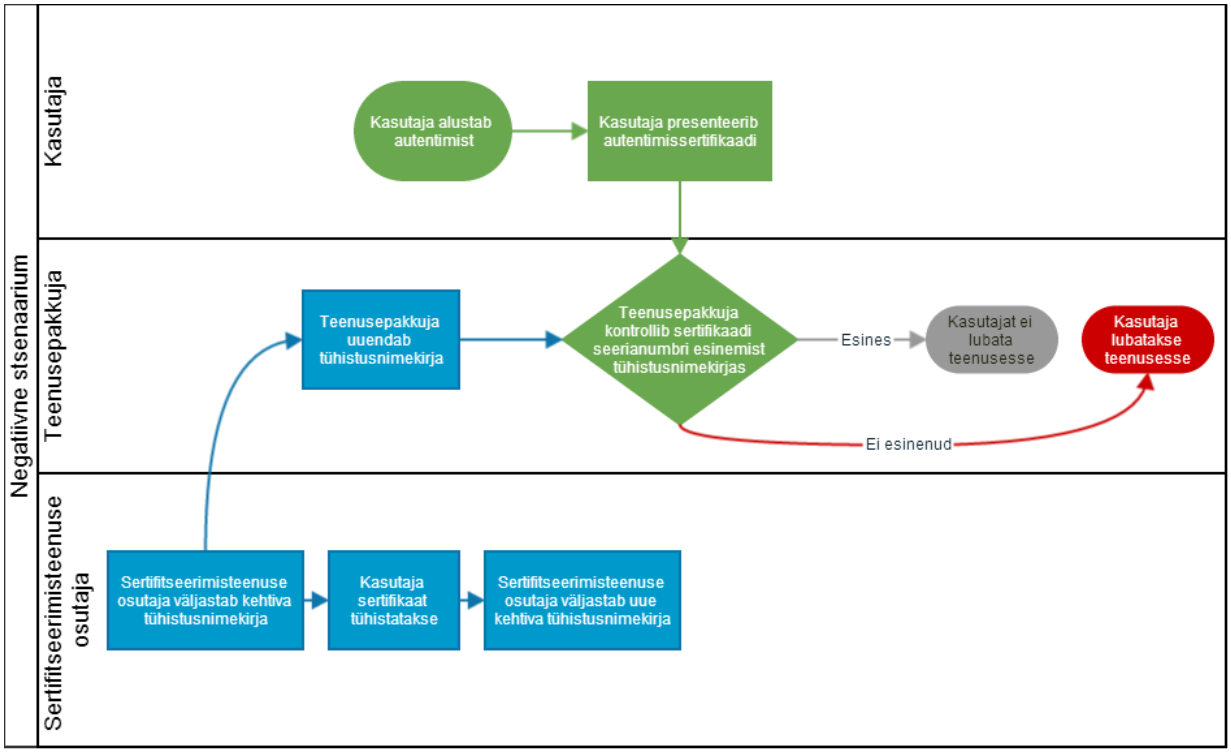
Joonis 1.

Positiivne stsenaarium, mille korral CRL kontrollimisel saadakse korrektne vastus. Kuna teenusepakkujal on tol ajahetkel värskeim tühistusnimekiri on tulemus korrektne.



Joonis 2.

Negatiivne stsenaarium. Teenusepakkuja annab ligipääsu andmetele hoolimata sellest et kasutaja sertifikaat on tühistatud, kuna viimane tühistusnimekiri ei ole veel teenusepakkujani jõudnud.



Et tühistusnimekirja vastu autentimisel ei ole võimalik tagada sertifikaadi kehtivusinfo ajakohasust, siis ei ole soovitatav antud meetodi kasutamine kõrget turvalisust nõudvates keskkondades.

Näide:

Sertifitseerimiskeskus uuendab tühistusnimekirja 2 korda ööpäevas. Seega halvimal juhul jääb ründajale 12 tundi + teenusepakkuja tühistusnimekirja uuendamise intervall eduka ründe sooritamiseks peale kasutajapoolset sertifikaatide tühistamise teate edastamist.

Tulenevalt eelnevast on mõistlik tühistusnimekirja kasutamisel autentimiseks alati teostada riskide hindamine ning hinnata infosüsteemi väärkasutamisest tulenevaid ohtusid. Riskide hindamisel võib aluseks võtta näiteks ISKE rakendusjuhendi versioonis 7.00 leiduvad järgmised riskiastmed:

- R0 – turvaintsidendiga (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmisega) ei kaasne märkimisväärseid kahjusid;
- R1 – kaasnevad vähe olulised kahjud, turvaintsident (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt märkimisväärseid takistusi asutuse funktsiooni täitmisele või märkimisväärseid rahalisi kaotusi;

- R2 - kaasnevad olulised kahjud, turvaintsident (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt olulise takistuse asutuse funktsiooni täitmisele või ohtu inimeste tervisele või keskkonnasaaste ohtu või olulisi rahalisi kaotusi;
- R3 - kaasnevad väga olulised (missioonikriitilised) kahjud, turvaintsident (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt asutuse funktsiooni täitmatajätmise või märkimisväärseid häireid riigikorralduses või ohtu inimelule või keskkonnasaastet või väga olulisi rahalisi kaotusi.

Kõrgema riskiastmega kui R0 on tühistusnimekirja kasutamine ebasoovitatav, kindlasti ei tohiks tühistusnimekirjaga autentimist kasutada kõrgemal tasemel kui R1.

4. Kasutatud allikad

https://www.ria.ee/public/ISKE/iske_rakendusjuhend_7_00.pdf