Sisekontrollisüsteemide toimimine isikuandmete kaitsel riiklikes andmekogudes

Kas inimene võib olla kindel, et tema kohta riigi registritesse kogutud teave on kuritarvituste eest kaitstud?

Riigikontrolli aruanne Riigikogule
Tallinn, 25. november 2008

Sisekontrollisüsteemide toimimine isikuandmete kaitsel riiklikes andmekogudes

Kas inimene võib olla kindel, et tema kohta riigi registritesse kogutud teave on kuritarvituste eest kaitstud?

Kokkuvõte auditeerimise tulemustest

Mida me auditeerisime?

Riigikontroll analüüsis isikuandmete õiguspärase kasutamise kindlustamist seitsmes riigi andmekogus (vt tabel 1). Andmekogude haldajad peavad isikuandmete kaitse seaduse[1] (edaspidi IKS) kohaselt tagama, et inimeste andmed on kuritarvituste eest kaitstud. Andmekogu infosüsteem peab toimima nõuetekohaselt, sh olema töökindel ja turvaline. Kõikidest andmete vaatamise, muutmise, kustutamise, edastamise jmt juhtudest aga peavad säilima logifailid, mille järgi on võimalik tagantjärele hinnata, kes, millal, milliste andmetega, mida ja miks tegi. Riigikontroll hindas, kuidas toimib sisekontrollisüsteem, mis peab tagama andmete õigsust ja säilimist ning vältima nende lekkimist.

Miks see on maksumaksjatele oluline?

Eestit on peetud edukaks e-riigiks, kus on õnnestunud juurutada hulganisti uuenduslikke e-teenuseid. Ulatuslikud andmekogud ja tänapäevased infotöötlusvahendid hõlbustavad ametnike tööd ja võimaldavad inimestele kiiremat, mugavamat ja üldjuhul nende jaoks ka odavamat teenust. Avalikkuse ette on aeg-ajalt jõudnud teavet andmekogudes olevate andmete ebaseaduslikust vaatamisest jmt väiksema kaaluga intsidentidest. Õnneks ei ole need e-riigi ja e-teenuste suhtes üldist umbusku tekitanud. Inimese andmete lekkimise tagajärjeks aga võib halvimal juhul olla isikuvastane kuritegu, identiteedivargus, laenu või kindlustuse kallinemine jne. Esimene suurem infosüsteemide kokkuvarisemine või tundlike andmete leke võib avalikkuse usalduse järsult murda, see omakorda võib tähendada e-riigi arengus tagasilööke, mida teistes riikides on juba kogetud.

Riiklikes registrites on andmed kõigi Eesti elanike kohta. Isikuandmeid on riigi- , aga ka erasektori andmekogudes oluliselt rohkem, kui inimesed oskavad aimata. Tänapäeva demokraatlikus ühiskonnas on inimese üks põhiõigusi õigus eraelu puutumatusele ning valdav enamik inimesi ei soovi, et nende kohta kogutud andmed oleksid teistele ilma mõjuva põhjuseta kättesaadavad. Seetõttu on oluline, et andmekogude haldajad ja andmete kasutajad tarvitaksid meetmeid, mis piiraksid volitamata isikute juurdepääsu andmekogus sisalduvatele isikuandmetele, välistaksid põhjuseta päringuid ning andmete pahatahtliku levitamise korral võimaldaksid tuvastada süüdlase.

[1] Vt http://www.riigiteataja.ee/ert/act.jsp?id=12909389 .

Riigikontroll loodab oma auditiga ühelt poolt tugevdada avalikkuse kindlustunnet, et isikuandmete kaitsele on ka seni tähelepanu pööratud, teiselt poolt toetada andmekogude haldajaid vajalike arenduste ja ümberkorralduste tegemisel. Selleks, et püsiks usaldus riigi infosüsteemide vastu, tuleb tagada elektroonilise andmetöötluse turvalisus. Auditi eesmärk on juhtida tähelepanu sellele, et e-riigis ei piisa heade infosüsteemide rajamisest, vaid andmetöötlejail tuleb luua töökorraldus, mis aitab tagada ja võimaldab kontrollida isikuandmete kasutamise õiguspärasust.

Andmekogudesse kogutavate andmete turvamiseks peavad kõik osapooled, nii andmete kogujad ja kasutajad kui ka inimesed ise, olema teadlikud isikuandmete kuritarvitamise ohtudest ja isikuandmete kaitse meetmetest. Inimesel on õigus kontrollida enda kohta talletatud informatsiooni ning saada ülevaade, kes ja mis eesmärgil tema andmeid kasutab. Kui selleks inimesele luua mugavad võimalused, muutub ta sel viisil ise üheks lüliks oma andmete kaitse ahelas.

Mida me auditi tulemusel leidsime?

Vaadeldud andmekogude sisekontrollisüsteemides leiti olulisi puudujääke, seetõttu puudub Riigikontrolli hinnangul kindlus, et riigi andmekogudes on inimeste andmed kuritarvituste eest piisavalt hästi kaitstud. Olukorra parandamiseks tuleks selgemalt teadvustada andmekogudesse kogutud andmete tõhusa kaitse vajadust, isikuandmete kaitse aspektist üle vaadata asutuse andmekogude kasutamisega seotud töökorraldus ning sisse viia regulaarne järelevalve andmete kasutamise üle. Enne eelnimetatud muudatuste tegemist aga ei saa olla kindel isikuandmete kaitstuses volitamata või väära tarvituse eest.

Sisekontrollisüsteemide nõrgim koht on järelevalve andmete kasutajate üle: logifaile isikuandmete töötlemise kohta säilitatakse ja analüüsitakse ebajärjekindlalt, mistõttu andmete õigusvastane vaatamine, muutmine, edastamine jmt ei ole piisava kindlusega välistatud. Andmekogude haldajad on panustanud infoturbele, kuid mitmel juhul jätnud tagaplaanile isikuandmete kaitsega seonduvad protseduurid. Üksikud andmekogude haldajad on teinud süstemaatilist järelevalvet isikuandmete töötlemise põhjendatuse üle ning on tuvastanud ka rikkumisi. Kuna enamik andmekogude haldajaid pole kontrolli teostanud, ei ole teada isikuandmete õigusvastase töötlemise tegelik ulatus. Osa vaadeldud infosüsteemidest ei võimalda saada piisavalt detailset infot isikuandmete töötlemise kohta ning vahendid järelevalve teostamiseks selle üle, kas isikuandmeid kasutatakse õiguspäraselt, on puudulikud. Teisel osal on olemas küll andmed, mille alusel oleks võimalik kontrollida, kuid kontroll ei toimu regulaarselt, vaid kaebuse alusel rikkumiskahtluse korral. Head näited on Siseministeeriumi ning Maksu- ja Tolliameti töökorraldus, kus vastavalt rahvastikuregistri ja maksukohustuslaste registri puhul on pisteline isikuandmete kasutuse kontroll juba kujunenud tööprotsessi loomulikuks osaks.

Mitmel juhul on andmekogu haldaja, sõlmides kasutuslepinguid väliste andmesaajatega, delegeerinud neile ka kohustuse tagada isikuandmete turvaline ja eesmärgipärane kasutamine. Siiski ei ole kõik vaatlusaluste andmekogude haldajad huvi tundnud nende kohustuste täitmise vastu. Paraku asutused, kes kasutavad teise asutuse andmekogu, ei kontrolli üldjuhul samuti, et nende ametnikud kasutaksid andmekogusid eesmärgipäraselt.

Vaatlusalustes andmekogudes on tekkinud mahajäämus riigi infosüsteemi kindlustavate süsteemide kasutuselevõtul. 1. juuliks 2008. a pidid kõik andmekogud kasutusele võtma infosüsteemide kolmeastmelise etalonturbe süsteemi[2], et tagada andmete kättesaadavus ning kaitse volitamata avalikustamise ja muutmise eest, kuid enamik andmekogudest ei ole püsinud etteantud ajagraafikus. Lisaks on infosüsteemide andmevahetuskiht[3], s. o X-tee, seni kasutusele võetud vaid osaliselt ning andmekogude registreerimine riigi infosüsteemi haldussüsteemis[4] ebatäielik. Kindlustavate süsteemide täies ulatuses kasutuselevõtu hilinemine takistab turvalist andmevahetust ja X-tee kaudu sooritatavate päringute põhjendatuse kontrollimist.

Puudub veendumus, et delikaatsete isikuandmete kaitseks on kasutatud efektiivseid meetmeid. Vastavalt EL andmekaitse direktiivile peavad liikmesriigid keelama delikaatsete isikuandmete töötlemise, kui selleks ei ole kaalukat põhjust ning töötlemise turvalisus pole tagatud. Mõistagi tuleb selliste andmete töötlemisel maandada nii tehnikast kui inimesest tulenevad riskid. Seega peab enne delikaatsete isikuandmete töötlemise algust olema loodud piisavalt turvaline infotehnoloogiline keskkond, samuti tuleb andmetega kokkupuutuvaid isikuid teavitada nende vastutusest. Isikuandmete kaitse seaduse järgi tuleb delikaatsete isikuandmete töötlemine registreerida Andmekaitse Inspektsioonis või määrata konkreetne vastutav isik, kes hindab delikaatsete isikuandmete töötlemise turvanõuete täitmist oma asutuses ja kindlustab seadusele vastavuse. Auditi käigus selgus, et on loodud juurdepääsud delikaatseid andmeid sisaldavatele andmekogudele, kuid suur hulk kasutajaid, sh vallad, linnad ja haridusasutused, ei ole end registreerinud delikaatsete isikuandmete töötlejatena. Ka andmekogude vastutavad töötlejad ei ole juurdepääsude loomisel sageli tähelepanu pööranud, kas välised andmesaajad on delikaatsete isikuandmete töötlemise registreerinud või isikuandmete kaitse eest vastutava isiku määranud. Vaadeldud linnadest ja valdadest enamikul puudus asutuse infoturbealane dokumentatsioon ning andmekogude kasutamise korda reguleerisid vaid andmekogu haldajatega sõlmitud lepingud. Seetõttu puudub ka veendumus, et delikaatsete isikuandmete kaitseks on kasutusel efektiivsed meetmed.

Inimestel on küll võimalik saada ülevaade, milliseid andmeid riik nende kohta on kogunud, kuid nende kasutamise kontrollimiseks puuduvad mugavad võimalused. Isik võib esitada teabenõude, et teada saada kes, millal ja miks on tema isikuandmeid vaadanud, kuid praktikas tehakse seda harva ning seetõttu ei ole riigiasutused piisavalt panustanud infotehnoloogiliste vahendite loomisele, mis hõlbustaksid teabenõuetele vastamist, rääkimata lahendusest, kus juba riigiportaalis saaks isik näha, kas ja kuidas tema andmeid on kasutatud. Positiivse algatusena on Kodakondsus- ja Migratsiooniamet loonud lahenduse, kus inimestel on

---

[2] Vabariigi Valitsuse 2007. a määrus infosüsteemide turvameetmete kohta, vt https://www.riigiteataja.ee/ert/act.jsp?&id=12901110.

[3] Vabariigi Valitsuse 2008. a määrus infosüsteemide andmevahetuskihi kohta, vt https://www.riigiteataja.ee/ert/act.jsp?&id=12956835.

[4] Vabariigi Valitsuse 2008. a määrus riigi infosüsteemi haldussüsteemi kohta, vt https://www.riigiteataja.ee/ert/act.jsp?&id=12933746.

võimalus riigiportaalis vaadata, kes ja kunas on nende kohta kogutud andmeid vaadanud, kuigi see lahendus ei kajasta hetkel kõiki võimalikke päringuid.

Auditeeritute vastused:

Eesti Riiklik Autoregistrikeskus nõustub eelnõus esitatud ettepanekutega ning lisab, et 2009. a esimesel poolel kasutusele võetava infosüsteemi rakendumisega auditis mainitud puudused kõrvaldatakse.

Majandus- ja Kommunikatsiooniministeerium peab riikliku liiklusregistri kohta esitatud ettepanekuid õigustatuks ning kinnitab, et puudujäägid saavad lahenduse 2009. aastal.

Haridus- ja teadusminister nõustub auditi soovitustega ning lubab neid edaspidises töös arvestada. Samas teatab ta, et osad auditis välja toodud puudujäägid, millele 2008. a suvel juhtis tähelepanu ka Andmekaitse Inspektsioon, on auditi valmimise ajaks juba kõrvaldatud. Minister jääb eriarvamusele vajaduse osas sõlmida haridusasutuste ning valdade ja linnadega EHISe kasutamise lepingud.

Kaitseressursside Amet nõustub tehtud soovitustega. Mitmed soovitused on auditi valmimise ajaks juba rakendatud ning teisi on võetud arvesse kaitseväeteenistuskohustuslike Eesti kodanike riikliku registri arendustöödel 2009. a. **Kaitseminister** hindab auditi soovituste täitmise 2009. a jooksul väga heaks.

Maksu- ja Tolliamet nõustub enamike soovitustega ja täpsustab oma seisukohti.

Kodakondsus- ja Migratsiooniamet nõustub üldjuhul auditi soovitustega, kuid toob välja asjaolu, et mitmed auditis välja toodud soovituste kohest rakendamist pärsib asutuse 2010. a kavandatav liitmine Politsei- ja Piirivalveametiga ning Siseministeeriumi info- ja kommunikatsioonitehnoloogia konsolideerimine ministeeriumi infotehnoloogia- ja arenduskeskusesse. Samuti on tuleval aastal vähenenud rahaliste vahendite hulk ning auditi soovituste rakendamiseks vajalikud arendustööd ei kuulu asutuse prioriteetsete põhiülesannete hulka. Amet jääb eriarvamusele andmekogu vastutava töötleja rolli osas delikaatsete isikuandmete töötlemise registreerimisel Andmekaitse Inspektsioonis. Ameti hinnangul ei ole kõik andmekogudevälised lepingulised töötlejad kohustatud registreerima delikaatsete isikuandmete töötlemist, vaid vastav kohustus on pandud vastutavale töötlejale.

Regionaalminister nõustub auditi seisukohtadega ja teatab, et mitmed auditi soovitused on juba osaliselt rakendatud. Käimas on rahvastikuregistri täiendamise projekt ning 2009. a valmivad senisest paremad rakendused järelevalve teostamiseks, samuti saab inimesel olema võimalus e-teenusena saada vastus tema kohta rahvastikuregistrisse tehtud päringute kohta.

Sotsiaalkindlustusamet nõustub üldjoontes auditi soovitustega, kuid toob välja asjaolu, et mitmete soovituste rakendamine on takerdunud seni ameti ja Sotsiaalministeeriumi vahelise ebamäärase tööjaotuse taha. Amet jääb eriarvamusele pensionikindlustuse registrit peegeldava andmebaasi osas, millele on juurdepääs valla- ja linnavalitsustel. Ameti arvates ei ole tegemist eraldi andmekoguga ning kohalike omavalitsusüksuste

juurdepääsuõigused ei vaja täpsustamist registri vastutava töötleja poolt. **Sotsiaalminister** teatab, et praegu toimuvad Sotsiaalministeeriumi ja Sotsiaalkindlustusameti vahel töökoosolekud leppimaks kokku riikliku pensionikindlustuse registri tööjaotuse osas.

Andmekaitse Inspektsioon teatab, et analüüsib põhjalikult auditis tehtud ettepanekuid töötada välja täiendavad juhendid ning vajaduse korral lülitab need 2009. a tööplaani.

Auditeeritud vallad ja linnad nõustuvad üldjuhul auditi seisukohtadega ning lubavad soovitustega arvestada. Enamik kohaliku omavalitsuse üksusi lubab täiendada sisemist asjaajamiskorda paroolihalduse ja järelevalvekorralduse sätetega.

Auditi valmimise jooksul on isikuandmete kaitse eest vastutava isiku jõudnud määrata Kanepi ja Anija vald, teised on alustanud toiminguid isikuandmete kaitse eest vastutava isiku määramiseks või delikaatsete isikuandmete töötlemise registreerimiseks Andmekaitse Inspektsioonis.

Isikuandmete päringute põhjendatuse kontrolliks on enamik auditeeritud valdadest ja linnadest sisse viinud või viimas päringute taotlusvormi. Torma ja Antsla vald märgivad, et registrite kasutamise hilisemaks järelevalveks võiks toimida ühtne registreerimissüsteem või päringute põhjuse sisestamiskoht riikliku registri infosüsteemis endas.

Sisukord

Valdkonna ülevaade

Isikuandmed – mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on.

Töötlemine on iga isikuandmetega tehtav toiming, sh kogumine, säilitamine, vaatamine, muutmine, avalikustamine, juurdepääsu võimaldamine, edastamine, kustutamine.

Infoturve on informatsiooni kaitse ja see koosneb organisatsioonilistest, füüsilistest ja infotehnoloogilistest meetmetest.

Vastutav töötleja on andmekogu eest vastutav asutus, kes peab andmekogu ise või annab selle ülesande haldusakti või lepinguga volitatud töötlejale edasi. Andmekogu pidamise üleandmine ei vabasta vastutusest: andmetöötluse nõuete täitmise eest vastutavad nii volitatud kui vastutav töötleja.

Volitatud töötleja on asutus, äri- või mittetulundusühing vm, kes on saanud haldusakti või lepinguga vastutavalt töötlejalt ülesande andmeid töödelda või kelle roll on määratud seaduses või määruses.

Andmekogu haldaja all mõeldakse käesolevas auditis nii vastutavat kui volitatud töötlejat.

Väline andmesaaja on asutus, äri- või mittetulundusühing vm, kes on andmekogu haldajaga sõlmitud lepingu alusel saanud juurdepääsu andmekogule.

1. Isikuandmete kaitset Euroopa Liidus reguleerib direktiiv 95/46/EÜ[5], mis sätestab isikuandmete kaitse üldised põhimõtted kõikides liikmesriikides. Sellest direktiivist juhindub ka Eesti isikuandmete kaitse seadus (edaspidi IKS) ning lisaks IKSile on isikuandmete töötlemisega seonduv reguleeritud ka avaliku teabe seaduses ja elektroonilise side seaduses.

2. Isikuandmete kaitse põhimõtted on järgmised: andmetöötlus peab olema seaduslik, eesmärgipärane, minimaalne, andmeid peab turvama volitamata töötlemise eest ja kasutama vaid piiratud ulatuses, andmed peavad olema kvaliteetsed ja teave nende kasutamise kohta isikule kättesaadav. Käesolevas auditis on tähelepanu pööratud eelkõige kolmele põhimõttele nimetatutest: isikuandmete töötlemise eesmärgipärasusele, nende kaitsele volitamata töötlemise eest ja isiku juurdepääsule tema kohta kogutud isikuandmetele.

3. Infoturbealased nõuded andmekogudele ja nende vastutavatele töötlejatele tulenevad isikuandmete kaitse seadusest ning avaliku teabe seadusest[6]. Viimasest tuleneb kohustus rakendada riigi ja kohalike andmekogude pidamisel riigi infosüsteemi kindlustavaid süsteeme. Isikuandmete kaitse seisukohalt on eriti oluline infosüsteemide kolmeastmelise etalonturbe süsteemi[7], infosüsteemide andmevahetuskihi[8] ja riigi infosüsteemi haldussüsteemi[9] kasutamine andmekogude pidamisel. Alates 1. juulist 2008. a. on kohustuslik rakendada riiklikult kindlaks määratud turvameetmete süsteemi, sh tuleb igale andmekogule määrata tema andmete iseloomust sõltuv turbeaste ja vastavalt sellele valida ja rakendada andmete kaitse meetmed. Seejuures tuleb aluseks võtta infosüsteemide kolmeastmelise etalonturbe süsteem (edaspidi ISKE), s. o rahvusvaheline infoturbe standard andmekogude pidamisel.

4. IKSi 4. peatükis sätestatakse, et isikuandmete töötleja on kohustatud kasutusele võtma organisatsioonilised, füüsilised ja infotehnilised turvameetmed isikuandmete kaitseks. Need meetmed on detailselt kirjeldatud ISKEs, seega ISKE rakendamine aitab tagada ka isikuandmete kaitse.

---

[5] Vt http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:ET:PDF.

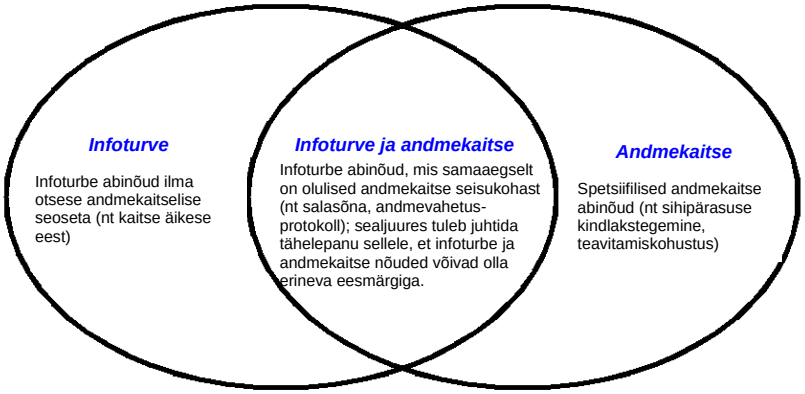
[6] Vt https://www.riigiteataja.ee/ert/act.jsp?id=12900546.

[7] Vt https://www.riigiteataja.ee/ert/act.jsp?&id=12901110

[8] Vt https://www.riigiteataja.ee/ert/act.jsp?&id=12956835

[9] Vt https://www.riigiteataja.ee/ert/act.jsp?&id=12933746

Joonis 1. Infoturbe ja andmekaitse vaheline suhe[10].



Kas teadsite, et

igaühel on õigus andmekogu vastutavalt töötlejalt teada saada, millise asutuse ametnik, millal ja millega seoses on tema isikuandmeid vaadanud.

5. Isikuandmete kaitset ei saa siiski käsitleda pelgalt infoturbe vaatepunktist, sest sageli sõltub väljakujunenud haldusprotseduuridest see, kas isikuandmeid kasutatakse sihipäraselt, kas isikut on andmekasutamisest teavitatud või kas isikuandmeid kogutakse minimaalses ulatuses.

6. Riigi- ja kohaliku omavalitsuse andmekogude täpne arv Eestis ei ole teada. Näiteks on aastaraamatu „IT avalikus halduses 2007" andmetel riigi- ja hallatavate asutuste andmekogusid kokku *ca* 700, aga riigi infosüsteemide haldussüsteem annab andmekogude arvuks 261. Samuti pole täpselt teada, kui paljud neist sisaldavad isikuandmeid. Riigikontroll analüüsis isikuandmete säilimise ja õiguspärase kasutamise kindlustamist seitsmes riigi andmekogus (vt tabel 1). Valitud andmekogud sisaldavad suures koguses isikuandmeid, sh delikaatseid isikuandmeid (välja arvatud maksukohustuslaste register) ning enamikul neist on palju kasutajaid ja väliseid andmesaajaid. Nimetatud andmekogude kasutamist vaadeldi nii andmekogusid haldavates asutustes kui ka viieteistkümnes valla- ja linnavalitsuses.

[10] Allikas: http://www.bsi.de/gshb/baustein-datenschutz/dokumente/b01005_hilfsmittel_tabelle.pdf, lk 2.

Tabel 1. Auditis vaadeldud andmekogud

Andmekogu nimi ja link põhimäärusele	Lühend aruandes	Vastutav töötleja (lühend aruandes)	Volitatud töötleja (lühend aruandes)	Andmed
Riiklik liiklusregister Põhimäärus: https://www.riigiteataja.ee/ert/act.jsp?id=927114	**LR**	Majandus- ja Kommunikatsiooni-ministeerium (MKM)	Eesti Riiklik Autoregistrikeskus (ARK)	Sõidukite, väikelaevade, juhtimisõigust tõendavate dokumentide, sõidumeeriku kaartide ja juhtide ametikoolituse andmed
Eesti Hariduse Infosüsteem Põhimäärus: https://www.riigiteataja.ee/ert/act.jsp?id=13011557	**EHIS**	Haridus- ja Teadusministeerium (HTM)	Riiklik Eksami- ja Kvalifikatsioonikeskus (REKK)	Haridust tõendavate dokumentide, õppeasutuste, õpetajate ja õppejõudude, õpilaste ning üliõpilaste andmed
Kaitseväeteenistuskohustus-like Eesti kodanike riiklik register Põhimäärus: https://www.riigiteataja.ee/ert/act.jsp?id=12920251	**KTKR**	Kaitseministeerium	Kaitseressursside Amet (KRA)	Kaitseväeteenistuskõlblikkuse ja kutsesobivuse ning kaitseväeteenistusalased andmed
Maksukohustuslaste register Põhimäärus: https://www.riigiteataja.ee/ert/act.jsp?id=12749854	**MKR**	Maksu- ja Tolliamet (MTA)	Maksu- ja Tolliamet	Isiku ja asutuse maksualased andmed
Isikut tõendavate dokumentide andmekogu Põhimäärus: https://www.riigiteataja.ee/ert/act.jsp?id=12991447	**ITDAK**	Kodakondsus- ja Migratsiooniamet (KMA)	Kodakondsus- ja Migratsiooniamet	Andmed isikut tõendavate dokumentide taotluste ja dokumentide kohta
Rahvastikuregister Seadus: https://www.riigiteataja.ee/ert/act.jsp?id=12806791	**RR**	Siseministeerium	AS Andmevara	Eesti kodanike ja Eestis elukoha registreerinud, elamisloa või elamisõiguse saanud välismaalaste isikuandmed ja dokumentide andmed
Riiklik pensionikindlustuse register Põhimäärus: http://www.riigiteataja.ee/ert/act.jsp?&id=717145	**PKR**	Sotsiaalkindlustus-amet (SKA)	Sotsiaalkindlustus-amet	Riiklike pensionide, toetuste ja hüvitiste määramise ja maksmise andmed

7. Kui isikuandmete töötlus on volitatud kellelegi teisele, peab vastutav töötleja veenduma, et volitatud töötleja täidab isikuandmete töötlemise nõudeid. Lisaks andmekoosseisu ja kasutuseesmärkide kindlaksmääramisele on vastutava töötleja kohustus otsustada andmete või teabe andmisest keeldumise ja andmete edastamise loa üle.

8. Isikuandmete töötlemise ja selle üle järelevalve korraldamise on keerukaks teinud Andmekaitse Inspektsiooni tõlgendus, et isikuandmete volitatud töötlejateks on ka kõik riigi- ja kohaliku omavalitsuse asutused, kellele on võimaldatud seadusest tulenevate või seaduse alusel pandud ülesannete täitmiseks juurdepääs andmekogule ja seal olevatele isikuandmetele. Tegelikkuses on need IKSi mõistes kolmandad isikud, kellele käesolevas dokumendis on viidatud ka kui välistele andmesaajatele.

9. Ülesanne teostada järelevalvet IKSi täitmise üle on Andmekaitse Inspektsioonil (edaspidi AKI). AKI 2008. aasta tööplaanides on märksõnadeks teadlikkuse tõstmine ja koostöö arendamine riigi- ning kohalike omavalitsuste asutustega, sh on teravdatud tähelepanu alla plaanitud võtta haridusasutused. Oma aastaaruandes[11] märgib AKI, et inimeste teadlikkuse tase isikuandmete kaitsest on kasvanud ning inspektsioon on muutunud registreerijast järelevalveasutuseks. Viimase aspekti positiivsest arengust annab tunnistust omaalgatuslike järelevalvete hulga kasv 2007. aastal.

Turvameetmete rakendamine andmekogudele

10. Isikuandmete kaitse seisukohalt on oluline infosüsteemide turvameetmete süsteemi, infosüsteemide andmevahetuskihi ja riigi infosüsteemi haldussüsteemi kasutamine andmekogude pidamisel. Auditi käigus hinnati vaatlusaluste andmekogude pidamisel järgmisi aspekte:

- riigi infosüsteemi kindlustavate süsteemide kasutuselevõttu vastavalt Vabariigi Valitsuse määrustele;
- infoturbepoliitika ja sellest tulenevate alamdokumentide vastavust IKSi nõuetele;
- arendustööde ja muudatuste halduse ajakohasust;
- järelevalve korraldust isikuandmete töötlemisel;
- andmeid töötlevate ametnike teadlikkust isikuandmete kaitse nõuetest.

Turvameede on tegutsemisviis või mehhanism infosüsteemide ja andmete turvalisuse saavutamiseks ja säilitamiseks.

Infovara on informatsioon, andmed ja nende töötlemiseks vajalikud rakendused.

ISKE on kolmeastmeline etalonturbe süsteem, s. o. minimaalne turvameetmestik, mis tuleb rakendada infovaradele neile ettemääratud turvataseme saavutamiseks ja säilitamiseks.

Riigi infosüsteemi kindlustavate süsteemide kasutuselevõtul on mahajäämus

11. ISKE kui üks kindlustavatest süsteemidest pidi olema rakendatud hiljemalt 2008. aasta 1. juuliks ning selle eesmärk on andmete kaitse volitamata avalikustamise ja muutmise eest ning andmete kättesaadavuse tagamine. Teine kohustuslik süsteem on riigi infosüsteemide haldussüsteem[12] (edaspidi RIHA), mille eesmärk on toetada andmekogude võimet vahetada andmeid ja ühiselt kasutada infot ja teadmisi, et infosüsteemid muutuksid isiku- ja teenusekeskseks. RIHA annab teavet selle kohta, millised andmed kusagil tekivad, milliseid teenuseid ja kellele infosüsteemid osutavad, millised on infosüsteemide omavahelised seosed jmt. Kolmandaks peab kogu andmevahetus riigi infosüsteemi sees, st kõigi riiklike ja KOVide andmekogude vahel, toimuma infosüsteemide andmevahetuskihi (X-tee) teenuste kaudu, tagades sellega süsteemi ühtsuse, turvalisuse ja läbipaistvuse. X-tee rakendamisest on lähemalt juttu aruande 2. peatükis.

[11] http://www.dp.gov.ee/document.php?id=696 lk 52

[12] Vt https://riha.eesti.ee/riha.

Riigi infosüsteemi kindlustavate süsteemide rakendamise tähtajad on ületatud

12. ISKE rakendamisega, st turvameetmete valiku ja juurutamisega, tegeletakse kõikides vaadeldud andmekogudes või nende üksikutes osades. Rakendamine algab asutuse infovarade loetlemisega ning neile vajaliku turbeastme ja turvaklassi määramisega. Andmekogu turvaklass on kohustuslik avalikustada RIHAs. Tegemist on olulise andmekogu iseloomustava näitajaga, mis sisaldab vajalikku infot ka riigi teiste andmekogude jaoks. Samuti on uute andmekogude loomisel turvaklass näidatud andmekogu põhimääruses, ehkki avaliku teabe seaduse kohaselt ei ole see põhimääruse kohustuslik element.

13. Kuigi turvaklassid olid vaadeldud andmekogudele ja nende osadele määratud, ei kajastunud need andmekogude põhimääruses (välja arvatud ITDAKi 3. juulil 2008 vastuvõetud põhimäärus, mis jõustub oktoobri alguses). PKR turvaklassid on kehtestatud asutuse peadirektori käskkirjaga, teiste andmekogude turvaklasse pole määratud üheski õigusaktis. Ka RIHAs puudus info andmekogu turvaklasside kohta (välja arvatud RR ja PKRi puhul).

14. RIHA määrus[13] jõustus 8. märtsil 2008. a. ning selle kohaselt pidid andmekogu asutajad või selle vastutavad töötlejad andmekogu RIHAs registreerima ja andmekogu dokumentatsiooni ajakohastama 1. juuliks 2008 a. RIHA infosüsteemi käivitamise ja kasutajajuhendite avaldamise hilinemine ning infosüsteemi arendustööde toimumine veel registreerimise tähtajale vahetult eelneval ja ka järgneval ajal on takistanud andmekogu haldajatel tähtajaliselt nõutava dokumentatsiooni edastamist RIHAsse. Augusti lõpu seisuga olid vaadeldud andmekogud RIHAs kajastatud, kuid nende kirjeldused olid puudulikud. Enamasti puudus info näiteks selle kohta, mil määral on andmekogu puhul rakendatud infosüsteemide kolmeastmelist etalonturbe süsteemi. Erandiks on EHIS, mille kohta on märgitud, et seda on rakendatud kuni 25% ulatuses nõutavast. RRi kohta on RIHAs juba aegunud info, nagu poleks kõnesoleva turbesüsteemi rakendamist alustatud. ITDAKi kohta on aga ekslik väide, et see nende jaoks üldse rakendamisele ei kuulu. Kuna määrus võimaldab taotleda MKMilt põhjendatult ka dokumentide koostamise ja esitamise tähtaja edasilükkamist, siis vaadeldud andmekogudest on korrektselt käitunud ITDAKi, PKRi ja MKRi haldajad, kes on kooskõlastanud MKMiga oma andmekogude kohta esitatava dokumentatsiooni esitamise uue ajakava.

[13] Vt https://www.riigiteataja.ee/ert/act.jsp?id=12933746

ISKE kasutuselevõtuga on probleeme

ISKE rakendamine on protsess, mis hõlmab järgmised etapid:

- infovaradest ülevaate saamine;
- turvaklassi ja turbeastme (madal, keskmine, kõrge) määramine;
- turvameetmete loetelu koostamine, vastutajate ja teostusplaani paikapanek
- rakendamise kontroll ja täiendav analüüs selle kohta, kas etalonmeetmed on tegelikkuses piisavad.

15. Auditi käigus ilmnes, et enamikul auditeerivatest asutustest oli probleeme ISKE täies ulatuses rakendamisega seadusega sätestatud tähtajaks. Ehkki Vabariigi Valitsuse määrus infosüsteemide turvameetmete kehtestamise kohta on vastu võetud juba 2004. aastal, on andmekogude haldajad jäänud ajahätta. 2007. aastal juhtis Riigikontroll oma auditis[14] probleemile tähelepanu ning soovitas majandus- ja kommunikatsiooniministril rakendada lisaabinõusid, et viia andmekogud vastavusse turvalisusnõuetega. Nimelt selgus tookord, et hulk andmekogusid polnud üldse alustanud ISKE rakendamisega. MKM oma vastuses selgitas, et andmekogude pidamise turvalisus on tagatud ning probleemiks on pigem see, et süsteemid pole nõuetekohaselt auditeeritud ja turvaprotseduurid pole asutustes selgelt formuleeritud. Sellega võib nõustuda, et elektrooniliste andmekogude pidamisel on alati olnud kasutusel turvameetmed ja andmete turvalisus on üldjuhul tagatud. ISKE rakendamisega aga on vastutavatel ja volitatud töötlejail ülesanne teha kindlaks, kas senised meetmed on ISKEst lähtudes piisavad.

16. Lisaks turvameetmete süsteemi rakendamisele on oluline tagada ka asjakohane järelevalve selle rakendamise üle. Vabariigi Valitsuse 20. detsembri 2007. a määruse „Infosüsteemide turvameetmete süsteem" muutmise eelnõu kohaselt on kõikide andmekogude vastutavatel töötlejatel tulevikus kohustuslik regulaarsete auditite läbiviimine[15]. Mida kõrgem turbeaste on andmekogus hoitavatele andmetele määratud, seda sagedamini tuleb läbi viia ISKE audit võimalike riskide hindamiseks ja rakendada abinõusid auditi käigus leitud probleemide lahendamiseks. Vaadeldud andmekogude puhul ISKE rakendamisel üldjuhul järelevalve etappi veel jõutud ei ole ega ole üldjuhul (välja arvatud RR) tellitud ka väliseid ISKE auditeid (vt tabel 2).

Tabel 2. ISKE rakendamine andmekogudes

Andme kogu	ISKE rakendamise seis	Kas ISKE rakendamise seisu on hinnanud väline auditor
ITDAK	Infovarad hinnatud, turvaklassid määratud.	Ei.
RR	Seoses uue infosüsteemi rakendamisega 2009. a tegeletakse olemasolevate turvameetmete täiendava analüüsiga.	Jah, Siseministeeriumi osas 2008. a, ASis Andmevara teostatakse igal aastal infoturbealane audit.
MKR	Rakenduskava realiseerimine lõppjärgus.	Ei.
LR	Rakendavad.	Ei. 2007. telliti infosüsteemide kaardistus, millega algas ISKE rakendamine.
KTKR	Infovarad hinnatud, koostatakse rakenduskava.	Ei. Kavas tellida järgmisel aastal.
PKR	Teostatakse olemasolevate turvameetmete täiendavat analüüsi.	Ei. Tellitud on asutuseväline analüüs ISKE rakendamise seisu kohta.
EHIS	Teostatud analüüs EHISe majutuse osas. Vastutava töötleja kohta ISKE rakendamise analüüs puudub.	Ei.

[14] Vt http://www.riigikontroll.ee/upload/failid/ka_20056_avalikteenus_01-11-2007_lopp.pdf

[15] Vt http://eoigus.just.ee/?act=6&subact=1&OTSIDOC_W=232928

17. Kokkuvõtvalt tuleb tõdeda, et kõikides andmekogudes ei ole ISKE nõutaval määral rakendatud, tööd selle nimel aga käivad. Ka RIHAs ei ole andmekogude kohta kõiki nõutavaid andmeid, kuid see on osaliselt põhjustatud 2008. a toimunud üleminekust RIHA uuele infosüsteemile, mis ei ole tähtajaliselt käivitunud. Kindlustavate süsteemide – ISKE ja RIHA – üksnes osalisest kasutuselevõtust ei järeldu tingimata, et andmekogus olevad andmed ei ole kaitstud. Samas ei anna andmekogudele kehtestatud kohustuste osaline täitmine veendumust, et isikuandmete kaitseks kasutusele võetud meetmed on piisavad.

18. Riigikontrolli soovitus auditeeritud andmekogude vastutavatele töötlejatele: Viia andmekogud ISKE nõuetega kooskõlla ning esimesel võimalusel ajakohastada teave oma andmekogu kohta RIHAs. Esmatähtis on hinnata oma infosüsteemide tegelikku turbevajadust lähtuvalt andmete iseloomust ning ühildada see ISKE nõuetega.

Majandus- ja Kommunikatsiooniministeerium ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega.

Haridus- ja teadusminister teatab, et Haridus- ja teadusministeeriumi juristid määravad kindlaks õigusaktid, millele vastavalt kehtestatakse konkreetsed nõuded ning neile vastavalt teostatakse ISKE nõudeid silmas pidades andmekogu inventuur.

Kaitseminister nõustub esitatud ettepanekuga.

Kaitseressursside Ameti peadirektor teatab, et KTKRi osas on andmekogu haldaja käesolevaks ajaks läbi viinud infosüsteemide turvanõuete hindamise ISKE järgi ning määranud turvaklassi, lähtudes tegelikust turbevajadusest.

Maksu- ja Tolliameti peadirektor antud soovituse osas seiskohta ei avalda.

Kodakondsus- ja Migratsiooniamet teatab, et „vastavalt Vabariigi Valitsuse 28.02.2008 määruse nr 58 „Riigi infosüsteemi haldussüsteem“ § 33 lõikele 4 on KMA 28.05.2008 esitanud taotluse saada pikendust RIHA-sse kantavate andmete tähtaja suhtes, MKM on rahuldanud taotluse 29.05.2008. Taotluse kohaselt oli septembris 2008 ITDAK-i kohta dokumentatsioon koostamisel, mistõttu ei olnud auditeeritava perioodi vältel ITDAK-i kohta varasemalt RIHA-sse kantud andmed korrektsed. Tänaseks on RIHA-sse ITDAK-i kohta andmed esitatud (vastavalt süsteemi võimalustele).

KMA-s on infovarad inventeeritud ning neile määratud turbeastmed KMA peadirektori 15.07.2008 käskkirjaga nr 188. KMA on teinud investeeringuid ja võtnud kasutusele erinevaid meetmeid seoses ISKE rakendamisega. Kuna Siseministeerium kavandab liita KMA alates 2010. a Politsei- ja Piirivalveameti koosseisu, ei ole võimalik esialgu pikaajalisi turbe tegevuskavasid kehtestada ja rakendada. Lisaks pärsivad nimetatud kavade kehtestamist ja rakendamist käesoleval perioodil info- ja kommunikatsioonitehnoloogia (IKT) konsolideerumine Siseministeeriumi infotehnoloogia- ja arenduskeskusesse, mille esimene etapp (IKT põhi- ja arendusteenuste konsolideerimine, sh IT

infrastruktuurilised baasteenused, side infrastruktuuride baasteenused, tarkvara arendus- ja haldusteenused) on kavas lõpetada 2010. a alguseks."

Regionaalminister teatab, et „ISKE rakendamist on alustatud. Turvaklassid on määratud ja kavas sätestada ka rahvastikuregistri seaduse muutmise seaduses. Turvaklassid on sisestatud ka RIHA infosüsteemi. Samade turvaklasside saavutamine on ka üks eesmärkidest, mis on toodud Euroopa Liidust taotletud rahaliste vahendite saamiseks tehtud taotluses ja mille saavutamise garanteerivad rahvastikuregistri täiendamise projekti käigus tehtavad infotehnoloogilised tööd ja uued seadmed, mis on soetatud ja osaliselt veel soetatakse projekti käigus. Koostöös rahvastikuregistri volitatud töötleja AS Andmevaraga alustatakse ISKE dokumentatsiooni kirjutamisega, mis lisanduks seaduses toodule. Rahvastikuregistri uue tarkvara lõpliku valmimise järgselt on Siseministeeriumil kavas tellida sõltumatult turvaeksperdilt täiendav turvaaudit, et olla veendunud, et rahvastikuregister vastab seaduses fikseeritud ISKE nõuetele."

Sotsiaalkindlustusameti peadirektor nõustub soovitusega ning märgib, et „27.01.2006 aasta ministri käskkirjaga nr 22 on IT vara haldamine ja sellega seonduvate dokumentide koostamine üle läinud Sotsiaalministeeriumile. ISKE rakendamine on Sotsiaalministeeriumi valitsemisalas jõudnud projekti I etapi lõpetamiseni (infovarade inventar, turvapoolitika koostamise projekt ja turvaklasside määramine). Projekti lõpptähtajaks on märgitud 17.03. 2009 ning siis hakatakse meetmeid rakendama. RIHAsse on SKA oma andmed sisestanud vana korra järgi. Hetkel toimub andmete kaardistamine ning uue korra järgi hakatakse sisestama enne 2009 a saabumist".

Infoturbe reeglite killustatus eri dokumentide vahel raskendab nende järgimist

19. Üks element andmete turvalisuse tagamisel on infosüsteemide turbe ja kasutamisega seonduvate tegevuste ja reeglite dokumenteerimine. See lihtsustab juhtimist ning toetab jätkusuutlikkust personalimuutuste korral. MKMi soovitustes riigiasutustele infotöö korralduse alase dokumentatsiooni koostamiseks[16] märgitakse, et vajalike kirjalikult jäädvustatud reeglite olemus ja hulk sõltub asutuse spetsiifikast, selle infotöö keerukusest ja kriitilisusest. Vastavalt ISKEle[17] ja MKM soovitustele peab iga suurem asutus, samuti riigi põhiregister, kehtestama muu hulgas infoturbepoliitika. Laia kasutajaskonnaga andmekogude puhul on oluline tagada ka kasutajaile mõistetavate ja isikuandmete kaitse nõudeid sisaldavate kasutusjuhendite olemasolu.

[16] Vt http://www.riso.ee/et/soovitused/tsoovitused.htm.

[17] Vt http://www.ria.ee/public/ISKE_rakendusjuhend_3_00_07092007.rtf lk 25.

Suuremas riigiasutuses, nt ministeeriumis, on soovitavad järgmised IT-korralduslikud dokumendid:

- asutuse IT nõukogu põhimäärus;
- asutuse IT strateegia (arengukava);
- IT osakonna põhimäärus;
- IT personali tööülesanded;
- infoturbe poliitika;
- asutuse IT sisekorra ja hooldamise eeskirjad;
- asutuses kasutatavate rakendusprogrammide juhendid;

20. Dokumentide koostamisel on asutuseti erinev praktika dokumentide arvu ja mahu osas. Infoturbe poliitika on võimalik koondada ühte dokumenti või jagada seda mitmete kitsama spetsiifikaga dokumentide vahel. Ühtse dokumendi puhul on lihtsam dokumentatsiooni täiendada ja parandada ilma riskita, et mõni valdkond unustatakse uuendamata, samuti välditakse kordusi ja vasturääkivusi, mis võivad kergemini juhtuda dokumentide paljususe korral. Andmekogude dokumentidega tutvudes leidsime, et infoturbe poliitika, samuti kõik teised infoturbealased dokumendid, ei sisalda alati viiteid nende alusdokumentidele. Samuti ei loetleta neis sageli alamdokumente, mis koostatakse infoturbe poliitikale tuginedes. SKA-l puudus infoturbe poliitika.

Infoturbe reeglitest on andmekogu kasutajal raske ülevaadet saada

21. Vaadeldud andmekogude infoturbealases dokumentatsioonis köidab tähelepanu killustatus ja tavakasutaja vaatenurgast lähtuvalt ka liigne keerukus. Andmekogu tavakasutajal on raske saada ülevaadet dokumentidest ja nende muudatustest, millega just tema peaks kursis olema. Erinevalt teistest vaadeldud andmekogudest sisaldab KTKRi „Kaitseressursside Ameti infotehnoloogiliste vahendite kasutamise eeskiri" loetelu dokumentidest ja tavadest, millest tuleb lähtuda selle asutuse infosüsteeme kasutades, ja annab sellega hea ülevaate olemasolevast reeglistikust.

22. Infoturbe reeglitest teadlikkuse tõstmisele aitab kaasa, kui asutuses kasutatavate rakendusprogrammide kasutusjuhendid annavad lisaks andmekogu kasutamise alastele selgitustele kasutajale lühiülevaate või viite asutuse infoturbealastele reeglitele (paroolihaldus, arvutivõrgu kasutamise eeskiri jmt). Kasutajal oleks oluliselt mugavam tutvuda üheainsa, temale suunatud dokumendiga, kui hakata otsima asutuse dokumendiregistrist, milline infoturbealane dokument teda võiks puudutada. Häid näiteid infosüsteemide kasutajajuhenditest leidsime KTKR, MKR ja LR puhul.

Välist andmesaajat ei teavitata piisavalt andmekogu infoturbe reeglitest

23. Välistele andmesaajatele mõeldud dokumentides tuleks eraldi tähelepanu pöörata infoturbele ja isikuandmete kaitsele. Väliseid andmesaajaid võib olla väga erinevaid – alates suurtest riigiasutustest kuni väikeste KOVide ja erafirmadeni – ning nende erineva võimekuse tõttu ei saa alati loota nende endi infoturbe reeglistikule. KOVide küsitlemisel ilmnes, et vaid üksikutel on olemas asutusesisesed dokumendid, mis reguleerivad andmekaitset. Andmekogu vastutaval töötlejal tuleb pakkuda lisateavet just selle andmekogu reeglite kohta, sh kasutaja kohustuste ja õiguste ning olulisemate turvalisuse ja isikuandmete kaitse aspektide kohta, nagu kasutuse eesmärgipärasus ja minimaalsus, salasõnade haldus, kasutajatugi ja järelevalve. Ühe võimalusena võib andmekogu haldaja välise andmesaajaga sõlmitud lepingus kohustada iga uut andmekogu kasutajat enne juurdepääsude loomist tutvuma andmekogu kasutamist puudutavate õiguste ja kohustustega ning allkirjastama sellekohase dokumendi.

24. Andmekogude kasutamise turvalisus KOVide puhul põhineb eelkõige lepingutega võetud kohustuste täitmisel, sh ametniku vastutusel ja paroolide korrektsel kasutamisel. KOVide küsitlemisel ilmnes muu hulgas, et asutusesisesed salasõnade kasutamise reeglid olid kehtestanud ainult Viiratsi vald ja Tartu linn. Teised vallad ja linnad märkisid, et salasõnade kasutamist reguleerivad ainult andmekogudega sõlmitud

lepingud. Samas on iga andmetöötleja kohustus tagada töötlemise turvalisus ning ainult lepingutes sätestatu rakendamine ei ole piisav turvalise andmetöötlemise tagamiseks KOVides.

25. Auditi tulemusel leidsime, et andmekogude haldajate infoturbealane dokumentatsioon on üldjuhul olemas, kuid ebapiisav on dokumentatsiooni sidustatus. Infoturbealased dokumendid ei täida oma eesmärki ja isikuandmete kaitset ei ole võimalik tagada, kui inimesed ei tea juhendite olemasolust ega tunne neid.

26. Riigikontrolli soovitus auditeeritud andmekogude haldajatele: Korrastada andmekogude dokumentatsioon MKMi soovitustest lähtuvalt. Optimeerida ja viia üksteisega kooskõlla eraldi seisvad IT-korralduslikud dokumendid, arvestades asjaolu, et andmekogu kasutajal oleks hõlbus leida teda puudutavad infoturbealaseid juhendeid. Dokumentide sõnastamisel pidada silmas, et adressaatide ring on IT-valdkonna spetsialistidest laiem.

Majandus- ja Kommunikatsiooniministeerium ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega.

Haridus- ja teadusminister teatab, et vastav dokumentatsioon on ajakohastamisel ning on kättesaadav ministeeriumi autoriseeritud kasutajatele mõeldud veebilehelt.

Kaitseminister nõustub soovitusega.

Kaitseressursside Ameti peadirektor teatab, et käesolevaks ajaks on tehtud soovitus rakendatud ning kindlasti arvestab KRA seda ka edaspidi andmekogu dokumentatsiooni täiendamisel.

Maksu- ja Tolliameti peadirektor jätab soovituse osas oma seisukoha avaldamata.

Kodakondsus- ja Migratsiooniamet teatab, et Siseministeeriumi haldusala IKT on kavas konsolideerida Siseministeeriumi infotehnoloogia- ja arenduskeskusesse ning lisaks on, tulenevalt KMA liitmisest Politsei- ja Piirivalveameti koosseisu, vajalik korrastada ka haldusalas IT-alased dokumendid.

Regionaalminister teatab, et 2009. aasta alguses alustatakse olemasolevate infoturbe dokumentide analüüsiga. Analüüsi tulemust ja Riigikontrolli soovitusi arvesse võttes tehakse muudatused ja täiendused olemaolevatesse dokumentidesse.

Sotsiaalkindlustusameti peadirektor nõustub soovitusega ja teatab, et „uue infoturbepoliitika tegemisel järgitakse soovitust. Lähtuvalt punkti 18 vastusest edastame auditi soovitused Sotsiaalministeeriumile".

27. Riigikontrolli soovitus SKA-le: Kehtestada asutuses infoturbepoliitika.

Sotsiaalkindlustusameti peadirektor nõustub auditi soovitusega ning märgib, et: „SKAle on koostatud esimene infoturbe kontseptsioon 2000 a AS Cybernetica poolt. Uut infoturbepoliitika dokumenti hakati koostama 2005 a lõpus ning see jäi projekti staadiumisse. Seda ei jõutud

peadirektori käskkirjaga kinnitada seepärast, et enne jõuti teatavaks teha plaan infotehnoloogia teenuste halduse konsolideerimisest Sotsiaalministeeriumi valitsemisalas. Uus ja ühtne infoturbe poliitika koostatakse ISKE raames Sotsiaalministeeriumi poolt kõigile oma allasutustele. Auditi soovitused edastame Sotsiaalministeeriumile."

28. **Riigikontrolli soovitus auditeeritud KOVidele:** Täiendada sisekorraeeskirju või asjaajamiskorda IT osas või kehtestada arvutivõrgu ja infotehnoloogia kasutamise eeskirjad, mis muu hulgas hõlmaksid paroolihaldust ja järelevalve korraldust isikuandmete kaitse aspektist.

Ambla vald peab otstarbekaks esimesel võimalusel kehtestada ametiasutuse arvutivõrgu ja infotehnoloogia kasutamise eeskirjad, mis muu hulgas hõlmaksid paroolihaldust ja järelevalve korraldust isikuandmete kaitse aspektist, ning ajakohastada asutusesisesed muud dokumendid.

Anija vald on arvamusel, et vallavalitsuse sisekorraeeskirjas ning Siseministeeriumi ja AS Andmevaraga sõlmitud lepingus RRi kasutamiseks fikseeritud kohustused hoida saladuses salakoode ja paroole puudutav info on piisavad tagamaks isikuandmete töötlemine vastavalt isikuandmete kaitse seaduse nõuetele (valla vastuse täisteksti on võimalik lugeda tabelist lk 54).

Riigikontrolli kommentaar: Leiame, et sisekorraeeskirjas antud valdkonda reguleeriv lause „samuti tuleb saladuses hoida asutuse turvasüsteeme ning salakoode puudutav informatsioon" ei ole piisav. Lisaks ei laiene rahvastikuregistri kasutamiseks sõlmitud lepingus kajastatud paroolide ja kasutajatunnuste hoidmise reeglid valla üldisele infotöö korraldusele.

Antsla vald teatab, et kehtestab arvutivõrgu ja infotehnoloogia kasutamise eeskirja.

Audru vald ei esitanud vastamistähtaja ja täiendava nädala jooksul oma arvamust soovitusele.

Haapsalu linn peab soovitust asjakohaseks ning valmistab ette vajalike muudatuste sisseviimist sisekorraeeskirjadesse.

Jõhvi vald teatab, et neil on plaanis koostada arvutivõrgu ja infotehnoloogia kasutamise eeskirjad, mis muu hulgas hõlmaksid paroolihaldust ja järelevalve korraldust isikuandmete kaitse aspektist. Nimetatud eeskirja loodab ta kehtestada 2009. aasta esimesel poolaastal.

Kanepi vald teatab, et kehtestab arvutivõrgu ja infotehnoloogia kasutamise eeskirjad, mis hõlmavad paroolihaldust ja järelevalve korraldust.

Tapa vald lubab vallavalitsuses viia läbi toimingud hindamaks puudjääke vallavalitsuse seda valdkonda reguleerivas dokumentatsioonis ja arvestab riigikontrolli ettepanekuid nende täiendamisel.

Tõstamaa vald teatab, et väljatöötamisel on vallavalitsuse arvutivõrgu ja infotehnoloogia kasutamise eeskiri, mis sätestab paroolide kasutamise ning andmekogule juurdepääsu omava ametniku tööülesannete täitmise.

Tartu linn ja **Viiratsi vald** nõustuvad esitatud soovitusega.

Puka ja **Vigala vald** teatavad, et täiendavad oma asjaajamiskorda IT osas.

Torma ja **Jõelähtme vald** ei avalda oma seisukohta soovituse osas.

Infoturbealane töökorraldus tagab info liikumise ja üldjuhul ka vajalikud edasiarendused

29. Vastavalt IKSile tuleb isikuandmete kaitseks kasutusele võtta mh organisatsioonilised turvameetmed. Uurisime auditi käigus, kas asutustes on paika pandud infoturbe kavandamise ja töökorralduse reeglid, sh juhtkonna infoturbealase teavitamise, infotehniliste puuduste või riskide avastamise ja likvideerimise ning turvaintsidenti korral käitumise kohta.

Puuduste ilmnemisele turvameetmetes reageeritakse adekvaatselt

30. Juhtkonna regulaarset infoturbealast teavitamist peavad vajalikuks MKRi (kord poolaastas), LRi (kord nädalas), RRi (kord kuus) haldajad. Lisaks antakse juhtkonnale jooksvalt ülevaade toimunud turvaintsidentidest. Regulaarset aruandlust ei maininud PKR, EHIS ja ITDAK, kus teavitus on pigem intsidendipõhine. KTKR haldajail on plaanis juurutada regulaarne juhtkonna teavitamine käimasoleva ISKE rakendamise raames. Seni on iga-aastase riskide maandamise tegevuskava koostamise käigus juhtkonnale antud ülevaade ka infotehnoloogiaalastest probleemidest.

31. Ajavahemikku puuduste ilmnemisest kuni infosüsteemi paranduste sisseviimiseni pidas enamik andmekogude haldajatest rahuldavaks. Vaid PKRil ja EHISel on olnud probleeme töökindluse ja arenduste venimisega. EHISe esindajad möönsid, et infosüsteemi arendamisel on piirid seadnud ressursside nappus. Ka PKRi puhul viidati, et arendusotsuste tegemine ei toimu SKAs piisavalt kiiresti. Arendusi saab tellida praktiliselt korra aastas, kuid alati ei ole tagatud kasutajate hinnangul esmavajalike arendusprojektide sattumine vastutava töötleja prioriteetide hulka. Uuendused viibivad ka seetõttu, et toimub Sotsiaalministeeriumi valitsemisala asutuste IT-alane ühendamine. Lisaks on otsustatud olemasolevasse infosüsteemi parendusi mitte teha, kuna käimas on uue süsteemi loomine.

Infoturbealast reeglistikku ei uuendata regulaarselt

32. Kõikide andmekogude esindajad nentisid, et infoturbealaste dokumentide uuendamine toimub vastavalt vajadusele. Samas pole ühegi andmekogu puhul sätestatud, millise kindla ajavahemiku tagant on kohustus dokumente analüüsida, et vajaduse korral sisse viia asutuse loogilisest arengust tingitud muudatused. Kui Vabariigi Valitsuses kiidetakse heaks infosüsteemide turvameetmete süsteemi puudutava määruse muutmise eelnõu, mis näeb ette kohustuse auditeerida andmekogude turvameetmete rakendamist, siis sõltuvalt turbeastmest, tuleb läbi viia sõltumatu audit iga 2, 3 või 4 aasta tagant. See audit oleks üks võimalusi, mille käigus on süstemaatiliselt võimalik kontrollida ka muudatuste kajastamist ja dokumentatsiooni ajakohasust.

33. Auditis ilmnes, et PKR hooldamise ja haldamise eest vastutav ametnik ei ole andmekogu haldaja ametnike koosseisus, vaid see ametikoht viidi seoses struktuurimuudatustega SKAs ja Sotsiaalministeeriumi valitsemisala IT konsolideerimisega üle ministeeriumi koosseisu. Kuna PKRi puhul on nii vastutav kui ka

volitatud töötleja SKA, tulevad nimetatud ametniku tööülesanded peamiselt SKA juhtkonnalt. Leiame, et andmebaaside spetsialisti alluvussuhe sellisel kujul ei pruugi tagada andmebaaside infoturbe häireteta korraldust ning jätkusuutlikkust personalimuudatuste korral, sest selget vastutust andmekogu haldamise osas SKA ja Sotsiaalministeeriumi vahel pole kindlaks määratud.

Olemas on kord käitumiseks turvaintsidentide korral

34. Kõikide vaadeldud andmekogude infoturbealastes dokumentides või kasutuslepingutes olid olemas reeglid käitumiseks turvaintsidentide korral ning loodud on piisavad mehhanismid, et hoida asutuse juhtkonda kursis infoturbealaste küsimustega. Samuti võime kogutud andmete põhjal järeldada, et turvaintsidentidele reageeritakse adekvaatselt ning üldjuhul jõutakse ka vajalike edasiarendusteni, mis välistavad intsidentide kordumise. Samas ilmneb auditi järgnevatest peatükkidest, et ehkki on esinenud isikuandmete põhjendamatut kasutamist ning on vaja olnud teha järelevalvet, ei ole osa infosüsteeme piisavalt arendatud just IKSi nõuete seisukohalt (päringute logimine, andmetöötlemise põhjused).

35. Riigikontrolli soovitus SKA-le ja Sotsiaalministeeriumile: Leppida kokku vastutus PKRi haldamise, sh isikuandmete õiguspärase kasutamise järelevalve osas ning tagada selge tööjaotus ja infovahetus. Kuni vastutav töötleja on SKA, peaks ka andmekogu haldamisega seotud ametnikud kuuluma SKA koosseisu.

Sotsiaalkindlustusameti peadirektor nõustub auditi soovitusega ning märgib järgmist: „Juba 08.11.2007 tegi SKA ettepaneku Sotsiaalministeeriumile alustada läbirääkimisi tööjaotuse selgemaks muutmise osas. Hetkel on osapooled alustanud aktiivselt lahenduste otsimist auditiaruandes välja toodud vastutava ja volitatud töötleja märkuste lahendamiseks."

Sotsiaalminister teatas, et hetkel toimuvad Sotsiaalministeeriumi ja Sotsiaalkindlustusameti vahel töökoosolekud leppimaks kokku riikliku pensionikindlustuse registri tööjaotuse osas.

Andmeid töötlevate ametnike teadlikkus isikuandmete kaitse nõuetest on erinev

36. Infosüsteemi turvalisuse üks olulisemaid komponente on tema kasutajate teadlikkus infoturbe nõuetest. Audit soovis leida vastust küsimusele, kas ja mil moel on andmeid töötlevad ametnikud läbinud väljaõppe, mis käsitleb infoturvet ja isikuandmete kaitset. Samuti küsiti nende endi hinnangut selle väljaõppe piisavuse kohta.

Andmekaitsealane koolitus asutustes toimub

37. Enamik vaadeldud andmekogude haldajatest on isikuandmete kaitse alal oma asutuse ametnikke koolitanud. Vaid LR haldaja möönab, et andmekogu kasutajate koolitustel isikuandmete kaitse aspektile eraldi tähelepanu ei ole pööratud. Lisaks koolituste läbiviimisele on teadlikkuse tõstmiseks laialdaselt kasutusel tava, et uus töötaja pärast tutvumist oma ametiülesannete täitmist reguleerivate dokumentidega (sisekorraeeskirjade, ametijuhendi, infosüsteemi kasutajajuhendi, andmete kasutamise lepinguga) kinnitab allkirjaga, et on neist teadlik. MTAs on väljaõppesse panustatud sel määral, et valmimas on uute töötajate tarvis elektrooniline koolitusmoodul, mille abil töötaja teeb läbi koolituse, seejärel teda testitakse ja vastavalt tulemusele antakse talle juurdepääs infosüsteemidele. Samuti kontrollib KMA oma ametnike

teadmisi, enne kui neile võimaldatakse juurdepääs asutuse andmekogudele.

38. Enamik andmekogu haldajaid koolitab isikuandmete kaitse teemadel ainult oma ametnikke. Näiteks SKA teavitustegevus on suunatud oma asutuse sisestele kasutajatele ning eraldi teavituskampaaniaid välistele andmesaajatele ei organiseerita. Hea näide laiema vastutuse tajumisest ka väliste andmesaajate teadlikkuse tõstmisel on Siseministeerium, kes on tegelenud RRi kasutajate koolitamisega valla-, linna- ja maavalitsustes. Traditsiooniline on iga-aastane rahvastikuregistri seminar, kus järelevalve ja isikuandmete kaitse teema on alati päevakorras. Haridusasutustele on korraldanud koolitusi isikuandmete töötlemise valdkonnas AKI.

39. Kõik auditis vaadeldud KOVid olid veendunud, et nende ametnikud teavad piisavalt isikuandmete kaitse nõuetest. Enamik andmebaasidesse juurdepääsuõigust omavatest ametnikest on osalenud AKI, Siseministeeriumi, maavalitsuste või omavalitsusliitude korraldatud koolitustel. Samas, hoolimata nende poolt töödeldavatest delikaatsetest isikuandmetest, ei ole enamik KOVidest end AKIs töötlejatena registreerinud või määranud andmekaitse eest vastutavat isikut. Sellest ilmneb, et teadmised IKSist tulenevatest kohustustest pole ülevaatlikud.

Muudatused ja uuendused vajavad kasutajatele tutvustamist

40. Andmekogude haldajad on võtnud kasutusele meetmed kasutajate teadlikkuse tõstmiseks isikuandmete kaitse nõuete osas ning enda hinnangul on auditeeritavate asutuste ametnikud teadlikud isikuandmete kaitse nõuetest ja andmetöötluse mõistest. Infoturbe ja isikuandmete kaitse korraldus ei ole piisav, kui ametniku tööle asumisel talle allkirja vastu dokumente ainult tutvustada. Dokumendid ja töökorraldus võivad muutuda ning infoturbealaste muudatuste tutvustamiseks ja andmekaitsealaste kohustuste meeldetuletamiseks on mugavaim viis kasutada lahendust, kus infosüsteemi sisenemisel peab kasutaja kinnitama reeglitega tutvumist. Selline lahendus võimaldab ka kõiki andmekogu kasutajaid ilma suuremate jooksvate kulutusteta teavitada.

41. Riigikontrolli soovitus auditeeritud andmekogude haldajatele: Täiendada andmekogu kasutajatele mõeldud juhendeid isikuandmete kaitse reeglitega. Uue kasutaja esmasel sisenemisel andmekogusse on võimalik kuvada andmekogu kasutamisreeglite, sh isikuandmete kaitse alaste reeglite loetelu, millega kasutaja peab edasiste toimingute tegemiseks tutvuma ja nendega nõustuma. Samuti võib igakordsel sisenemisel andmekogusse tutvustada juhendites tehtud muudatusi ja kuvada meeldetuletust, et andmeid tohib kasutada konkreetsete tööülesannete täitmiseks.

Majandus- ja Kommunikatsiooniministeerium ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega.

Haridus- ja teadusminister teatab, et Haridus- ja Teadusministeerium lisas andmekogu kasutajaliidese juurde vastava juhendi isikuandmete töötlemise põhimõtetega. Arvestame ettepanekut ning loome vastava funktsionaalsuse menüü valiku ette, kus auditeeritav peab kinnitama teadete lugemist enne funktsionaalsuseni jõudmist.

Kaitseminister nõustub tehtud soovitusega.

Kaitseressursside Ameti peadirektor arvestab tehtud soovitusega 2009 aasta KTKR-i arendustööde teostamisel.

Maksu- ja Tolliameti peadirektor teatab, et „rakendusse logimisel ei ole otstarbekas kuvada põhjalikku selgitust kasutamisreeglite, s.h turvanõuete kohta. Ilmselt on lahenduseks uue töötaja värbamisel talle kohe allkirja vastu "Infosüsteemide kasutamise korra" tutvustamine".

Riigikontrolli kommentaar: Riigikontroll nõustub, et uue töötaja värbamisel tuleb talle allkirja vastu tutvustada tema tööd puudutavaid eeskirju, kuid leiab, et nende dokumentide väiksemahuliste muudatuste või täienduste tutvustamine ja andmekaitse reeglite perioodiline meenutamine ning nendega tutvumise kohta kinnituste kogumine on kõigile osapooltele lihtsam andmekogusse sisselogimisel, kuna see on nende igapäevane töövahend.

Kodakondsus- ja Migratsiooniamet teatab, et „2009. a eelarve ja investeeringute vähendamise tõttu on KMAs suunatud arendustööd nendesse valdkondadesse, mis on prioriteetsete põhiülesannetena määratletud (VIS, SIS, biomeetria rakendamine jne), ning lisaks meetmetele, mis on seotud andmebaaside ja infosüsteemide teenustaseme säilitamiseks või olemasolevate lepinguliste kohustuste täitmiseks. Kuid KMA viib regulaarselt läbi andmekaitsealaseid koolitusi, millega tagatakse andmekogu kasutajate teadlikkus andmekaitsealastest reeglitest."

Regionaalminister teatab, et „vastavalt kasutatavale infotehnoloogilisele lahendusele ilmub rahvastikuregistrile juurdepääsu soovivale kasutajale ekraanile teavitustekst, kus on toodud ära andmete kasutamise ainukese eesmärgina ametiülesannete täitmine, samuti teavitatakse kasutajaid sellest, et registri kasutamise üle teostatakse järelevalvet. Samuti saavad kõik registri uued kasutajad AS-lt Andmevara suulised instruktsioonid enne kasutajaõiguste üleandmist. Uue tarkvara valmimisel on võimalik seda teksti täiendada ja lisada täiendav informatsioon juhendi näol".

Sotsiaalkindlustusameti peadirektor nõustub soovitusega ning märgib, et „SKAs on määratud isikuandmete kaitse eest vastutav isik, kes teostab järelevalvet isikuandmete kaitse seaduse, avaliku teabe seaduse ja ametis kehtestatud juhendite ning kordade üle. Lisaks teeb ta vähemalt korra aastas igas regioonis ühe andmekaitsealase sisekoolituse. Iga kahe nädala tagant koguneval juhtkonna koosolekul juhib ta juhtide tähelepanu asjaoludele, millele tuleb tähelepanu pöörata. Samuti toimub infosüsteemide paroolide kättejagamisel õiguste ja kohustuste tutvustamine. Füüsiliste ja organisatsiooniliste turvameetmete täiustamine leiab aset infoturbepoliitika koostamisel Sotsiaalministeeriumi poolt. Auditi soovitused edastame Sotsiaalministeeriumile."

Delikaatsete isikuandmete töötlemise registreerimisel on puudujääke

42. Euroopa Liidu direktiivi 95/46/EÜ artiklis 18 on sätestatud andmetöötleja kohustus teavitada delikaatsete isikuandmete töötlemisest oma riigi järelevalveasutust, kes seejärel töötlejate nimekirja avalikustab.

Selle direktiivi artikkel 29 alusel moodustatud töögrupi raportist18 ilmneb, et järelevalveasutuse teavitamisel isikuandmete töötlemisest on kolm peamist eesmärki:

- see aitab isikutel, kelle andmeid töödeldakse, saada ülevaadet isikuandmete töötlejatest,
- aitab andmetetöötlejail hoida end kursis andmekaitse nõuetega ning
- aitab andmekaitsega tegelevat järelevalveorganit, võimaldades olla kursis andmete töötlemise seisuga oma riigis.

Viimane eesmärk võimaldab järelevalveasutusel paremini analüüsida kitsaskohti ja seada prioriteete oma tegevustele isikuandmete kaitse tagamisel.

43. IKS paneb kõigile isikutele ja asutustele kohustuse registreerida delikaatsete isikuandmete töötlemine AKIs. Delikaatsete isikuandmete töötlemist ei pea registreerima üksnes juhul, kui asutuses on määratud isikuandmete kaitse eest vastutav isik. Kui delikaatsete isikuandmete töötlemine ei ole AKIs registreeritud või ei ole määratud andmekaitse eest vastutavat isikut ja sellest AKIt teavitatud, on selliste andmete töötlemine ebaseaduslik. AKI võib keelduda delikaatsete isikuandmete töötlemise registreerimisest muu hulgas juhul, kui rakendatud isikuandmete organisatsioonilised, füüsilised ja infotehnilised turvameetmed ei taga IKSi § 25 sätestatud nõuete täitmist. Seaduse säärane sõnastus eeldab, et AKI veendub enne registreerimist selles, et töötlemisele rakendatavad turvameetmed tagavad IKSi täitmise. Registreering peab andma kindlustunde nii üksikisikutele kui ka andmekogude haldajatele, et organisatsiooni andmetöötlus on turvaline ja vastab andmekaitse nõuetele.

Vastutavad ja volitatud töötlejad on AKIs registreeritud

44. Vaadeldud seitsmest andmekogust kuus (v. a MKR) sisaldavad delikaatseid isikuandmeid ning nende haldajad on registreerinud delikaatsete isikuandmete töötlemise AKIs. Lisaks on SKA ja KMA määranud isikuandmete kaitse eest vastutava isiku.

45. Registreerimisotsuse tegemiseks ei piisa alati turvameetmeid kirjeldavate dokumentide analüüsist. Selle näiteks on EHISe andmeid dubleeriva delikaatseid isikuandmeid sisaldava keskkonna mittesihipärane kasutuselevõtt HTMis (vt p 52), mille olemasolu AKI-le esitatud dokumentatsioonis ei kajastu. Pisteliselt ja suurema riskiastmega andmekogude puhul võib osutuda vajalikuks andmekogu turvameetmete rakendamist ja vastavust IKSile ka reaalselt kontrollida.

46. Registreerimise üks eesmärkidest on aidata kaasa, et andmetöötlejate teadlikkus isikuandmete kaitse nõuete kohta kasvaks. Registreerimiskohustus on kõigil delikaatsete isikuandmete töötlejatel ja seetõttu peaksid andmekogude vastutavad töötlejad enne delikaatsetele

[18] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp106_en.pdf lk 6.

isikuandmetele juurdepääsu võimaldamist veenduma, et välised andmesaajad on saanud õiguse delikaatsete isikuandmete töötlemiseks.

Välised andmesaajad registreerivad end AKIs harva

47. Auditi käigus selgus, et PKRil on kasutajad KOVide ning EHISel KOVidele lisaks ka haridusasutuste näol, kel on juurdepääs delikaatsetele isikuandmetele, kuid nad pole enamasti registreeritud delikaatsete isikuandmete töötlejatena või ei ole teavitanud AKIt andmekaitse eest vastutava isiku määramisest. Nii oli 2008. a aprilli seisuga AKIs registreeritud vaid 14 haridusasutust sadadest omataolistest ning 11 KOVi 227st. EHISe vastutavad töötlejad on korduvalt informeerinud kasutajaid registreerimise vajadusest. Üleskutsega teha korda isikuandmete töötlemise alane dokumentatsioon pöördus käesoleva aasta mais Õpetajate Lehe vahendusel koolide poole ka AKI. Oktoobri alguse seisuga on registreeritute ja vastutava isiku määranute nimekirja lisandunud 52 haridusasutust ning 7 valda ja linna.

48. Delikaatsete isikuandmete töötlemise registreerimist on pärssinud AKI seisukoht, et kõik riigi- ja kohaliku omavalitsuse asutused, kellele on loodud juurdepääs andmekogule, on isikuandmete volitatud töötlejad. IKS § 27 lg 1 sätestatu kohaselt esitab vastutav töötleja delikaatsete isikuandmete töötlemise registreerimistaotluse ka volitatud töötleja eest. AKI tõlgenduse kohaselt peaksid näiteks registreerimistaotluse KOVide nimel dubleerivalt esitama vähemalt Siseministeerium, SKA ja HTM kui vaadeldud andmekogude vastutavad töötlejad. Kuna tegelikult on KOVid ja teised lepingutega andmekogule juurdepääsu saanud asutused IKSi mõistes kolmandad isikud, siis tuleb taotlus delikaatsete isikuandmete töötlemiseks AKI-le esitada neil endil.

49. 2008. a algul muudeti isikut tõendavate dokumentide seadust ning lisati biomeetriliste andmete hulka allkirja- ning näokujutis. Seega sisaldab ITDAK delikaatseid isikuandmeid, mida väljastatakse lepingute alusel välistele andmesaajatele ilma eelneva veendumiseta selles, et viimastel on delikaatsete andmete töötlemiseks kasutusel piisavad turvameetmed. Intervjuu käigus kinnitati, et kuna andmekogus toimuvad sel aastal ümberkorraldused, siis on kavas lepingud samuti üle vaadata ning kontrollida, kas kõikidel andmekasutajatel on delikaatsete isikuandmete töötlemiseks luba või kas on määratud isikuandmete kaitse eest vastutav isik.

50. Väliste andmesaajate registreerimist delikaatsete isikuandmete töötlejana on valitud andmekogudest seni kontrollitud ainult KTKRi puhul, mille eeliseks võrreldes teiste andmekogudega on väliste andmesaajate väike hulk. Arstlikele komisjonidele KTKRi juurdepääsuõiguse andmise otsustamisel oli registreeringu olemasolu üks eeltingimusi ning oli juhtumeid, mille puhul Kaitseministeerium ja KRA piirasid kasutajate juurdepääsu delikaatsetele isikuandmetele kuni nad polnud töötlemist registreerinud.

51. Riigikontroll tegi kindlaks, et SKA ei luba välistele andmesaajatele otsejuurdepääsu PKR andmetele, vaid on nende jaoks loonud eraldi andmekogu, kuhu tõstetakse uuendatud andmed kord nädalas ja mida KOVid kasutavad X-tee vahendusel. KOVide ametnikud pääsevad ligi ainult oma valla või linna (Tallinnas linnaosa) elanike andmetele. Selline lahendus on tekkinud, kuna PKRi andmeid on KOVidel vaja sotsiaalhoolekande juhtimise ja korraldamise ülesannete täitmiseks ning andmed kantakse üle riikliku sotsiaalregistri hajutatud registrisse, mis

koosneb valla- ja linnavalitsustes peetavatest kohalikest sotsiaalregistritest. Mitmeid aastaid tagasi Sotsiaalministeeriumi ja SKA poolt ning AKI nõusolekul ajutiselt kasutusele võetud lahendus andmete edastamiseks ei ole kooskõlas praegu kasutatavate tehniliste lahendustega ega infoühiskonna arengukavaga. SKA ei ole PKRi kõrvale täiendavalt tekitatud delikaatseid isikuandmeid sisaldavat andmekogu AKIs registreerinud ega kehtestanud sellele andmekogule eraldi infoturbealaseid nõudmisi.

52. HTM haldas EHISes paralleelselt kahte identset reaalsete isikuandmetega registrit, millele mõlemale on kasutajatel põhimõtteliselt juurdepääs olemas. Teise keskkonna eesmärk oli andmete kvaliteedi kontroll enne nn pärisbaasi ülekandmist. Samas delikaatsete isikuandmete kasutamine andmete kvaliteedi testimiseks ei ole andmete eesmärgipärane kasutus. Paralleelne keskkond suleti osaliselt 2008. a mais pärast vastavasisulist ettekirjutust AKI poolt ning HTM kinnitas, et 11. novembriks 2008. a testkeskkonda isikuandmeid loetaval kujul ei jää ja edaspidi üle ei kanta.

53. Riigikontroll on veendunud, et andmete peegeldamine eraldi andmebaasi või dubleerivasse keskkonda sama andmebaasi sees on põhjendamatu, sest muudab keerukamaks andmekogu haldamise ja isikuandmete kaitse.

54. Vaadeldud andmekogude näitel selgus, et enamjaolt pole välised andmesaajad määranud isikuandmete kaitse eest vastutavat isikut ega registreerinud end delikaatsete isikuandmete töötlejana, mistõttu ei ole AKI saanud anda kinnitust, et delikaatseid isikuandmeid töödeldakse turvaliselt. Ka andmekogude haldajad ise ei kontrolli üldjuhul juurdepääsude loomisel välise andmesaaja õigust delikaatsete isikuandmete töötlemiseks. Seega puudub veendumus, et on tagatud turvaline isikuandmete töötlemine.

55. Riigikontrolli soovitus AKI-le:

- Viia läbi delikaatseid isikuandmeid sisaldavate andmekogude haldajate riskianalüüs ning suurema riskitasemega andmekogude haldajate juures kontrollida isikuandmete kaitse nõuete järgimist ka kohapeal.

- Tõhustada teavitustööd ning võtta kasutusele täiendavaid meetmeid (juhendite koostamine, vajaduse korral väärteomenetluse algatamine) selleks, et haridusasutused ning valla- ja linnavalitsused, kes juba töötlevad delikaatseid isikuandmeid, oleksid teadlikud neile kehtivatest isikuandmete kaitse nõuetest, registreeriksid end delikaatsete isikuandmete töötlejatena ning tegelikkuses tagaksid delikaatseid isikuandmeid sisaldavate andmekogude ja nende kasutamise piisava turvalisuse.

Andmekaitse Inspektsiooni peadirektor teatab, et Andmekaitse Inspektsioon analüüsib põhjalikult talle tehtud ettepanekuid juhendite väljatöötamiseks ja vajaduse korral lülitab need 2009. aasta tööplaani.

56. Riigikontrolli soovitus SKA-le: Lõpetada registreerimata dubleeriva andmekogu pidamine ning tagada välistele andmesaajatele nende

seadusest tulenevate või seaduse alusel pandud kohustuste täitmiseks vajalik juurdepääs andmetele teiste lahenduste kaudu.

Sotsiaalkindlustusameti peadirektor ei nõustu soovitusega ja selgitab, et: „SKA ühines X-teega kui Eesti riigi põhilisi andmebaase ühendava turvalise andmevahetuskihiga juba 2002. a, olles üks esimesi X-teega ühinenud riigiasutusi. X-tee päringute teostamise tehnoloogia realiseeriti selle tarbeks spetsiaalsete andmetabelite moodustamise teel. Sellise tehnoloogia kasutamise eesmärgiks oli võimalikult kiiresti vastata teise ametkonna päringutele, tagamaks sellejuures registri andmete turvalisus. X-teele välja kantud andmeid võiks võrrelda andmeaidaga, kus välja ei kanta kogu online baasi infot, vaid antud eesmärgi huvides korrastatud infot. Nagu andmeait, nii ei ole ka X-teele välja kantud info kasutajate poolt muudetav, vaid ette nähtud üksnes päringute teostamiseks. X-teele andmete väljakandmise puhul ei tehta andmete lisamist, vaid vanad andmed kustutatakse. Sellest nähtub väga täpselt, et ei ole tegemist eraldi andmekoguga, vaid on kuuajalise väljavõttega vahetabelid."

Riigikontrolli kommentaar: Vastavalt avaliku teabe seaduse § 43[1] nimetatakse andmekoguks korrastatud andmete kogumit, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks. Ka regulaarselt ajakohastatavat väljavõtet PKRi andmebaasist tuleb käsitleda kui andmekogu.

57. Riigikontrolli soovitus HTMile: Lõpetada reaalsete isikuandmetega dubleeriva keskkonna kasutamine EHISes.

Haridus- ja teadusminister teatab, et alates 01.11.2008 a on Haridus- ja Teadusministeerium lõpetanud reaalsete isikuandmete töötlemise EHISe arenduskeskkonnas.

58. Riigikontrolli soovitus auditeeritud andmekogude (v.a MKR ja KTKR) haldajatele: Enne andmekogu delikaatsetele isikuandmetele juurdepääsu lubamist kontrollida, kas juurdepääsu taotleja on määranud isikuandmete kaitse eest vastutava isiku või registreerinud end AKIs delikaatsete isikuandmete töötlejana.

Majandus- ja Kommunikatsiooniministeerium ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega.

Haridus- ja teadusminister teatab, et täiendab protseduurireegleid uute kasutajate lisamisel. Vastav funktsionaalsus luuakse asutuse administraatori juurde rolli lisamise alla.

Kodakondsus- ja Migratsiooniamet teatab, et „KMA hinnangul IKS-ist ei tulene, et kõigil andmete töötlejatel on kohustus registreerida delikaatsete isikuandmete töötlemine, vaid selline kohustus on pandud vastutavale töötlejale.

IKS-i eelnõu seletuskirjas on selgitatud järgnevalt: „erinevalt kehtinud IKS-ist on eelnõus endise pideva vastutava töötleja ja volitatud töötleja eristamise asemel räägitud üldisest isikuandmete töötlejast. Vastutava ja volitatud töötleja eristamisest siiski täielikult loobuda ei ole olnud võimalik, sest mõningad kohustused IKS-is kehtivad üksnes vastutava töötleja suhtes, nt on delikaatsete isikuandmete töötlemise AKI-s

kohustatud registreerima vastutav töötleja, mitte aga volitatud töötleja (§ 27 lg 1), kes töötleb isikuandmeid vastutava töötleja järelevalve all, kusjuures vastutav töötleja ei vabane vastutusest nende isikuandmete töötlemise eest.“ IKS § 7 lg 3 annab volitatud töötlejale definitsiooni: 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. Antud selgitus viitab asjaolule, et volitatud/välised töötlejad (sh lepingulised töötlejad) ei ole kohustatud delikaatsete isikuandmete töötlemist registreerima AKI-s.”

Riigikontrolli kommentaar: Andmekogu vastutaval töötlejal on kohustus registreerida endapoolne delikaatsete isikuandmete töötlemine. Kui vastutav töötleja on andmekogule määranud volitatud töötleja, siis peab eelnimetatud töötlemise taotluse volitatud töötleja eest esitama vastutav töötleja. See ei vabasta delikaatsete isikuandmete registreerimise kohustusest väliseid andmesaajaid ehk IKSi mõistes kolmandaid isikuid, kes peavad ise registreerima delikaatsete isikuandmete töötlemise või määrama isikuandmete kaitse eest vastutava isiku.

Regionaalminister teatab, et „enne juurdepääsuõiguste andmist delikaatsele isikuandmetele kontrollitakse Siseministeeriumi poolt alati, kas kasutaja vastab selliste andmete töötlemiseks õiguse saamise tingimustele. Kui kasutaja nimetatud tingimustele ei vasta, siis juurdepääsu ei anta enne, kui vastavad õigused on AKI-lt saadud“.

Sotsiaalkindlustusameti peadirektor nõustub soovitusega ja selgitab, et „delikaatsete isikuandmete päringute puhul, mida ei soorita KOVid, teostab Sotsiaalkindlustusameti andmekaitse peaspetsialist alati kontrolli AKI kodulehel olevast registrist, kas päringut sooritav asutus on end registreerinud delikaatsete isikuandmete töötlejana”.

59. Riigikontrolli soovitus auditeeritud KOVidele (v.a Tartu linn ning Puka ja Vigala vald): Kindlustada delikaatsete isikuandmete töötlemise vastavus IKSile ja registreerida selleks delikaatsete isikuandmete töötlemine AKIs või määrata isikuandmete kaitse eest vastutav isik.

Ambla vald teatab, et kindlustamaks delikaatsete isikuandmete töötlemise vastavus IKSile, registreerivad nad esimesel võimalusel KOVi delikaatsete isikuandmete töötlejana AKIs.

Anija vald teatab, et on vastavalt isikuandmete kaitse seaduse § 27 ja § 30 isikuandmete kaitse eest vastutavaks isikuks määranud registripidaja, mille kohta on vormistatud vallavanema käskkiri 17.11.2008 nr 193.

Antsla vald nõustub soovitusega ja teatab, et valmistab ette dokumente AKIs registreerimiseks. Lisaks valmistab vald, koostöös maakonna IT spetsialisti abiga kogu maakonna omavalitsustele, ette dokumentatsiooni ISKE nõuete täitmiseks.

Audru vald ei esitanud vastamistähtaja ja täiendava nädala jooksul oma arvamust soovitusele.

Haapsalu linn teatab, et on alustatud eeltöid isikuandmete kaitse eest vastutava isiku määramiseks.

Jõelähtme vald teatab, et on alustanud toiminguid Jõelähtme Vallavalitsuse registreerimiseks AKIs delikaatsete isikuandmete töötlejana.

Jõhvi vald teatab, et alustas vastava taotluse koostamisega nii vallavalitsuse kui ka hallatavate asutuste registreerimiseks AKIs. Taotluse plaanitakse esitada veel 2008. aastal.

Kanepi vald teatab, et Kanepi Vallavalitsuse 07.11.2008. a korraldusega nr 228 on määratud isikuandmete kaitse eest vastutav isik.

Tapa vald teatab, et viib läbi hindamise, kas vallavalitsusele, lähtuvalt vallavalitsuse haldussuutlikkusest ja delikaatsete isikuandmete töötlemise mahust, on otstarbekam registreerida delikaatsete isikuandmete töötlemine AKIs või määrata isikuandmete kaitse eest vastatav isik. Otsuse tegemine IKSi vastava regulatsiooni täitmiseks on võimalik pärast vastava hindamise läbiviimist.

Torma vald avaldab, et delikaatsete isikuandmete töölemise registreerimine AKIs peaks olema üheselt mõistetav – kas registreerimise taotluse esitab RR kohta KOV või Siseministeerium.

Riigikontrolli kommentaar: Valla näol on IKSi mõistes tegemist kolmanda isikuga, kellele antakse juurdepääs rahvastikuregistrile. Sel juhul peab delikaatsete isikuandmete töötlemise või isikuandmete kaitse eest vastutava isiku määrama vald. Kui see ülesanne oleks Siseministeeriumil, siis peaks viimane kontrollima kõigi KOVide vastavust IKSi nõuetele. See ei ole kõikide kolmandate isikute osas mõeldav ega otstarbekas.

Tõstamaa vald teatab, et nad registreerivad isikuandmete töötlemise AKIs vastavalt kehtivale seadusandlusele.

Viiratsi vald nõustub soovitusega.

Asutuses rakendatavad sisekontrollimehhanismid

60. IKSi § 25 lg 1 kohustab isikuandmete töötlejat võtma kasutusele organisatsioonilised, füüsilised ja infotehnoloogilised turvameetmed isikuandmete kaitseks. Käesoleva peatüki fookuses on küsimus, kuidas on andmekogude puhul korraldatud sisekontroll, mis tagaks eesmärgipärase andmetöötlemise ja välistaks kõrvaliste isikute juurdepääsu isikuandmetele. Sisekontrolli elementidest keskenduti järgnevatele:

- Kas ametnike juurdepääsuõigused andmekogudele on dokumenteeritud ja volitamata juurdepääs infotehnoloogiliselt välistatud?
- Kas tagantjärele on võimalik kindlaks teha, kelle poolt ja millistele isikuandmetele andmetöötlussüsteemis juurdepääs saadi? Kas kõigist neist elektroonilistest toimingutest on võimalik talletada jälg, s. o logi?
- Kas andmekogu vastutav töötleja analüüsib regulaarselt nii oma asutuse kui ka väliste andmesaajate puhul isikuandmete päringuid ning andmete muutmisi?

Päring on andmete väljastamiseks tingimuste loetelu edastamine andmekogusse. Päringu tulemusel saadakse päringuvastus.

61. Rõhutada tuleb iga andmekasutaja, mitte ainult vastutava töötleja vastutust selle eest, et andmekogus olevaid andmeid ei vaadata, muudeta, edastata ega töödelda muul viisil ebaseaduslikult. Lisaks IKSile reguleerivad andmekasutajate vastutust andmekogule juurdepääsu võimaldavad lepingud ja üldjuhul ka asutuste sisekorraeeskirjad. Kuigi asutusel, kelle ülesandeid päringu tegija täidab, on täpseim ülevaade päringute põhjendatusest, on ka andmekogu vastutaval töötlejal kohustus teha järelevalvet kõigi andmekasutajate päringute ja andmete muudatuste põhjendatuse üle.

Ametijuhendites ei kajastu juurdepääsuvajadus andmekogudele

Olulisemad organisatsioonilised meetmed:

- õige tööülesannete jaotus infosüsteemi haldamisel;
- mõistlik juurdepääsude reguleerimine;
- paroolide turvaline kasutamine;
- efektiivne andmeturbe nõuete täitmise kontroll.

62. Vastavalt IKSi § 25 lg 2 p 4 on isikuandmete töötleja kohustatud tagama, et igal andmetöötlussüsteemi kasutajal oleks juurdepääs isikuandmetele vaid selles ulatuses, mis on tema tööülesannete täitmiseks vajalik. Kirjalikult tuleb jäädvustada see, kellel, millise aja vältel ja millistele andmetele juurdepääsuks on õigus infosüsteemi siseneda. Nõnda on võimalik tagantjärele andmete kasutamise õiguspärasust kontrollida. Selline kirjapanek juba iseenesest aitab teadvustada nii juurdepääsu andja kui saaja vastutust ning iga juurdepääsu saaja juurdepääsuvajadus kaalutakse põhjalikult läbi. Ka ISKE meede M2.1[19] näeb ette, et kehtestatakse infosüsteemide kasutajate vastutus ja reeglid, ning meede M2.5, et juurdepääsuõiguste andmine dokumenteeritakse. X-tee kaudu andmekogusid kasutav asutus on kohustatud määrama isikud, kellel on õigus, või ameti- ja töökohad, millel töötamisega kaasneb õigus esitada päringuid X-tee kaudu[20].

[19] Allikas: http://www.ria.ee/28949.

[20] Vt https://www.riigiteataja.ee/ert/act.jsp?&id=12956835 § 15 lg 4.

Enamasti on andmekogudele juurdepääsu ulatus põhjendatud

63. Auditi käigus selgus, et PKRi ja ITDAKi puhul on ametnike ülesanded vastavuses nende kasutajarollidega andmekogudes. AS Andmevara töötajatel on kasutusel nn juurdepääsukaart, kus kajastub RRile ligipääsu ulatus, kestus ja põhjus. Teiste andmekogude puhul ning RRi kasutavate Siseministeeriumi ametnike kohta oli võimalik infosüsteemist teha väljavõte juurdepääsuõiguste kohta, kuid asutuse sisedokumentides olid ametiülesanded ja juurdepääsuõigused omavahel sidumata.

64. Auditeeritavatel andmekogudel olid olemas protseduurid, kuidas kindlaks teha andmetele juurdepääsu põhjendatus. Uue juurdepääsuõiguse saamiseks või olemasolevate õiguste muutmiseks on andmekogude valdajate juures loodud astmeline süsteem, kus vahetu ülemus koostab või kinnitab juurdepääsu taotluse ning selle loomise põhjendatust hindab ka juurdepääsuõigusi vormistav taotlejast sõltumatu üksus. Viimane võrdleb taotluses toodud aluseid ka ametijuhendites kirjeldatud tööülesannetega. Siiski ilmnes, et mitmel juhul olid tööülesanded juhendis kirjeldatud väga üldiselt ning nende põhjal oli raske kindlaks teha täpset vajaminevate andmete ulatust.

65. ITDAK paistis silma põhjalikkusega juurdepääsuõiguste määramisel. Juurdepääsu vajaduse andmekogule otsustab vahetu ülemus lähtuvalt ametnikule antavatest volitustest. On algatatud volituste sidumine piiratud andmehulkadega andmekogu sees. Kõigi ametnike detailseid juurdepääsuõigusi sisaldavat käskkirja on kohustus uuendada kord poolaastas, praktikas aga on osutunud vajalikuks käskkirja uuendamine iga mõne nädala tagant, mistõttu käskkirja kinnitajatel on tõenäoliselt koormav jälgida igakordsete muudatuste mahtu või põhjendatust.

66. Problemaatilisem on juurdepääsuõiguste administreerimine väliste andmesaajate juures. Praktikas antakse juurdepääs päringuid tegevale asutusele või äriühingule, kes ise otsustab oma töötajate juurdepääsuõigused. Nii on see lahendatud ka X-tee puhul ja enamasti see ongi mõistlik, sest näiteks RRi andmeid kasutab sadu asutusi ja juriidilisi isikuid, kelle mitme tuhande ametniku ja töötaja juurdepääsuõiguse üle otsustamine käiks Siseministeeriumile objektiivselt üle jõu. Teiselt poolt säilib vastutava töötleja kohustus kindlustada isikuandmete töötlemise õiguspärasus. Selleks on vaja omada ülevaadet juurdepääsu põhjendatusest ja kõigist kasutajatest. Piisavaks saab pidada RRi puhul kasutusel olevat skeemi, kus välised andmesaajad pöörduvad esmalt taotlusega vastutava töötleja ehk Siseministeeriumi poole, kes kaalub taotluse põhjendatust, enne kui luuakse juurdepääs ja sõlmitakse andmekasutuse leping, mille lisades märgitakse vajaduse korral ka kõigi andmekogule juurdepääsuõigusega isikute nimed.

67. Auditi raames selgus, et kõigil KOVidel on võimalik, viidates toimetulekutaotluste põhjendatuse kontrollimisele sotsiaalhoolekande seaduse § 22^1 lg 3^2 p 2 alusel, taotleda juurdepääsu liiklusregistrile. Samas oli viieteistkümnest auditis vaadeldud KOVist seda teinud vaid 4 (vt lisa A), kusjuures üks KOV (Antsla) oli küll juurdepääsuõigused saanud, kuid ei ole enam kui aasta jooksul teinud ühtegi päringut. Samuti olid MKR andmetele juurdepääsuõigused kahel (Jõelähtme ja Tapa) vallal, mis ei olnud esitanud ühtegi päringut. Seega ilmneb, et andmekogu vastutava töötleja huvides on juurdepääsutingimuste

sätestamine kujul, mis tagab õiguse juurdepääs teatud aja möödudes andmekaitse huvides sulgeda, kui andmekogu ei kasutata.

68. Riigikontroll tuvastas pisteliste testide käigus, et seitsmest andmekogust kahe puhul ei olnud võimalik kindlaks teha, kas dokumenteeritud juurdepääsuõigused ühtisid ametnike tegelike õigustega. KTKRi puhul test tulemust ei andnud, kuna puudus dokument juurdepääsuõiguste kohta, mida saanuks ametiülesannetega võrrelda.

Esines vastuolusid juurdepääsuõigusi kirjeldavas dokumentatsioonis

69. PKRi puhul tuvastati, et juurdepääsuõigusi kirjeldav dokument oli mõnes kontrollitud lõigus aegunud ega vastanud tegelikkusele. Vastavalt dokumendile "Sotsiaalkindlustusameti teenistujate juurdepääs SKA andmekogudele" on peaspetsialistil õigus ainult lugeda klassifikaatorite andmeid. Testiga selgus, et peaspetsialistil on õigus klassifikaatorite andmeid lisaks lugemisele ka muuta ja klassifikaatoreid luua. Peaspetsialisti enda selgituse kohaselt on see ka tema ametijuhendist tulenev ülesanne. Seega on PKRile juurdepääse kirjeldav dokument testitud ametniku ametijuhendis sisalduvate ülesannete ja tema igapäevatööga vastuolus. Ajakohastamata on ka ametikohtade nimetused SKA infoturbealastes dokumentides. Näiteks andmebaaside peaadministraatori ametikoht kadus struktuurireformi käigus 2007. aastal ja tegelikult täidab nimetatud ametikoha ülesandeid Sotsiaalministeeriumi peaspetsialist, kuid dokumentides on endiselt ülesandeid jagatud SKA andmebaaside peaadministraatorile.

70. Kasutajaõiguste põhjendatuse kontrolli takistab SKAs huvide konflikt alluvussuhetes, kuna juurdepääse PKRile jagavad ametnikele osaliselt pensioniametite peaspetsialistid, kes alluvad vahetult pensioniameti juhile. Nii tekib olukord, kus peaspetsialistil lasub kohustus täita vahetu juhi korraldust ja ta ei saa täita talle pandud sõltumatu järelevalvaja rolli juurdepääsude jagamisel.

71. Otsustamismenetlus konkreetsetele töötajatele isikuandmetele juurdepääsu võimaldamiseks on vaadeldud andmekogude puhul olemas ja üldjuhul usaldusväärne. Samas ei ole juurdepääsuõigused enamjaolt kuigi detailselt dokumenteeritud (kellel, mis aja vältel, millistele andmetele ja mis eesmärgil juurdepääs on), kuigi ametijuhenditest on võimalik üldjuhul tuletada tööks tarvilike andmekogude juurdepääsuvajadus ja andmete hulk.

72. **Riigikontrolli soovitus auditeeritud andmekogude haldajatele**: Vaadata üle andmekogude juurdepääsuõigusi ja tööülesandeid kirjeldavad dokumendid asutuses (näiteks ametijuhendid) nii, et neist ilmneks andmekogudele juurdepääsuõiguse vajadus ja selle ulatus.

Majandus- ja Kommunikatsiooniministeerium ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega.

Haridus- ja teadusminister nõustub soovitusega.

Kaitseminister ja **Kaitseressursside Ameti peadirektor** nõustuvad soovitusega.

Maksu- ja Tolliameti peadirektor teatab, et „andmekogule juurdepääsuõiguse taotluses on ametniku vahetul ülemusel kohustuslik märkida kasutajagrupp (õiguste ulatus), juurdepääsu ajaline periood ja

kasutamise põhjendus (vajadus). Ametijuhenditesse andmekogude ja nende kasutajagruppide sissekirjutamist ei pea otstarbekaks, kuna siis tuleks suurema osa ametnike ametijuhendeid suhteliselt sageli muuta“.

Kodakondsus- ja Migratsiooniamet teatab, et „ametisiseselt on ametnikele ITDAK-le juurdepääsuõiguse andmine reguleeritud käskkirjaga, milles on ette nähtud protsess volituse saamiseks ning lõpetamiseks ja sama käskkirjaga peetakse ka ülevaadet kõigist olemasolevatest ametisisestest volitustest.

Ametivälised juurdepääsud avatakse eeldusel, et vastav asutus on teinud taotluse KMA-le ning et neil on olemas seaduslik alus andmete töötlemiseks. Enne andmevahetuse avamist teeb KMA analüüsi, kas taotleval asutusel on õiguslik alus olemas ning kas taotluses soovitud andmehulk vastab eelkõige eesmärgipärasuse ja minimaalsuse põhimõtetele ning milline tehniline lahendus on vajalik/võimalik. Kui kõik eelnev on korras, siis tehakse taotlevale asutusele ettepanek reguleerida andmevahetus lepinguga ning ühtlasi sätestab KMA nõuded andmete töötlemiseks nimetatud lepingus (sh pidada arvestust volituste üle ja ka KMA pädevuse teha järelevalvet andmete töötlemise üle)“.

Regionaalminister teatab, et Siseministeerium vaatab üle kõigi oma asutuse siseste kasutajate ametijuhendid ja täpsustab neid juurdepääsuõiguste vajaduse ja ulatuse osas.

Sotsiaalkindlustusameti peadirektor nõustub soovitusega ja märgib, et „SKA teenistujate juurdepääsu dokument viiakse kooskõlla lähtuvalt viimasest struktuurimuudatusest.

Punktis 70 ei nõustu auditi soovitusega ja selgitame järgmist. Pensioniameti peaspetsialisti ametijuhendis ei ole sõltumatu järelevalve teostaja rolli. Peaspetsialisti ülesandeks on uue töötaja puhul arvutivõrgu kasutusloa taotluse projekti koostamine.”

Riigikontrolli kommentaar (punkti 70 osas): Kui peaspetsialisti tööülesannete hulka ei kuulu ametnike juurdepääsuõiguste põhjendatuse hindamine, siis puudub Pensioniametites andmekogudele ligipääsude loomisel taotlejast sõltumatu juurdepääsuulatuse hindamine.

Infotehnoloogiliselt ei ole välistatud juurdepääsuõiguste ühine kasutamine

73. Juurdepääsu andmekogu andmetele saab infotehnoloogiliselt piirata, kui eri kasutajagruppidele (näiteks klienditeenindajad, andmesisestajad, andmebaasi administraatorid, järelevalvajad jne) on loodud eri kasutajamoodulid. Tüüpiliselt eristatakse kasutajarolle sõltuvalt sellest, kas ja millises ulatuses on kasutajal õigus andmeid vaadata, muuta, lisada ja/või kustutada. Samuti võib näiteks kitsendada kasutajate õigusi arvuti IP-aadressist lähtuvalt ja anda juurdepääsuõigused ainult oma regiooni andmetele, tuvastada kasutajat talle eelnevalt antud sertifikaadi alusel, lukustada kasutajakonto, kui see on pikalt kasutamata jmt. Juurdepääsuõigus peab olema isiklik, mittejagatav, sest ainult nõnda saab kindlustada selge vastutuse andmete töötlemise eest. Võttes kasutusele kõrge turvaastmega autentimismeetodi, saab välistada eri arvutitest samaaegne süsteemi sisenemise ja minimeerida ilma juurdepääsuõiguseta isiku poolt toimingute tegemise.

Hetkel on võimalik juurdepääsuõiguste ühine kasutamine

74. Auditi käigus ilmnes, et osal andmekogudest on endiselt olemas võimalus ühe ja sama kasutajakonto kaudu samaaegselt enam kui ühest arvutist süsteemi siseneda. PKRi puhul selgus, et 2007. aastal on olnud juhtumeid, kus uuele ametnikule on antud kasutada endise töötaja konto või on võõraid kasutajakontosid kasutatud ajutise asendamise ettekäändel. EHISe praegune programm ei välista samuti võimalust, et ühe ja sama kasutajanimega sisenetakse andmekogusse mitmest arvutist samaaegselt. 2009. aastal on EHISes kavas võimaldada sisenemist vaid ID-kaardi ja m-IDga, mis lahendab selle probleemi. MKR esindajad leidsid, et juurdepääsuõiguste muutmine on vahetu juhi vastutusel ning muutmine käib kiiresti, seega ei ole põhjendamatuid takistusi juurdepääsuõiguste ajakohastamisel ega teki vajadust võõrast kasutajakontot ajutiselt kasutada.

Näiteid infotehnoloogilistest juurdepääsupiirangutest:

- infosüsteemi jaotamine mooduliteks kasutajagruppidest lähtuvalt;
- piiratud kasutajakeskkonna loomine – kasutaja saab teha vaid üht tööd;
- õiguste eristamine (vaataja, algataja, muutja, kinnitaja jne);
- ühe regiooni kasutaja ei näe teise regiooni andmeid;
- eri turvatasemega autentimismeetodid veebiteenuste jaoks, avalikult edastatavast lihttekstiparoolist krüpteeritud edastamise ja sertifikaatidepõhise autentimiseni (ID-kaart).

75. Näitena infotehnoloogiliste piirangute loomise kohta, mis arvestavad asutuse toimimise erisusi, võib tuua ITDAKi, kus on võimalik andmeid muuta vaid siis, kui eelnevalt on infosüsteemis algatatud menetlus. Andmete vaatamisele selline piirang ei kehti. Päringu tegemiseks tuleb aga valida põhjus, millise toiminguga seoses see esitatakse. PKRi vastutava töötleja hinnangul on ka neil lihtne kontrollida andmekasutuse eesmärgipärasust, sest iga andmepäring peab olema seotud hilisema dokumendiga, näiteks toetuse andmise või sellest keeldumise otsuse, pensioni määramise vm dokumendiga, kuid ITDAKile sarnast lahendust nad ei kasuta.

76. Vastavalt ISKE meetmele M2.371 tuleb regulaarselt otsida süsteemidest kasutamata kontosid ja need kustutada. Kasutamata kontod kujutavad põhimõttelist turvariski. Risk on seda suurem, mida suuremate volitustega konto on. RRi puhul kasutatakse sertifikaadipõhist ligipääsu, mis aegub automaatselt, kui seda pole kasutatud 6 kuud. PKRis aeguvad kasutajakontod paari kuu möödudes viimasest kasutusest. Samasugusel põhimõttel oleks võimalik ka teiste andmekogude puhul tuvastada isikuid, kes pole andmekogu pikemat aega kasutanud, analüüsida isiku juurdepääsuvajadust ning selle puudumisel kasutajakonto kustutada. Aegumisega on tagatud ka, et töölt lahkunud isikule ei jää kasutusõigused pikaajaliselt kehtima.

Vähe kasutatakse andmekogusse siseneja tuvastamiseks ID-kaarti

77. Järjest enam andmekogusid on läinud (KTKR, ITDAK) või minemas (EHIS, RR) üle kasutajate tuvastamisele ID-kaardi põhjal, mis välistab samaaegselt kahest arvutist andmekogusse sisenemise ning selle, et keegi teine logib kasutaja teadmata andmekogusse ning teeb tema nime all päringuid. Andmekogude haldajad peaksid kõigi väliste andmesaajate puhul tegema kohustuslikuks ID-kaardi kasutamise ning võimaldama juurdepääsu andmekogule vaid läbi turvalise andmevahetuskihi, s. o X-tee kaudu.

78. Juurdepääsuõiguste ühise kasutamise juhud ilmnesid ka KOVides, Enamikus auditeeritud KOVides teeb andmekogudele juurdepääsuõigust omav ametnik andmekogust päringuid ka oma kolleegide palvel, kuid ei talleta infot selle kohta, kelle taotlusel ja miks päring oli vajalik. Teiste palvel päringute tegemise on Ambla ja Viiratsi vallavalitsus välistanud oma töökorraldusega. Lisaks on Vigala vallavalitsuses välja töötatud taotluse vorm, kus fikseeritakse päringu põhjus. Haapsalus tuleb päringutaotlus esitada e-posti teel ja Antsla vallavalitsuses on vaja registreerida kõik päringutaotlused. Kui juurdepääsuks kasutatakse X-

teed ja ID-kaarti, mis võimaldavad üheselt kindlaks teha küll päringu tegija, säilib KOVil siiski endiselt vajadus fikseerida päringu algataja ja põhjus.

79. **Riigikontrolli soovitus ARKile, SKA-le ning MTA-le:** Teha ID-kaart peamiseks autentimisvahendiks andmekogule juurdepääsu andmisel ning välistada seeläbi kasutajakonto jagamine.

Eesti Riikliku Autoregistrikeskuse direktor nõustub soovitusega.

Sotsiaalkindlustusameti peadirektor nõustub soovitusega ja märgib, et „ettepanek võetakse arvesse ja katsutakse leida rahalised vahendid ID-kaardiga autentimiseks. Seoses 27.01.2006 a ministri käskkirjaga nr 22 on IT vara haldamine ja sellega seonduvate riigihangete teostamine üle läinud Sotsiaalministeeriumile. SKA pädevusse on jäänud ainult ettepanekute tegemine. Auditi soovitused edastame Sotsiaalministeeriumile“.

Maksu- ja Tolliameti peadirektor teatab, et „hetkel on MTA rakendustes võimalik autentida ka ID-kaardiga ja see ongi levinuimaks autentimisvahendiks. Samuti on ID-kaardi lugejad kõikidel ametnikel kättesaadavad. Siiski ei ole meil lähiajal plaanis välistada kasutajatunnuste võimalust“.

80. **Riigikontrolli soovitus auditeeritud andmekogude haldajatele**: Tagada pikalt kasutamata seisnud kasutajakontode sulgemine ja kustutamine. Sätestada infoturbe dokumentatsioonis ja väliste andmesaajatega sõlmitavates lepingutes tingimused kontode deaktiveerimiseks ja kustutamiseks ning sellega seotud tähtajad.

Majandus- ja Kommunikatsiooniministeerium ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega.

Haridus- ja teadusminister teatab, et „EHISe volitatud töötleja on seni sulgenud kõik kontod, mida ei ole kasutatud viimase 12 kuu jooksul. Lisame andmevahetuslepingutes kontode haldamise põhimõtete juurde lisatingimused konto kehtivuse osas. Samuti tuleb luua automaatne kontode sulgemine koos teavitusega konto sulgemisest kasutaja poolt antud meiliaadressile“.

Kaitseminister nõustub soovitusega.

Kaitseressursside Ameti peadirektor teatab, et KTKRi osas on soovitus rakendatud.

Maksu- ja Tolliameti peadirektor teatab, et „MTA siseselt sulguvad pikalt kasutamata kasutajakontod automaatselt. Väliste andmesaajatega sõlmitavatesse lepingutesse peame sellise lisasätte sisseviimist põhjendatuks.”

Kodakondsus- ja Migratsiooniamet teatab, et „KMA-s peavad osakonnajuhatajad vähemalt kord poole aasta jooksul vaatama üle kõik ametnikele antud volitused ning lisaks võib ka jooksvalt neil tulla ette vajadus vaadata üle oma osakonna ametnikele antud volitused. Välistel töötlejatel on andmevahetuslepingu kohaselt kohustus pidada arvestust

antud volituste üle ning KMA-l on õigus kontrollida nende reaalsusega vastavust."

Regionaalminister teatab, et „kasutajate õiguste lõpetamine on osaliselt automaatne ja osaliselt tagatud lepingute täiendamise protseduuri käigus. Samuti teostab volitatud töötleja esindaja korrapärast kontrolli kasutajate üle ja kui ilmneb, et mõne asutuse kasutaja ei ole juba mitmel kuul järjest päringuid teinud, siis pöördutakse selgituste saamiseks vastava asutuse poole ja koostöös korrastatakse juurdepääsu andmed. Kasutajate õiguste lõpetamise kord on fikseeritud ka kasutajatega sõlmitavates lepingutes".

Sotsiaalkindlustusameti peadirektor nõustub soovitusega ning märgib, et „SKA infosüsteemis on varasemast ajast juba kasutusele võetud süsteem, et kui isik ei ole kaks kuud oma kontot kasutanud, siis see deaktiveeritakse. Juhul kui ISKE raames valmib infoturbe dokumentatsioon, siis sinna lisatakse kontode sulgemise täpne regulatsioon. Auditi soovitused edastame Sotsiaalministeeriumile."

81. **Riigikontrolli soovitus auditeeritud KOVidele**: Kui KOVis teevad päringuid andmekogule juurdepääsuõigust omavad ametnikud lisaks oma tööülesannetele ka teiste isikute palvel, siis luua süsteem, millega oleks võimalik tagada päringu algataja ja päringu põhjuse hilisem tuvastamine.

Ambla vald teatab, et välistab ametiülesannete väliste päringute tegemist töökorraldusega. Nende hinnangul on ametiülesannete väliste päringute tegemine lubamatu.

Anija vald hindab ettepanekut väga heaks ning teatab, et vallavalitsus on välja töötanud päringu esitamise vormi, milles fikseeritakse päringu esitaja ja päringu esitamise põhjus ning andmete väljastamise kuupäev päringu esitajale. Kirjalikud ja allkirjastatud päringud säilitatakse hilisema tuvastamise võimaldamiseks vastavalt isikuandmete kaitse seaduse nõuetele.

Antsla vald nõustub ettepanekuga ja teatab, et senini on registreeritud teistele ametnikele tehtavaid päringuid registreerimisraamatus. Lisaks teeb vald ettepaneku, et registrites oleks võimalik enne päringu tegemist lisada päringu põhjus.

Audru vald ei esitanud vastamistähtaja ja täiendava nädala jooksul oma arvamust soovitusele.

Haapsalu linn teatab, et on rakendanud rahvastikuregistri päringute registreerimise ainult elektroonilise taotluse alusel. Teiste andmekogude kasutamise vajadust on neil vaja veel monitoorida ning vajaduse korral loovad nad ühtse süsteemi.

Jõelähtme vald teatab, et on alustanud toiminguid sellise süsteemi loomiseks, millega oleks võimalik tagada päringu algataja ja päringu põhjuse hilisem tuvastamine.

Jõhvi vald avaldab, et „selline süsteem on koormav igale ametnikule, kes päringuid teostavad, kuid isikuandmete päringute põhjenduse (eesmärgi) suhtes vajalik. Vastava korra kehtestame arvutivõrgu ja infotehnoloogia kasutamise eeskirja osana".

Kanepi vald teatab, et väljatöötamisel on taotluse vorm, kus fikseeritakse päringu põhjus.

Puka vald märgib, et vallavalitsuses kasutavad andmekogusid volitatud isikud personaalselt ja ühist kasutamist ei toimu. Kui ametnik teeb päringuid andmekogudest teiste isikute palvel, siis ta vastutab täielikult andmekogust päringute seaduspärasuse eest. Vallavalitsus kavandab asjaajamiskorra täpsustamist IT osas, et luua päringu algatamise ja päringu põhjuse hilisema tuvastamise võimalused.

Tapa vald teatab, et esmase lahendusena on viidud sisse süsteem päringute esitamiseks ja säilitamiseks e-mailiga, kus märgitakse ka päringu teostamise põhjus.

Torma vald märgib, et registritesse logimise registreerimiseks ja hilisemaks järelevalveks võiks toimida ühtne registreerimissüsteem (võimalusena võiks olla registris endas vastava märke tegemise koht).

Tõstamaa vald teatab, et väljatöötamisel on vallavalitsuse arvutivõrgu ja infotehnoloogia kasutamise eeskiri, mis sätestab lisaks muule ka teiste ametnike algatusel tehtud päringute põhjuste fikseerimise.

Vigala vald teatab, et vallas on välja töötatud taotluse vorm, kus fikseeritakse taotleja andmed, andmete töötlemise eesmärk, kelle andmeid töödeldakse ning andmete koosseis.

Tartu linn ja **Viiratsi vald** nõustuvad esitatud soovitusega

Kõikidest isikuandmetega tehtud toimingutest ei jää logisid

Logimine on kirjete koostamine arvuti ja kasutaja tegevuste kohta.

82. IKS § 25 lg 2 p 3 ja 5 nõuavad andmetöötlejalt andmete kasutamise logide olemasolu selleks, et tagantjärele oleks võimalik kindlaks teha, millal, kelle poolt ja milliseid isikuandmeid vaadati, salvestati, muudeti, kustutati või muul moel töödeldi. Vastavalt riigi infosüsteemide haldamise jälgitavuse põhimõttele tuleb kõik kasutaja pöördumised andmekogu poole ja neile saadud vastused talletada (infosüsteemide andmevahetuskihiga liitunud infosüsteemide korral turvaserverite turvalogides). Andmete olemasolu andmekogus ja nende töötlemise fakti peab olema võimalik tuvastada ja taastada[21]. Samuti nõuab ISKE meede M7.17 igale infosüsteemile sisemise IT-auditi ja andmekaitse kontrolli rajamist. Selle eelduseks on piisavalt täpsete logikirjete olemasolu.

Üheselt ei mõisteta, milliseid tegevusi on vaja logida

83. Riigikontroll uuris, kuidas logitakse isikuandmete päringuid, andmete muutmist ja vaatamist ning kas on pööratud tähelepanu nende logide analüüsile. Kõikide vaadeldud infosüsteemide puhul olid logisüsteemid olemas, kuid nende detailsus ja ulatus erinev. Tuvastasime, et seitsmest andmekogust vaid neljal olid olemas logid, mis võimaldavad valdavas osas kindlaks teha, mis hetkel milliseid andmeid kasutaja vaatas. Auditi toimumise ajal koostas AKI ettekirjutuse EHISe haldajaile luua logid EHISes isikuandmete vaatamise kohta ning HTM kinnitas, et päringu logide säilimine tagatakse alates 11. novembrist 2008.

[21] Vabariigi Valitsuse 2008. a määrus „Riigi infosüsteemi haldussüsteem" § 5.

Tabel 3. Logide säilitamine isikuandmetega tehtud toimingute kohta.

Andme kogu	Isikuandmete muutmise kohta	Isikuandmete vaatamise kohta (milliseid andmeid, kelle kohta, kes vaatas)
ITDAK	Jah	Jah
RR	Jah	Jah
MKR	Jah	Üldjuhul jah, teatud kasutajarollide puhul ei
LR	Jah	Ei
KTKR	Jah	Osaliselt. On näha isikukaardile sisenemine, kuid mitte vaadatud andmeväljad
PKR	Jah	Osaliselt jah
EHIS	Jah	Ei

Allikas: Riigikontrolli test.

84. Kui andmekogusse tehakse väljastpoolt asutust laekunud soovi alusel (näiteks kaebuse, teabenõude, selgitustaotluse vmt vormis) ühekordseid isikuandmete päringuid, siis jääb sellest üldjuhul (EHIS välja arvatud) jälg päringu teostanud ametniku kohta. Tagantjärele päringu põhjendatuse tõendamine on raskendatud, sest päringu alust tuleb enamikul juhtudel otsida dokumendiregistrist, kus kajastuvad alusdokumendid. Vaid ITDAKi infosüsteemne lahendus lihtsustab järelevalvet, kuna seal on vaja enne päringu tegemist valida selle tegemise põhjus. Üks pakutud valikuvõimalustest on „ametiväline päring". Samuti jääb KMA dokumendiregistrisse jälg andmete edastamise kohta. Riigikontrolli hinnangul on kõigil andmekogudel vaja leida meetmed, mis võimaldavad seostada päringu tegijat ja tegemise põhjust. Vastasel juhul on keeruline kaitsta ametnikke võimalike süüdistuste eest põhjendamatute päringute tegemises.

Sõltuvalt päringutingimuste loetelu või päringuvastuse mahukusest eristatakse **liht- ja masspäringuid**.

Lihtpäring on otsing isiku või objekti konkreetse ainuomase tunnuse (nt isikukood, registreerimisnumber jmt) alusel.

Masspäring (ka liitpäring) on otsing mingite üldiste tunnuste alusel, mille vastuseks on andmete loetelu.

85. Masspäringute puhul päringu valikukriteeriume logidesse enamasti ei jää. See tähendab, et andmekogusse andmete lisandumisel või seal muutmisel ei pruugi hiljem päringut korrates olla võimalik täpselt tuvastada kõiki andmeid, mis päringu algsele teostajale nähtavaks said. Samuti ei jää logi masspäringust, kui see teostatakse näiteks otse andmebaasi mootori kaudu. ITDAKis, RRis, EHISes ja MKRis on siiski teatud rakendusi kasutades võimalik hiljem suuremahulisi päringuid korrata ja selle tulemusena teha kindlaks, milliseid andmeid töödeldi. KTKR on lahendanud olukorra selliselt, et suuremahulise päringu vastusena kuvatakse piiratud hulk andmeid, mis on piisavad soovitud andmesubjekti tuvastamiseks, ning viimase andmete edasine vaatamine logitakse juba lihtpäringuna. Kui masspäringuid ei ole võimalik korrata, ei pruugi infosüsteem tagada isikuandmete kaitse nõudeid, mille kohaselt igal isikul on õigus teada, millal ja milleks tema andmeid on kasutatud. Samas puudub selge seisukoht, kas juhul, kui masspäringu tulemusena teatud isiku andmed satuvad suuremahulise päringuvastuse koosseisu ja rohkem neid ei töödelda, on sellise töötlemise avaldamine isikule tema taotluse alusel põhjendatud.

Logide haldus ja kontroll eri andmevahetuskanalites on ebaühtlane

86. Kui X-tee kasutamisel on üheselt paika pandud andmevahetuse logimise reeglid, siis ühtsus puudub, kui andmevahetuseks kasutatakse muid rakendusi. Näiteks RR pakub oma andmetele juurdepääsuks kolme rakendust: WebCom, Regina ja RRWeb, MKRi andmeid pärib politsei

oma infosüsteemide POLISe ja KAIRI vahendusel. Ka EHIS on koolidele ja enamikele KOVidele kättesaadav otse üle oma veebirakenduse. Iga sellisel rakendusel on ka eri viis andmetega tehtud toimingute logimiseks. Näiteks on Regina ja RRWebi logide detailsus veidi erinev. 2009. aastal võetakse kasutusele uus RRi tarkvara, mis põhineb X-tee arhitektuuril ja vahetab välja Regina ja RRWebi. Politseinike poolt andmekogudesse tehtavaid päringuid logitakse andmekogu poolel üldjuhul vaid päringu teinud politseiasutuse täpsusega. Näiteks saab MTA kindlaks teha MKRi politseiametnike poolt tehtud päringuid vaid asutuse, mitte vahetu isiku täpsusega. Samas kinnitati MTAst, et Politseiametil on lihtne tuvastada konkreetse päringu teinud politseiniku isik ja asutustevahelise hea koostöö tõttu ei takista asjade selline korraldus päringute põhjendatuse kontrolli.

87. Sageli on andmekogude haldajad kinni oma vanades süsteemides ja uued X-teed kasutavad lahendused viibivad, sest vanade arendamiseks on juba tehtud suured kulutused. Samas ei ole Riigikontrolli hinnangul otstarbekas teha edasisi kulutusi infosüsteemidesse, mis ei vii riigis ühtse andmevahetussüsteemi ja selle kontrollimehhanismide tekkeni. Tuleb siiski tõdeda, et kõik auditis vaadeldud andmekogud on andmevahetuskanalina kas suuremal või vähemal määral kasutusele võtnud X-tee. Isikuandmete kaitse aspektist on heakskiidetav just selle kanali kasutus, kuna X-teega liitumine tagab isikuandmete töötlemise põhjendatuse järelevalveks vajalike andmete olemasolu.

88. Andmekogudes, kus logide põhjal kasutajate järelevalvele oli seni vähem tähelepanu pööratud või järelevalvega tegeles IT-valdkonna spetsialist, olid vajalikud logid üldjuhul olemas, kuid töövahendid nende töötlemiseks ja jälgimiseks olid ebamugavad. Oluliselt rohkem oli logianalüüsi tööriistale tähelepanu pööratud RRi, MKRi ja ITDAKi haldajatel. KMA-l on täiendavalt valmimas süsteem, mis võimaldab teha järelevalvet oma asutuse ametnike päringute põhjendatuse üle, mida nad teevad X-tee kaudu asutusevälistes andmekogudes. Samuti on piiratud ulatuses rakendatud lahendust isikule tema kohta tehtud päringute kuvamiseks riigiportaali vahendusel. Riigikontrolli hinnangul oleks logide ja nende analüüsi süsteeme välja töötades kasulik vahetada kogemusi teiste andmekogude vastutavate töötlejatega, kellel on selles valdkonnas suuremad kogemused.

89. **Riigikontrolli soovitus SKA-le, HTMile ja ARKile :** Täiendada andmekogude logimisprotseduure nii, et oleks võimalik tuvastada ka päringute sooritaja, päringu tegemise aeg, põhjus ning päringu tulemusena kuvatud isikuandmed. Seeläbi tagada piisavate logide olemasolu isikuandmete töötlemise kohta, et isikul oleks võimalik saada teavet enda andmete töötlemisest ning vastutaval töötlejal oleks võimalik teha järelevalvet andmete töötlemise üle ja kuritarvituse ilmnemisel süüdlane välja selgitada.

Sotsiaalkindlustusameti peadirektor nõustub osaliselt auditi soovitusega ja selgitab, et sotsiaalmaksu vaatamise andmeid logitakse ja hiljem on võimalik tuvastada, kes ning millal neid andmeid vaatas.

Haridus- ja teadusminister teatab, et „23.10.2008 a rakendus EHISes täiendav logisüsteem, mis võimaldab tagantjärgi kindlaks teha kes, millal ja milliseid isikuandmeid on vaadanud. Isikuandmete vaatamist sisaldavate logifailide säilitamisaeg on 3 kuud. Isikuandmete

salvestamise, muutmise ja kustutamise logifailide arhiveerimisele ajalisi piiranguid ei ole seatud. HTMis tuleb määrata vastutav isik, kellele luuakse võimalus logidega tutvumiseks."

Riigikontrolli kommentaar: Riigikontroll leiab, et isikuandmete vaatamist sisaldavate logifailide kolmekuuline säilitamistähtaeg on põhjendamatult lühike (vt ka punkti 94).

Eesti Riikliku Autoregistrikeskuse direktor nõustub soovitusega.

90. **Riigikontrolli soovitus auditeeritud andmekogude haldajatele:** Luua võimalused päringulogide hõlpsamaks kontrolliks. X-tee kaudu tehtud päringute analüüsisüsteemi arendamisel on soovitav teha koostööd teiste asutustega, kel on vastavad lahendused olemas või väljatöötamisel.

Majandus- ja Kommunikatsiooniministeerium ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega.

Haridus- ja teadusminister teatab, et võtab eesmärgiks logide kättesaadavaks tegemise andmevahetuskanali X-tee kaudu.

Kaitseminister nõustub soovitusega.

Kaitseressursside Ameti peadirektor teatab, et käesolevaks ajaks on KRAs kinnitatud vastavasisuline dokumentatsioon ja loodud infotehnoloogiline võimekus päringulogide kontrollimiseks.

Maksu- ja Tolliameti peadirektor X-tee logide süsteemi peame adekvaatseks, kuid meelsasti oleme valmis tutvuma teiste asutuste lahendustega.

Kodakondsus- ja Migratsiooniamet teatab, et „2009. a eelarve ja investeeringute vähendamise tõttu on KMA-s suunatud arendustööd nendesse valdkondadesse, mis on prioriteetsete põhiülesannetena määratletud (VIS, SIS, biomeetria rakendamine jne), ning lisaks meetmetele, mis on seotud andmebaaside ja infosüsteemide teenustaseme säilitamiseks või olemasolevate lepinguliste kohustuste täitmiseks."

Regionaalminister teatab, et päringute kontrollimiseks valmib eraldi tarkvara rahvastikuregistri tarkvara täiendamise projekti käigus.

Sotsiaalkindlustusameti peadirektor nõustub soovitusega ning edastab soovituse Sotsiaalministeeriumile (vt ka punkti 79 vastust).

Puudub ühtne arusaam logide säilitamise nõuetest

91. Vastavalt isikuandmete kaitse nõuetele on isikuandmete töötleja kohustatud tagama logide olemasolu selle kohta millal, kellele ja millised isikuandmed edastati, samuti selliste andmete muutusteta säilimise. Tulenevalt avaliku teabe seadusest otsustab andmekogu haldaja andmekogu pidamisega seotud korralduslikud küsimused, sh andmetöötluse logide säilitamise tähtajad. Tähtajatult säilitavad andmete muudatuste ja päringutega seotud logisid käesoleval hetkel ITDAK, LR, MKR, KTKR ja RR. EHISe puhul säilitatakse vaid muudatuste ja süsteemi sisenemise logid. Mitmed auditeeritud möönsid, et lähitulevikus tekib vajadus otsustada, kui kaua ja milliseid logisid säilitada, sest nii logimine kui nende säilitamine kulutab süsteemi- ja salvestusressursse.

92. Logide säilitamisel tuleb veel täiendavalt kindlaks määrata, kui kaua on võimalik ja vajalik logisid aktiivses kasutuses hoida (näiteks võrgus reaalajas ligipääsetavana) ja kui pikk iga on näiteks lintidele vm välisele andmekandjale arhiveeritud logidel. MKR peab oma praktikas logide aktiivseks kasutusperioodiks ühte aastat, mille möödudes logid arhiveeritakse. PKRi vastutava töötleja seisukoht oli, et piisab, kui logid on aktiivseks kasutuseks kättesaadavad kahe kuu jooksul. RRis sõltub aktiivse perioodi pikkus logiserveri mälumahust, mis teatud mahu saavutamisel logid arhiveerib.

Andmete säilitamise tähtaegadele on kehtestatud erinevaid nõudeid

93. Olgugi et vastutav töötleja peab määrama logide säilitamise tähtaja, pole auditeeritavad seda üldjuhul dokumenteerinud. Tuleb möönda, et hetkel ei ole ammendavaid kriteeriume, et määrata isikuandmete töötlemise logide säilitamistähtaeg, ning andmekoguti on seisukohad tähtaegade suhtes erinevad. Üks võimalus on lähtuda sellest, et logisid säilitatakse sama kaua kui andmeid endid, kuid selline lahendus eeldab järjest suuremaid kulutusi säilitamisvahenditele ja -protseduuridele, sest andmemahud kasvavad. Teine võimalus on analüüsida eri õigusaktidest tulenevaid või tuletatavaid tähtaegu isikuandmete töötlemise logide säilitamiseks ning hinnata nende sobivust eri andmegruppidele või töötlemise viisidele. Näiteks on õigusaktidest võimalik välja lugeda järgimisi tähtaegu isikuandmete töötlemise ja sellega seotud logide säilitamiseks:

- Vabariigi Valitsuse 24.04.2008 määruse nr 78 „Infosüsteemide andmevahetuskiht“ (§ 19 lg 2) kohaselt varustatakse X-tee andmevahetus krüptograafiliselt aheldatud logiga, et tagada selle hilisem võltsimatus ja terviklus. Logisid tuleb säilitada vähemalt kolm aastat. X-tee osaline võib logide säilitamisele määrata pikema tähtaja.

- Karistusseadustiku § 157 (Kutse- ja ametitegevuses teatavaks saanud saladuse hoidmise kohustuse rikkumine) ja § 157^1 (Delikaatsete isikuandmete ebaseaduslik avaldamine) sätestatud kuritegude aegumise tähtaeg on viis aastat. Logid võivad nendes paragrahvides kirjeldatud kriminaalasjade menetlemisel olla olulised tõendid delikaatsete isikuandmete töötlemise asjaolude selgitamisel.

- IKSi § 42 (Delikaatsete isikuandmete töötlemise registreerimiskohustuse ja isikuandmete välisriiki edastamise nõuete ning andmesubjekti teavitamise kohustuse rikkumine) ja § 43 (Isikuandmete kaitse turvameetmete ja isikuandmete töötlemise nõuete rikkumine) sätestatud väärtegude aegumise tähtaeg on kaks aastat.

- Elektroonilise side seaduse (§ 111^1 lg 4) järgi on sideettevõtja kohustatud säilitama andmeid telefoni- ja internetiteenuse kohta üks aasta alates side toimumise ajast. Jälitus- või julgeolekuasutuse järelepärimisi ja nende alusel antud teavet säilitatakse kaks aastat.

- Schengeni infosüsteemi riikliku registri põhimääruse (§ 24 lg 1) järgi on registrisse esitatud andmete pikim võimalik säilitustähtaeg kümme aastat.

- Riikliku statistika seaduse (§ 6 lg 3) kohaselt on andmesubjektil õigus üks kord aastas tutvuda riikliku statistilise vaatluse korraldaja poolt tema kohta kogutud andmetega.

- Tsiviilseadustiku üldosa seaduse § 150 järgi on kahju õigusvastasest tekitamisest (sh isiklike õiguste kahjustamise puhul) tuleneva nõude aegumistähtaeg kolm aastat alates sellest, kui isik sai kahjust ja kahju hüvitama kohustatud isikust teada või pidi teada saama, kuid mitte pikem kui kümme aastat kahju põhjustanud teo tegemisest või sündmuse toimumisest.

94. Riigikontrolli hinnangul võib sõltuvalt andmete iseloomust olla isikuandmete muudatuste logide säilitamise vajadus sama pikk kui andmete endi säilitustähtaeg, selleks et tagantjärele oleks võimalik kindlaks teha, millal, kelle poolt ja milliseid isikuandmeid salvestati, muudeti või kustutati. Päringulogide säilitamise tähtaja otsustamisel tuleb Riigikontrolli hinnangul lähtuda esmalt andmesubjekti õigusest saada informatsiooni kes, millal ja miks on tema andmeid vaadanud. Teiselt poolt on oluline andmekogu haldaja ja välise andmesaaja võimalus kontrollida kasutajate päringute põhjendatust. Eeltoodu tõttu on Riigikontroll seisukohal, et päringulogide säilitamise tähtaeg sõltub ennekõike töödeldavate isikuandmete olulisusest, nende turbetasemest, delikaatsusest ja nendega seotud süütegude aegumistähtaegadest. Delikaatsete isikuandmete töötlemisel tuleks logisid säilitada minimaalselt viis aastat, muudel juhtudel minimaalselt kaks aastat.

Logide säilitamise tähtaegu pole kindlaks määratud

95. Logidele reaalajas juurdepääsu pikkuse võiks ka edaspidi otsustada andmekogu vastutav töötleja, võttes aluseks andmekasutuse järelevalvetoimingute sageduse ning selle, kuivõrd pikka perioodi on selle andmekogu andmete puhul tavaks kontrollida. Samuti tuleks arvestada asjaolu, kui palju andmesubjektid ja välised andmesaajad esitavad teabenõudeid ning kuivõrd aeganõudev ja töömahukas on arhiveeritud andmekandjatelt logides talletatud informatsiooni hankimine.

96. **Riigikontrolli soovitus AKI-le:** Kaaluda juhendi loomist, mis sätestab minimaalsed nõuded isikuandmete töötlemise logimiseks ning täpsustab, millisel juhul tuleb isiku taotlusel edastada talle masspäringu toimumise, teostaja ja põhjuse kohta samasugused andmed nagu lihtpäringu puhul (vt p 85). Lisaks peaks juhend selgitama isikuandmete töötlemisest jäävate logide säilitamise vajalikkust ja põhimõtteid, millele tuginedes asutused saavad kehtestada logidele säilitustähtaegu. Ilma vastavate suunisteta võib kujuneda olukord, kus asutustes logide säilitamise tähtaeg võib olla soovitud teabe saamiseks või järelevalvetoimingute tegemiseks liialt lühike. Eelmainitud juhendi koostamisel tuleb muu hulgas arvestada seda, kui suurt kahju on võimalik inimesele tema isikuandmete õigusvastase töötlemisega teha, samuti isikuandmete kuritarvitamisega seotud süütegude aegumistähtaegasid ning andmetöötluse järelevalve korraldust andmekogudes.

Andmekaitse Inspektsiooni peadirektor teatab, et Andmekaitse Inspektsioon analüüsib põhjalikult talle tehtud ettepanekuid juhendite väljatöötamiseks ja vajaduse korral lülitab need 2009. aasta tööplaani.

97. **Riigikontrolli soovitus andmekogude haldajatele:** Määrata logide säilitamise tähtajad andmekogu põhimääruses.

Majandus- ja Kommunikatsiooniministeerium ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega.

Haridus- ja teadusminister teatab, et „on algatanud EHISe põhimääruse muutmise. EHISe põhimäärus on võimalik esitada ministeeriumitevahelisele kooskõlastamisele peale andmekogu registreerimist RIHA-s. Fikseerime põhimääruses isikuandmete päringute logifailide arhiveerimise tähtajad“.

Kaitseminister ja **Kaitseressursside Ameti peadirektor** nõustuvad soovitusega.

Maksu- ja Tolliameti peadirektor teatab, et „püüame uurida, millised piiranguid seavad logide hoidmisele EL õigusaktid ja nendest lähtudes kehtestame tähtajad, mida kajastame nii andmekogu põhimääruses kui ka MTA infoturbepoliitikas“.

Kodakondsus- ja Migratsiooniamet teatab, et KMA on väliste andmetöötlejate puhul sätestamas logide säilitamise tähtaegu lepingutes.

Regionaalminister teatab, et „tänasel päeval säilitatakse logisid tähtajatult analoogselt rahvastikuregistri andmetele. Toetudes AKI poolt käesoleva auditi alusel antavale seisukohale samas küsimuses, viiakse logide säilitamise kord ja tingimused rahvastikuregistri seadusesse.”

Sotsiaalkindlustusameti peadirektor nõustub osaliselt soovitusega ja selgitab, et „leiame, et logide säilitamise tähtajad peab paika panema kõikidele ühtlaselt, arvestades töödeldavate isikuandmete koosseisu. Delikaatsetele üks ja tavaandmetele teine säilitamise tähtaeg“.

Logide muudetamatus on üldjuhul tagatud

98. Administraatori ligipääs logidele peab olema piiratud selliselt, et tal puuduks võimalus mõjutada tema enda poolt hallatavate logide terviklikkust. Vastasel juhul tekib oht, et logid ei ole ehtsad ja algupärased. Lisaks organisatsioonilistele juurdepääsu piirangutele saab logide muudetamatust tagada infosüsteemselt.

Logide muudetamatus on tagatud organisatsiooniliselt ja osaliselt ka infotehnoloogiliselt

99. Kõikide vaadeldud andmekogude puhul on kasutusel põhimõte, et logidele saab ligipääsu vaid piiratud hulk isikuid, kellel on selleks ametialane vajadus. Üldjuhul on nendeks isikuteks andmebaaside administraatorid ja isikud, kellele on pandud järelevalve kohustus. MKRis on administraatoril ainult andmete lugemise, mitte aga muutmise ja kustutamise õigus. Samuti jääb administraatori tegevusest logi, st logi jääb ka logide muutmise kohta. Viimane lause kehtib samuti EHISe administraatori tegevuse kohta. PKRis mööndi, et teoreetiliselt on logide muutmine võimalik. Selleks aga peavad muutjal olema põhjalikud eriteadmised logifailidest ja andmebaasi administraatori tasemel juurdepääs infosüsteemidele. Lisaks peaks muutjal olema hea ülevaade seostest andmete vahel, et õigesti tõlgendada logifailide infot, kuna infosüsteemi dokumentatsioonis puudub logide seletus.

100. Päringulogide muudetamatuse tagamiseks seotakse ITDAKis logikirjed üksteisega viisil, mis võimaldab tuvastada muutmise. Andmemuudatuste ning kasutajate autentimise logi muudetamatuse tagamiseks on juurutamisel lahendus, mille eesmärgiks on logikirjete tekkeaja fikseerimine, allkirjastamine ja/või krüpteerimine. Nende meetodite abil tagatakse, et andmete muutmine ilma sellest jälgi jätmata ei ole võimalik. Samalaadne lahendus on plaanis ka uues RRi tarkvaras. Momendil arhiveeritakse RRi logid piiratud ligipääsuõigustega kataloogis, pikemaajalisel säilitamisel on tarvitusel ka täiendavad füüsilised turvameetmed.

Kontroll päringute põhjendatuse üle pole piisav

101. Iga isikuandmete päring andmekogust peab seostuma päringu tegija tööülesannetega. Riigi andmekogudes olevate isikuandmete põhjendamatu töötlemine on keelatud, sh on õigusvastane ametnike uudishimust tingitud isikuandmete vaatamine. Päringulogide analüüs kui kontrollimehhanism võimaldab selliseid kuritarvitusi ennetada ja avastada. Kontrolli oluliseks osaks on võimalus tagantjärele tuvastada, kes, milleks ja milliseid andmeid kasutas. Selleks on vaja, et infosüsteemi logifailides säiliks kogu isikuandmetega seotud tegevuste ajalugu. Juba ainuüksi fakt üksikasjalike ja muudetamatute logide olemasolu kohta mõjub kuritarvitusi ennetavalt, sest teadmine, et igast tegevusest jääb järele jälg, pärsib ebaseaduslike päringute tegemist.

Regulaarset ja süstemaatilist päringute põhjendatuse kontrolli ei toimu

102. Vaadeldud andmekogudest võib hea näitena esile tuua RRi, MKRi ja ITDAKi. Nende puhul on isikuandmete kaitse alane järelevalve oma asutuse ametnike, MKRi ja RRi puhul ka väliste andmesaajate üle ülesandeks tehtud vastutavate töötlejate sisekontrolli ametnikele või järelevalvespetsialistidele, kel on hea ülevaade inimeste töökohustustest ja ettevalmistus järelevalve teostamiseks. LRi, KTKRi ja PKRi puhul on logide kontroll IT osakonna ülesandeks, kuid hoolimata sellest, et tehnilised võimalused on olemas, ei ole süstemaatilist kontrolli andmepäringute põhjendatuse üle tehtud. EHISe puhul puuduvad tehnilised võimalused tehtud päringute põhjendatuse kontrolliks.

103. Regulaarne järelevalve päringute põhjendatuse üle toimub vaid MKRi ja RRi vastutavate töötlejate poolt. PKR ja LR seiravad küll andmekogude kasutajaid, kuid 2007. aastal nad päringute põhjendatuse üle järelevalvet teinud ei ole, põhjendades seda kaebuste puudumisega. Järelevalvet teostatakse vaid siis, kui on tekkinud kuritarvituse kahtlusi. PKR juures lähtuvad kontrollitoimingud kaebustest, taotlustest või turvaintsidentidest. EHISes on seire peaeesmärgiks sisestatud andmete vastavuse tagamine, seetõttu kontrollitakse eelkõige andmete muudatuste logi. Päringute kohta logid EHISes puuduvad ja seetõttu ei ole võimalik ka järelevalve. ITDAKis ja KTKRis on seni puudunud jooksev järelevalve, kuid on tehtud konkreetseid ettevalmistusi, et veel käesoleval aastal hakata teostama kontrolli päringute põhjendatuse kohta.

Päringute põhjendatuse kontroll on asutustes tööülesandena fikseerimata

104. Auditi käigus selgus, et üheski andmekogus, välja arvatud KTKR, pole vajalikuks peetud ametliku dokumendina kehtestada juhendit, kuidas päringute põhjendatuse üle järelevalvet teostada. RRis ja MKRis, kus jooksvalt järelevalvega küll tegeletakse, ei ole selleks juhendit tehtud ja nii Siseministeerium kui ka MTA viitavad vajaduse puudumisele selle järele. Järelevalve meetmeid tuleb pidevalt ajakohastada, seepärast saab pidada põhjendatuks paindlikkuse eelistamist.

105. Küsimusele, kas 2007. aastal on vastutav töötleja oma andmekogu kasutajate hulgas avastanud rikkumisi päringute põhjendatuse osas, vastas seitsmest andmekogust viis (RR ja MKR välja arvatud) eitavalt. Samas tõdeti, et sääraseid kontrollimisi pole ka läbi viidud.

106. Tõhusaks saab pidada Siseministeeriumi kontrolli RRi väliste andmesaajate suhtes, sest nii SKAs, KMAs, ARKis kui ka KOVides esines juhtumeid, kus Siseministeerium palus asutustel täpsustada konkreetsete päringute põhjuseid ning tuvastati andmete põhjendamatut vaatamist. PKRiga toimunud intsidendid, mida 2007. aastal oli kokku 4, olid seotud kasutajaõiguste loovutamisega kaastöötajatele. RRi juhtumite puhul küsib vastutav töötleja selgitusi päringu sihipärasuse kohta, ja kui põhjendust ei ole ning asutus oma vastuses ei viita rakendatud meetmetele (nt distsiplinaarkaristus, täiendav koolitus vmt), pöördub Siseministeerium AKI poole järelevalve menetluse alustamiseks.

107. **Riigikontrolli soovitus HTMile, SKA-le ja ARKile:** Määrata logide kontrollimise eest vastutavad isikud ning tagada neile võimalused ja vahendid regulaarse riskipõhise kontrolli läbiviimiseks isikuandmete töötlemise eesmärgipärasuse üle.

Haridus- ja teadusminister teatab, et teeb vastavad muudatused töötajate ametijuhendites ning määrab logide kontrollimise ja isikuandmete töötlemise järelvalve eest (sh väliste andmesaajate osas) vastutavad isikud.

Sotsiaalkindlustusameti peadirektor nõustub soovitusega ning selgitab, et „SKA teeb Sotsiaalministeeriumile ettepaneku luua selline võimalus SKA isikuandmete kaitse eest vastutava isiku jaoks."

Eesti Riikliku Autoregistrikeskuse direktor nõustub soovitusega.

Mõnede andmekogude väliste andmesaajate kontroll on puudulik

Vastutav töötleja määrab kõigile volitatud töötlejaile kindlaks[22]:
1) isikuandmete töötlemise eesmärgid;
2) töödeldavate isikuandmete koosseisu;
3) isikuandmete töötlemise korra ja viisi;
4) isikuandmete kolmandatele isikutele edastamise lubamise.

108. IKSi § 7 lg 4 sätestab andmekogu vastutava töötleja vastutuse kõigi oma andmekogu kasutajate isikuandmete töötlemise nõuete täitmise eest. Selle nõude täitmiseks peab vastutav töötleja esmalt sätestama andmekasutajaga sõlmitavas lepingus viimase õigused ja kohustused ning teostama järelevalvet isikuandmete töötlemise nõuete täitmise üle. Sageli reguleerivad välistele andmesaajatele andmekogule juurdepääsuõiguste andmise korda detailsemalt andmekogude põhimäärused.

Mitmel juhul on lepingud väliste andmesaajatega sõlmimata

109. EHIS, ITDAK, LR, MKR, RR sõlmivad isikuandmetele juurdepääsu võimaldamiseks lepingud (ITDAKil varasemast ka andmete vastuvõtmise-üleandmise aktide nime all) väliste andmesaajatega. Need lepingud sisaldavad muu hulgas ka andmetele juurdepääsu saaja kohustust andmeid eesmärgipäraselt kasutada. HTM ei ole EHISega seoses lepinguid KOVide ja haridusasutustega sõlminud, küll aga teiste riigiasutustega, nagu näiteks SKA ja Haigekassa. KTKRil samuti lepingud puuduvad. Samas on KTKRi puhul välised andmesaajad

[22] IKS § 7, vt https://www.riigiteataja.ee/ert/act.jsp?id=12909389 .

üldjuhul haldusalasisesed, kellele juurdepääsu andmine ja kohustused on sätestatud kaitseministri vastava käskkirjaga.

110. PKRi haldajate hinnangul neil välised andmesaajad andmekogule ligi ei pääse, mistõttu pole ka vastavaid kasutuslepinguid. Auditi käigus selgus siiski, et SKA teeb regulaarselt väljavõtteid PKRi andmetest, millele on KOVide jaoks loodud juurdepääs X-tee kaudu. Kõigil auditeeritud KOVidel oli juurdepääs PKRi andmetele, mille kohta aga puudub kasutustingimusi sätestav leping.

Väliste andmesaajate poolt tehtud päringute põhjendatuse üle ei ole sageli kontrolli ka lepingu olemasolu korral

111. Auditi käigus ilmnes, et vastutus andmete eesmärgipärase kasutuse eest on (lepingute olemasolu korral) pandud lepingujärgsetele välistele andmesaajatele ning ükski vaadeldud andmekogude haldajatest ei tee järelevalvet nende töötlemiskeskkonna turvalisuse üle. Väliste andmesaajate teenistujate juurdepääsude ja päringute põhjendatuse üle kontrolli üldjuhul (RR ja MKR välja arvatud) ei teostata. RR on vaadeldavatest andmekogudest kõige laialdasemalt kasutatav ning tema puhul on välja töötatud meetmed juurdepääsude ja andmete eesmärgipärase kasutamise kontrolliks kõigi kasutajate puhul. MKR teostab samuti järelevalvet väliste andmesaajate, nagu näiteks KOVide üle.

112. Ehkki auditi käigus selgus, et EHISe kasutamise osas on järelevalve puudulik ning päringute põhjendatust ei saa logide puudumise tõttu kontrollida, ilmnes üllatusena, et viis KOVi tajub, et nende päringute põhjendatust kontrollitakse HTM/REKKi poolt. Järelevalve mulje võib olla tekkinud sellest, et EHISe vastutava/volitatud töötleja jälgib andmete muutmist ja teavitab, kui leitakse viga sisestatud või muudetud andmetes, ning palub selle ametnikul või haridusasutuse esindajal parandada.

113. Eeluurimise või jälitustegevuse käigus politseiasutuste poolt kogutavate andmete, st ka tehtavate päringute avaldamine on piiratud muu hulgas IKS § 20 lg 1 p 3 ja 4 alusel. Enamiku andmekogude puhul näeb andmekogu haldaja päringu teostajana vaid päringu teinud asutust ning logid päringu konkreetse teostaja kohta säilitavad politseiasutused.

114. Riigikontrolli hinnangul on politseiasutuste puhul põhjendamatu rakendada piiratud korda kõigi ametnike poolt sooritatavate päringulogide avaldamisele IKS § 20 sätestatud alustel. Päringute korral, mida teevad LRist ja ITDAKist politseiasutused, eeldavad andmekogude haldajad, et järelevalvet päringute põhjendatuse üle teostab politseiasutus ise. Ka MKR ei teosta järelevalvet politsei päringute üle, ehkki logid andmete vaatamise kohta on politseiasutuse täpsusega olemas.

Kohalikud omavalitsused ise päringute põhjendatust ei kontrolli

115. Kõikidest auditeeritud KOVidest on üksnes Tartu linn kontrollinud oma ametnike päringute põhjendatust. Samas on seda tehtud vaid RRi päringute kohta. RRi logisid oma ametnike poolt tehtud päringute kohta on küsinud ka Haapsalu linn, kuid päringute põhjendatuse üle järelevalvet teostatud pole.

116. Teised KOVid pole kontrollinud, kas nende ametnike päringud RRi on põhjendatud. Samas ei saa seda seletada sellega, et tunnetatakse niigi Siseministeeriumi-poolset järelevalvet (8 valda ja linna 15st), sest nende andmekogude korral, mille puhul tunnetatakse andmekogu vastutava töötleja järelevalvet vähem (MKR – 5 ja PKR – 2 omavalitsust 15st) või ei tunnetata üldse (LR), puudub samuti järelevalve KOVide poolt.

117. Enamik auditis vaadeldud KOVisid pole oma ametnike päringulogisid küsinud ei turvaserveri administraatorilt ega vastutavalt töötlejalt ega ole seetõttu saanud ka päringute põhjendatust hinnata. Omavalitsused teavad üldjuhul, et X-tee vahendusel tehtud päringute kohta jäävad alles logid, mida saab vajaduse korral vaadata. Teadlikud ei olda, et kui KOVil on enda hallata X-tee turvaserver, mille kaudu toimub kogu andmevahetus, talletuvad sinna ka kõik KOVi ametnike poolt X-tee vahendusel tehtud päringulogid. Kui turvaserveri administreerimiseks on sõlmitud kokkulepe väljapool KOVi, saab logisid küsida turvaserveri administraatorilt. Mitme andmekogu kasutajalepingus on viidatud õigusele küsida logisid ka vastutavalt töötlejalt.

118. Kuna KOVid ei küsi vastutavailt töötlejailt logisid, peavad andmekogude vastutavad töötlejad olema teadlikud asjaolust, et hoolimata lepingutega KOVidele antud isikuandmete kaitse alastest ülesannetest ei ole KOVid neid ülesandeid järelevalve osas täitnud. Kuna üldvastutus isikuandmete kaitse eest on andmekogu vastutaval töötlejal, on taunimisväärne, kui nad ise pole asunud kontrollima päringute põhjendatust ega astunud samme, et KOVid täidaksid lepinguga võetud isikuandmete andmekaitse kohustust.

X-tee võimalusi andmetöötluse jälgimisel kasutatakse vähe

119. X-tee võimaldab jälgida väliste andmesaajate päringuid piisava täpsusega, seetõttu on Riigikontrolli hinnangul vaja avada juurdepääs oma andmekogule just X-tee vahendusel. Viimane võimaldab kasutajate turvalist identifitseerimist ning sellega ka ülevaadet, kellel on andmekogule juurdepääsu õigused. Samuti saab nende logide põhjal väliselt andmesaajalt vajaduse korral küsida, kas mõni nende konkreetne päring oli põhjendatud või mitte. Kui X-tee asemel on kasutusel teised andmevahetusviisid, tuleb vastutaval töötlejal tagada logiandmete olemasolu, et hinnata kasutajate andmetöötluse põhjendatust.

120. Riigikontrolli hinnangul ei ole kontroll andmekogude väliste andmesaajate üle piisav. Lepingutega järelevalve üleandmine ei vabasta andmekogu vastutavat töötlejat talle IKSi ja andmekogu põhimäärusega pandud järelevalve ülesannetest.

121. Riigikontrolli soovitus auditeeritud andmekogude haldajatele:

- Kajastada lepingutes väliste andmesaajatega neile mõeldud infoturbe nõuded, sh isikuandmete kaitse, koos nende kinnitusega nõuetele vastavuse kohta ning samuti meetmed puhuks, kui väline andmesaaja lepingut rikub. Samuti peaks leping kajastama, kuidas ja millises mahus peavad välised andmesaajad teostama järelevalvet isikuandmete töötlemise põhjendatuse üle ning kuidas teavitatakse sellealasest tegevusest ja tulemustest andmekogu haldajat.

- Koostöös Siseministeeriumiga eraldi kindlaks määrata juurdepääsuõigused politseiasutuste ametnikele tulenevalt nende spetsiifilistest tööülesannetest ning asuda koostöös politseiasutustega tegema regulaarselt järelevalvet nende päringute põhjendatuse üle, mille suhtes ei rakendu IKS § 20 piiratud kord.

Majandus- ja Kommunikatsiooniministeerium ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitustega.

Haridus- ja teadusminister teatab, et vastavad punktid on väliste andmesaajatega reguleeritud andmevahetuslepingutes.

Riigikontrolli kommentaar: Asjaolu, et haridusasutustel ning valdadel ja linnadel on seadusest tulenevalt õigus omaenda andmetele juurdepääsuks EHISes, ei taga, et nad täidavad infoturbe ja isikuandmete kaitse tagamisega seotud nõudeid. Kuna HTM ei ole EHISega seoses sõlminud lepinguid KOVide ja haridusasutustega (vt ka punkt 109), siis leiab Riigikontroll, et mitmete väliste andmesaajate osas on HTM jätnud esitamata nõuded infoturbele ja järelevalvele isikuandmete töötlemise põhjendatuse üle.

Kaitseminister ja **Kaitseressursside Ameti peadirektor** nõustuvad soovitustega.

Maksu- ja Tolliameti peadirektor teatab, et „X-tee lepingute osas sisaldusid infoturbenõuded ka seni. Muud väliste andmesaajatega sõlmitavad lepingud hakkavad edaspidi läbima kooskõlastust sisekontrolliosakonna poolt, mille käigus jälgitakse infoturbenõuete sisaldumist. Politseiametnike juurdepääsuõiguste osas peab MTA läbi rääkima Politseiameti politseikontrollibürooga."

Kodakondsus- ja Migratsiooniamet teatab, et „ITDAK-i andmete töötlemise lepingutes on kajastatud andmekaitsenõuded, lepingu rikkumisega seotud sanktsioonid, järelevalve teostamise ja sellest teavitamise nõuded, andmetöötlemise lõpetamisega seotud nõuded jm nõuded, millest tuleb andmetöötluses kinni pidada. Lisaks andmevahetuslepingu kohaselt peavad ITDAK-i põhimääruses toodud turvaklassile vastavatele organisatsioonilistele, füüsilistele ja infotehnilistele turvameetmetele tähelepanu pöörama ka välised andmetöötlejad. KMA kavandatakse liita alates 2010. a Politsei- ja Piirivalveameti koosseisu, mistõttu tuleb 2009. a üle vaadata kogu andmevahetuse regulatsioon tervikuna tänase Politseiameti ja Piirivalveametiga."

Regionaalminister teatab, et „registri kasutajatega sõlmitavates lepingutes on kirjas, mis eesmärgil võib registrisse päringuid teha. Samuti kohustus tagada rahvastikuregistri andmete töötlemine vastavalt rahvastikuregistriseadusele, isikuandmete kaitse lokaalvõrgus vastavalt IKSile ning paroolide ja salasõnade salajas hoidmise kohustus. Lisaks on lepingutes kirjas ka loetelu tegevustest, mille eest kasutaja vastutab ning Siseministeeriumi ja AKI poolne järelevalve korraldamine ning õigus katkestada kasutaja ühendus kui on ilmnenud isikuandmete kaitse nõuete rikkumine. Rahvastikuregistri kasutajatel on nendega sõlmitud lepingu kohaselt õigus saada aruandeid andmete töötlejate poolt teostatud päringute kohta ajaperioodide lõikes. Lepingutes ei ole väliste andmesaajate ühest kohustust teostada järelevalvet isikuandmete töötlemise põhjendatuse üle ja teavitada sellest andmekogu haldajat. Rikkumise dokumenteerimise ja rikkumisest teavitamise kord on sätestatud rahvastikuregistri seaduses (§-d 63 ja 64). Täiendades ja ajakohastades rahvastikuregistri töötlemise lepinguid, arvestame ka Riigikontrolli ettepanekuid".

Sotsiaalkindlustusameti peadirektor teatab, et „Sotsiaalministeeriumi ja Sotsiaalkindlustusameti andmevahetuslepingud sisaldavad edaspidi lepingu lisa, mis on juba välja töötatud, kuid pole veel rakendamist

leidnud. Selles on sätestatud vastaspoole üldised andmeturbenõuded." SKA peadirektor lisab teise soovituse kohta, et politseiasutuste ametnikel puudub juurdepääs PKRile, kuid nende poolt teostatavatele päringutele on alati lisatud seaduslik alus ning vajalikud põhjendused, miks vastavaid andmeid on vaja.

122. **Riigikontrolli soovitus SKA-le:** Sõlmida PKRi väliste andmesaajatega lepingud, kus määrata kindlaks osapoolte õigused, kohustused ja vastutus.

Sotsiaalkindlustusameti peadirektor ei nõustu soovitusega ning selgitab, et „SKA-l on sõlmitud lepingud mitmete PKR-st andmeid päringute baasil saavate asutustega nt Haigekassa, EHIS jne. KOVidega ei sõlmitud lepinguid, kuna seda liitumise ajal ei nõutud. Ettepanek oleks, et RIA võiks luua universaalse lepingu, mis sätestaks X-teele juurdepääsu, kus oleks sätestatud, mis tingimustel ja mis õigustega saadakse teistelt andmekogudelt andmeid."

Riigikontrolli kommentaar: KOVid on samasugused andmesaajad nagu nimetatud teised asutused. Andmekogu vastutav töötleja vastutab muu hulgas ka selle eest, et andmekogus olevaid andmeid ei vaadata ebaseaduslikult. Seetõttu on andmekogule juurdepääsu andmisel põhjendatud kahepoolse lepingu sõlmimine.

Vastavalt Vabariigi Valitsuse 24.04.2008. a määruse nr 78 „Infosüsteemide andmevahetuskiht" § 20 vastutab X-teega liitunud asutus või isik tema turvaserveri kaudu teenuse kasutaja X-tee keskkonnale juurdepääsuõiguste andmise eest. RIA ülesanne on vastavalt määrusele tagada X-tee haldamine ja arendamine.

123. **Riigikontrolli soovitus HTMile, SKA-le, ARKile ja KMA-le:** Võtta kasutusele meetmed, kontrollimaks väliste andmesaajate isikuandmete kaitse nõuete täitmist. Selleks määrata oma asutuses järelevalve eest vastutajad ning arendada infosüsteemides välja järelevalve teostamiseks vajalik funktsionaalsus.

Haridus- ja teadusminister teatab, et teeb vastavad muudatused töötajate ametijuhendites ning määrab logide kontrollimise ja isikuandmete töötlemise järelvalve eest (sh väliste andmesaajate osas) vastutavad isikud. Lisaks kaalutakse võimalust täiendada haridusasutuse välishindamise protseduuri.

Sotsiaalkindlustusameti peadirektor nõustub soovitusega osaliselt ning selgitab, et „olukord, kus register peab enda väliste kasutajate üle täielikku isikuandmete kontrolli teostama, on üsna suure ja ressursse nõudva kohustuse tekitamine. Välistele kasutajatele lubatakse andmete kasutamist kindlatel alustel, tavaliselt on selleks seadusest tulenev alus/kohustus. Eeldatav on pistelise kontrolli teostamine mõningate isikute/päringute osas. Kui välja töötada infosüsteem, mis hakkaks kontrollima mingitel kindlatel alustel väliste kasutajate päringuid, on see ülemäära kulukas ettevõtmine. Lisaks on Eesti Vabariigis seadustega paika pandud, mis alustel, kes ja mis ulatuses andmeid töödelda tohib. On loodud Andmekaitse Inspektsioon, kes kontrollib isikuandmete töötlemist. Register saab ja peabki võtma endale teatud kohustused väliste kasutajate osas, kuid selle peab ühtlaselt sätestama. Juhendi koostamine, mida üks register oma väliste kasutajate osas inspekteerima

peab, võiks tulla AKI-lt koostöös suuremate registrite pidajatega. Ei ole mõtet luua ühtki uut nõuet, mida keegi teostada ei suuda“.

Eesti Riikliku Autoregistrikeskuse direktor nõustub soovitusega.

Kodakondsus- ja Migratsiooniamet teatab, et „hetkel on käimas protsess, kus KMA on uuendamas andmevahetuslepinguid. Uutes andmevahetuslepingutest on muu hulgas sätestatud väliste töötlejate endi kohustus teostada regulaarset järelvalvet andmete töötlemise üle ning lisaks nende auditite tulemuste teavitamise kord KMA-le. KMA-s on määratud isik, kes kontrollib eelpool nimetatud auditite KMA-sse jõudmist, nende sisu ning koordineerib ka juhtkonna teavitamist auditite sisust. Lepingus on sätestatud KMA-le õigus teostada järelevalvet (selline õigus on kajastatud ka varasemates lepingutes).”

Inimese juurdepääs oma andmetele ning tema kohta tehtud päringutele

Inimese soovil tuleb talle teatavaks teha[23]:

- tema kohta käivad isikuandmed;
- isikuandmete töötlemise eesmärgid;
- isikuandmete koosseis ja allikad;
- kolmandad isikud või nende kategooriad, kellele isikuandmete edastamine on lubatud;
- kolmandad isikud, kellele tema isikuandmeid on edastatud;
- isikuandmete töötleja või tema esindaja nimi ning isikuandmete töötleja aadress ja muud kontaktandmed.

124. Vastavalt IKSi § 10 võib haldusorgan isikuandmeid töödelda vaid avaliku ülesande käigus seaduses, välislepingus või Euroopa Liidu otsekohalduvas õigusaktis ettenähtud kohustuse täitmiseks. Kui isikuandmete töötlemine ei ole seaduse alusel lubatud, on inimesel õigus nõuda oma isikuandmete töötlemise lõpetamist ja kogutud andmete kustutamist või neile juurdepääsu sulgemist. IKSi § 19 kohaselt on isikul õigus küsida isikuandmete töötlejalt enda kohta kogutud isikuandmeid ning infot nende andmete töötlemise kohta. Samuti on inimesel õigus nõuda ebatäpsete või eksitavate andmete parandamist.

125. Auditi käigus vaadati, kas andmekogude haldajad on loonud soodsad tingimused selleks, et inimene saaks tutvuda tema kohta kogutud andmetega. Samuti hinnati, kas andmekogudel on olemas kõikehõlmav info, sh info isikuandmete vaatamise ja kasutamise eesmärgi kohta, mida IKSi kohaselt inimesel on õigus nõuda.

Inimestele on loodud mitmeid häid võimalusi tutvuda enda kohta kogutud andmetega

126. Kõik vaadeldud andmekogud on loonud inimesele head võimalused tema kohta kogutud isikuandmetega tutvumiseks. Lisaks traditsioonilisele viisile küsida infot teabenõude või selgitustaotlusega pakuvad kõik auditis vaadeldud andmekogud võimalust riigiportaali või MTA e-maksuameti vahendusel tutvuda enda kohta kogutud andmetega. RR ja MKR pakuvad ainsana sama kanali kaudu ka võimalust teavitada vea leidmisest oma andmetes või statistiliste andmete muutumisest. KMA aga võimaldab veebi vahendusel kindlaks teha oma isikut tõendava dokumendi taotluse menetlemise seisu ja dokumendi kehtivust ning LR andmeid isiku sõidukite kohta.

127. Lisaks andmetele endile on isikul õigus saada teavet selle kohta, kes tema andmeid on töödelnud ja kellele neid on edastatud. Ainult KMA on riigiportaalis välja töötanud lahenduse, millega isikul on võimalik näha, kas tema andmeid on keegi pärinud. See lahendus ei hõlma hetkel siiski KMA-siseseid ega teiste riigiasutuste poolt tehtud päringuid, vaid ainult inimese enda poolt X-tee vahendusel tehtud ja näiteks notarite sooritatud päringud. Teiste andmekogu kasutajate sooritatud päringute kohta KMA riigiportaalis ülevaadet ei anna.

Oma andmete töötlemise kohta saab infot enamasti vaid teabenõude abil

128. Teiste vaadeldud andmekogude puhul tuleb inimesel oma andmete töötlemisest teadasaamiseks esitada teabenõue, millele vastatakse sõltuvalt andmekogust erineva täpsusega. RRil on kavas infosüsteemi täiendada viisil, et isikul endal oleks veebi kaudu võimalik näha oma andmete töötlejaid. Ka MKR ja LR on pidanud samasuguseid plaane. EHISe puhul saab juhul, kui isikuandmeid on muudetud, teabenõude esitaja teada muudatuste tegija. Kui muudatusi pole tehtud, on ainus võimalus saada infot selle kohta, kellel on õigus tema andmetele ligi pääseda (tegemist võib olla sadade isikutega), aga ei ilmne, kes neist ka tegelikult isiku andmeid on kasutanud. Nagu eespoolgi mainitud, vajab EHIS edasiarendamist, et oleks võimalik tuvastada andmeid reaalselt vaadanud ametnikku.

---

[23] IKS § 19, vt https://www.riigiteataja.ee/ert/act.jsp?id=12909389.

129. Kui inimene esitab teabenõude ja soovib teada enda andmete töötlejat, on andmekogude haldajate jaoks probleemiks otsustada, millise detailsuse astmega isikuandmete päringu teostajat näidata – kas ametniku, allüksuse või asutuse täpsusega. Ehk teisisõnu – kas ka päringu teostanud ametnikul on õigus privaatsusele? IKSi § 19 lg 1p 6 sätestab, et andmesubjektile tuleb teatavaks teha isikuandmete töötleja või tema esindaja nimi, lubades seega mõlemaid variante. RRi esindajate sõnul on nemad üldjuhul jäänud teabenõude vastuses ametiasutuse tasemele ega avalikustata päringu teinud ametniku nime, ehkki võimalik oleks vastata väga täpselt, mis andmeid, kelle kohta ja kelle poolt vaadati. Riigikontrolli hinnangul piisab, kui inimesele antakse teada tema andmete töötleja asutuse või selle allüksuse täpsusega. Samas peab vajaduse tekkides olema võimalik asutusesiseselt tuvastada ka konkreetne ametnik, kes andmetele ligi pääses.

Andmete töötlemise põhjust on tagantjärele raske välja selgitada

130. Kui andmekogu kasutavad välised andmesaajad X-tee kaudu, on olemas ka andmed selle kohta, kes, millisest asutusest ja milliseid andmeid on töödelnud ning isikute teabenõuetele vastamisega probleeme ei teki. Kui küsitakse aga ka töötlemise täpsemat põhjust, ei ole vahet, kas andmevahetuseks kasutatakse X-teed või muud lahendust, sest päringu põhjused logides ei kajastu. Vastuse saamiseks tuleb üldjuhul otsida päringute seoseid asutuse dokumendiregistriga, ametijuhenditega vmt. Infotehniliselt oleks probleemi võimalik lahendada, kui päringu tegemisel panna selle teostajale kohustus fikseerida päringu tegemise põhjus. Sellise lahenduse teed on läinud KMA oma asutusesiseste ja X-tee kaudu ligipääsu omavate kasutajatega, et lisada andmetöötlemisele läbipaistvust. Selline lahendus ei pruugi iga andmekogu puhul sobilik olla, sest ei suudeta luua ammendavat põhjuste loetelu või need jäävad liiga üldsõnaliseks ega rahulda inimest.

131. Politseiasutuse ametnike tehtud päringute andmeid isikule ei avaldata. Kõik andmekogud on politseiasutuse poolt nende andmekogusse tehtud päringuid käsitlenud kriminaalasja andmetena, mille kohta andmekogu vastutav töötaja isikule teavet ei väljasta. Hetkel puudub infosüsteemides võimalus, et päringu tegija saaks valida päringu tegemise põhjuse, samuti ei rakendata eri tööülesannetega tegelevatele politseiametnikele nende tööülesannetest sõltuvalt erinevaid juurdepääsumooduleid. Seetõttu pole võimalik hinnata, kas informatsiooni konkreetse päringu kohta peaks isikule avaldama või mitte. Näiteks kui liikluspolitsei kontrollib e-politsei vahendusel andmekogudest eeskirjade rikkuja andmeid, ei ole see kindlasti põhjus, miks isik ei tohiks päringu kohta informatsiooni saada. Samas ei tohi informatsioon kriminaalmenetluse või jälitustegevuse käigus isiku kohta tehtud päringutest ennatlikult temani jõuda.

Isikute huvi enda andmete töötlemise kohta on väike

132. Auditi käigus selgus, et andmekogu haldajale võib olla äärmiselt keeruline ja töömahukas isiku taotluse alusel tuvastada, millal, millises andmetöötlusprotsessis, kelle poolt ja mis otstarbel tema isikuandmeid kasutati. Hõlpsaid analüüsivahendeid selleks andmekogudes ei ole. Üks põhjuseid on kindlasti praegu veel andmesubjektide väike huvi sellist infot andmekogude haldajatelt küsida ning sellest tulenevalt ka andmekogude haldajate vähene huvi selliseid analüüsivahendeid välja töötada.

133. Andmesubjektidele hõlpsa ligipääsu avamine päringulogidele on kõige kindlam viis saada vihjeid võimalike kuritarvituste kohta ning rikkujad vastutusele võtta. Enamik KOVisid nendib, et neile pole esitatud ühtegi kaebust ega küsimust nende poolt sooritatud päringute kohta ja seetõttu ei ole nad pidanud eraldi vajalikuks ka ise järelevalvet teostada. Ka andmekogude vastutavad töötlejad põhjendavad päringute kontrolli vähesust või puudumist kaebuste vähesusega.

Andmetöötluse läbipaistvus aitaks kontrollida töötlemise põhjendatust

134. Kiirendades isiku andmete ja nende kohta päringute tegemise info jõudmist isiku endani, saab luua täiendava võimaluse isikuandmete töötlemise eesmärgipärasuse kontrollimiseks. Riigikontrolli hinnangul on otstarbekas infosüsteeme arendada edasi suunas, kus inimestel oleks võimalus iseseisvalt vaadata nende kohta eri asutuste poolt andmekogudesse tehtud päringute andmeid, sh päringu põhjust. Põhjuste märkimine infosüsteemi tugevdaks kaitset isikuandmete väärkasutuste vastu, lihtsustaks järelevalvet ning võimaldaks andmekogudel luua lahendusi, kus isik ise näeb riigiportaalis kõiki tema andmetega tehtud toiminguid IKSis sätestatud täpsusega.

135. Kaalumist vajab, kui pika ajavahemiku kohta isikul päringute infot on võimalik saada. Kui isik esitab teabenõude põhjendamatult pika ajaperioodi kohta, võib isikuandmete töötlejate kindlakstegemine osutuda liigselt töömahukaks ja aeganõudvaks. Sel juhul on vaja sätestada, millal teabenõude täitmise kulud kaetakse teabenõude esitaja poolt. Seni on laekunud vaid üksikuid teabenõudeid, kuid isikuandmete kaitse alase teadlikkuse tõustes selletaolised päringud kindlasti sagenevad. Riigikontrolli hinnangul saaks eelmainitud olukorda selgust tuua AKI juhend.

136. Riigikontrolli soovitus auditeeritud andmekogude haldajatele: Arendada andmekogude infosüsteeme nii, et info väljastamine isikuandmete töötlemise kohta oleks edaspidi kiirem ja vähem töömahukas. Arendamisel tuleb silmas pidada, et infot andmete töötlemise kohta kuvataks nii andmebaasi haldaja kui ka andmebaasi väliste andmesaajate toimingute kohta.

Majandus- ja Kommunikatsiooniministeerium ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega.

Haridus- ja teadusminister teatab, et arvestab nõudeid iga uue arenduse analüüsi- ja disaini faasist alates.

Kaitseminister ja **Kaitseressursside Ameti peadirektor** ei väljenda seisukohta soovituse osas.

Maksu- ja Tolliameti peadirektor teatab, et infosüsteemide arenduse ühe alusdokumendina on MTA-l kavas välja töötada baasnõuded arendajale, mis hõlmavad ka logimist.

Kodakondsus- ja Migratsiooniamet teatab, et „ITDAK-i puhul on info andmete töötlemise kohta väliste andmetöötlejate poolt kajastatud kodanikuportaalis, muutes seeläbi kodaniku üheks lüliks andmekaitseprotsessis. Edaspidistes arendustöödes juhindub KMA esitatud soovitusest KMA kui töötleja kohta.”

Regionaalminister teatab, et „alates 2009. aasta III kvartalist on igal isikul e-teenusena võimalus saada vastus tema kohta rahvastikuregistrisse tehtud päringute kohta. Päring annab vastuseid alates valmimise hetkest, sest vanade andmete kuvamine ei ole tehniliselt võimalik. Varasemate päringute kohta on võimalik saada teavet, pöördudes rahvastikuregistri volitatud töötleja poole. Pooldame Riigikontrolli seisukohta, et isikule antakse teada tema andmete töötleja asutuse või selle allüksuse täpsusega“.

Sotsiaalkindlustusameti peadirektor nõustub soovitusega ning selgitab, et edastab soovituse Sotsiaalministeeriumile (vt vastus punktile 79).

/allkirjastatud digitaalselt/

Ülle Madise
II auditiosakonna peakontrolör

Riigikontrolli soovitused ning ministrite, riigiasutuste ja kohaliku omavalitsuse üksuste juhtide vastused

Riigikontroll tegi auditi põhjal ministeeriumidele, riigiasutustele ja kohaliku omavalitsuse üksustele mitmeid soovitusi.

Allpool olevad tabelid annavad kokkuvõtliku ülevaate tehtud soovitustest ja saadud vastustest.

Ministrite, riigiasutuste ja kohaliku omavalitsuse üksuste juhtide üldised kommentaarid

Eesti Riikliku Autoregistrikeskuse direktor teatab täiendavalt, et „mitmed aruande eelnõus mainitud puudused olid meile teada juba mõned aastad tagasi. Siis alustasime uue infosüsteemi (ARIS2) projekteerimisega, mis peaks enamiku senistest isikuandmete töötlemise puudujääkidest kõrvaldama. ARIS2 infosüsteem on kavas kasutusele võtta 2009. a esimesel poolel."

Kaitseminister peab esitatud hinnanguid ja tähelepanekuid sisuliseks ja asjakohasteks. Minister toetab Kaitseressursside Ameti peadirektori poolt esitatud seisukohti ja hindab nende jõustamist 2009. aasta jooksul väga heaks.

Kaitseressursside Ameti peadirektori arvates on eelnõu hinnangud ja tehtud soovitused asjakohased ja aktsepteeritavad. Kaitseressursside Amet tänab audiitoreid asjaliku auditi eest ning arvestab Riigikontrolli aruandes toodud tähelepanekute ja soovitustega 2009. aasta tegevusplaani koostamisel.

Ambla vald teatab, et „teeb täheldatud puudujääkide osas ametiasutuse töökorralduses vajalikud muudatused, võttes senisest tõhusamaid rakendusmeetmeid töökorralduses, mis aitaks tagada isikuandmete kasutamise kontrollitavust, õiguspärasust, välistaks põhjuseta päringuid, tagaks isikuandmete kaitse põhimõtetele vastava seadusliku, eesmärgipärase, minimaalse ja turvalise andmetöötluse.

Esimesel võimalusel rakendame meetmed andmekaitset reguleerivate asutusesiseste dokumentide täiendamiseks IT osas, kehtestades reeglid paroolihalduseks ja järelevalve korralduseks lähtuvalt isikuandmete kaitse aspektist ning KOV-i registreerimise delikaatsete isikuandmete töötlejana AKI-s.

Andmetöötlejana, kellele on võimaldatud seadusest tulenevate või seaduse alusel pandud ülesannete täitmiseks juurdepääs riiklikele andmekogudele ja seal olevatele isikuandmetele turvalise töötlemise nõuete täitmiseks, rakendame koostöös riigi andmekogude haldajatega meetmeid asutuse infotehniliseks arenduseks liitumisel ISKE turvameetmete rakendamiseks.

Lisaks teavitame, et andmetöötlusega seotud ohtude ja riskide maandamiseks ning andmekaitsealase pädevuse tõstmiseks on meie ametiasutuse teenistujad läbinud k.a. novembris ADDENDA koolituse „Isikuandmete kaitse ja avaliku teabe seaduse täitmine"."

Anija vald teatab, et „vallavalitsuse sisekorraeeskirja § 21 sätestab:

"V TEENISTUSE TÕTTU TEATAVAKS SAANUD SALADUSED § 21. Kõik ametnikud on kohustatud hoidma saladuses asutusesiseselt kasutatavat infot (k.a hallatavaid asutusi puudutav info), isikuandmeid ja muid delikaatseid andmeid, mis on neile teatavaks saanud nii otseselt, seoses oma teenistusülesannete täitmisega, kui ka neid mis on teatavaks saanud juhuslikult. Samuti tuleb saladuses hoida asutuse turvasüsteeme ning salakoode puudutav informatsioon".

Rahvastikuregistri andmete töötlemiseks on Anija vald, Siseministeerium ja AS Andmevara

12.03.2003 sõlminud lepingu nr 10.1-3/63/373-03KOV 140 mille punkt 3.2.4 sätestab: Kasutaja on kohustatud hoidma salajas kõiki rahvastikuregistri kasutamiseks vajalikke paroole ja kasutajatunnuseid.

Oleme arvamusel, et sisekorraeeskirjas ning lepingus fikseeritud kohustused hoida saladuses salakoode ja paroole puudutav info on piisavad, tagamaks isikuandmete töötlemine vastavalt isikuandmete kaitse seaduse nõuetele. Samuti on ametniku vastutus määratud ka ametijuhendis, näiteks registripidaja ametijuhendis on vastutus fikseeritud alljärgnevalt:

"5.1. Registripidaja vastutab:

5.1.1. isiklikult oma tööülesannete õigeaegse ja korrektse täitmise eest; 5.1.2. registriandmete säilimise ja salastatuse tagamise eest seoses isikuandmete ja andmekogude kaitse nõuetest kinnipidamise kohustusega; 5.1.3. talle ametikoha tõttu teatavaks saanud riigi- ja ärisaladuse, teiste inimeste perekonna- ja eraellu puutuvate andmete ning muu ainult asutusesiseseks kasutamiseks määratud informatsiooni hoidmise eest;""

Jõhvi vald märgib täiendavalt, et:

„1. Esitatud aruande eelnõu toob välja asjaolu, et puudujäägid isikuandmete kaitsel algavad juba riiklikest andmekogudest, mistõttu saab vaid tõdeda, et vastava seadusandluse kehtestamisel ei ole arvestatud andmetöötlejate reaalse olukorra ja valmisoleku ning ressurssidega seaduse rakendamisel.

2. Aruande neljanda lehe lõpus on märgitud, et KMA on loonud lahenduse, kus inimestel on võimalus riigiportaalis elektrooniliselt vaadata, kes ja kunas on nende kohta kogutud andmeid vaadanud. Nimetatud väide ei ole tõene, kuna vastava päringu tegi mitmeid kordi vallasekretär ning algselt vastas süsteem, et vallasekretär on ise päringu teinud oma andmete kohta, kuid ühtegi ametnikku-ametkonda riigiportaal siiski ei kajasta.

3. Aruande punktis 53 on Riigikontroll veendunud, et andmete peegeldamine eraldi andmebaasi või dubleerivasse keskkonda sama andmebaasi sees on põhjendamatu, sest muudab keerukamaks andmekogu haldamise ja isikuandmete kaitse – oleme Riigikontrolli sellise veendumusega nõus, kuid kuidas käituda olukorras, kus koolikohustuslike laste arvestust tuleb KOVidel pidada paberkandjal, samas on olemas EHIS, kus võiks kõik kajastuda, kuid milline süsteem ei anna vastust päringule olukorras, kus KOV territooriumil elava kuid teise KOVi koolis käiva lapse koolikohustuse täitmise kohta.

4. Punktis 78 toodud kasutamata kontode kustutamise osas tuleks kaaluda sertifikaadi aegumise tähtaega (võib-olla isegi iga registrit eraldi vaadelduna) või siis süsteemi, kuidas kasutajakontosid taastada või avatuna hoida tähtajalisena või teatud

tähtaegadel, sest tavaolukorras, kus asutuses on nt andmekogu üks põhi andmetöötleja, kuid teine ligipääs on võimaldatud põhitöötaja asendajale puhkuse ajaks, sellisel juhul põhitöötajat asendav isik andmekogu ei kasutagi."

Torma vald on seisukohal, et kontrolliaruande eelnõu on igati asjakohane ja argumenteeritud ning toob välja mõned olulisemad seisukohad, „mis vajaksid erilist tähelepanu Riigikogu riigieelarve kontrolli komisjonile esitatavas aruandes:

a) registritesse sisselogimisel peaks kõik kasutama ID-kaardiga autentimist, siis ei tekiks ka olukorda, kus ühes asutuses kasutatakse ühte parooli mitme töötaja poolt;

b) omavalitsustes tõhustada teavitustööd kehtivatest isikuandmete kaitse nõuetest (info peaks olema üheselt mõistetav - koolituste info on erinev);

c) EHIS-s tagada suurem turvalisus ning täiendada tarkvara (näit. selles osas, mis puudutab KOVi territooriumil elavaid lapsi, kes õpivad väljaspool antud KOVi territooriumi, ei ole võimalik teha päringuid nende õpilaste kohta);

d) delikaatsete isikuandmete töötlemise registreerimine AKIs peaks olema üheselt mõistetav – kas registreerimise taotluse esitab RR kohta KOV või siseministeerium;

e) registritesse logimise registreerimiseks ja hilisemaks järelevalveks võiks toimida ühtne registreerimissüsteem (võimalusena võiks olla registris endas vastava märke tegemise koht)."

Riigikontrolli soovitused	Auditeeritute vastused
ISKE rakendamine 18. Viia andmekogud ISKE nõuetega kooskõlla ning esimesel võimalusel ajakohastada teave oma andmekogu kohta RIHAs. Esmatähtis on hinnata oma infosüsteemide tegelikku turbevajadust lähtuvalt andmete iseloomust ning ühildada see ISKE nõuetega. **(p-d 11–17)**	**Majandus- ja Kommunikatsiooniministeerium** ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega. **Haridus- ja teadusminister** teatab, et Haridus- ja Teadusministeeriumi juristid määravad kindlaks õigusaktid, millele vastavalt kehtestatakse konkreetsed nõuded ning neile vastavalt teostatakse ISKE nõudeid silmas pidades andmekogu inventuur. **Kaitseminister** nõustub esitatud ettepanekuga. **Kaitseressursside Ameti peadirektor** teatab, et KTKRi osas on andmekogu haldaja käesolevaks ajaks läbi viinud infosüsteemide turvanõuete hindamise ISKE järgi ning määranud turvaklassi, lähtudes tegelikust turbevajadusest. **Maksu- ja Tolliameti peadirektor** antud soovituse osas seiskohta ei avalda. **Kodakondsus- ja Migratsiooniamet** teatab, et „vastavalt Vabariigi Valitsuse 28.02.2008 määruse nr 58 „Riigi infosüsteemi haldussüsteem" § 33 lõikele 4 on KMA 28.05.2008 esitanud taotluse saada pikendust RIHA-sse kantavate andmete tähtaja suhtes, MKM on rahuldanud taotluse 29.05.2008. Taotluse kohaselt oli septembris 2008 ITDAK-i kohta dokumentatsioon koostamisel, mistõttu ei olnud auditeeritava perioodi vältel ITDAK-i kohta varasemalt RIHA-sse kantud andmed korrektsed. Tänaseks on RIHA-sse ITDAK-i kohta andmed esitatud (vastavalt süsteemi võimalustele). KMA-s on infovarad inventeeritud ning neile määratud turbeastmed KMA peadirektori 15.07.2008 käskkirjaga nr 188. KMA on teinud investeeringuid ja võtnud kasutusele erinevaid meetmeid seoses ISKE rakendamisega. Kuna Siseministeerium kavandab liita KMA alates 2010. a Politsei- ja Piirivalveameti koosseisu, ei ole võimalik esialgu pikaajalisi turbe tegevuskavasid kehtestada ja rakendada. Lisaks pärsivad nimetatud kavade kehtestamist ja rakendamist käesoleval perioodil info- ja kommunikatsioonitehnoloogia (IKT) konsolideerumine Siseministeeriumi infotehnoloogia- ja arenduskeskusesse, mille esimene etapp (IKT põhi- ja arendusteenuste konsolideerimine, sh IT infrastruktuurilised baasteenused, side infrastruktuuride baasteenused, tarkvara arendus- ja haldusteenused) on kavas lõpetada 2010. a alguseks." **Regionaalminister** teatab, et „ISKE rakendamist on alustatud. Turvaklassid on määratud ja kavas sätestada ka rahvastikuregistri seaduse muutmise seaduses. Turvaklassid on sisestatud ka RIHA infosüsteemi. Samade turvaklasside saavutamine on ka üks eesmärkidest, mis on toodud Euroopa Liidust taotletud rahaliste vahendite saamiseks tehtud taotluses ja mille saavutamise garanteerivad rahvastikuregistri täiendamise projekti käigus tehtavad infotehnoloogilised tööd ja uued seadmed, mis on soetatud ja osaliselt veel soetatakse projekti käigus. Koostöös rahvastikuregistri volitatud töötleja AS Andmevaraga alustatakse ISKE dokumentatsiooni kirjutamisega, mis lisanduks seaduses toodule. Rahvastikuregistri uue tarkvara lõpliku valmimise järgselt on Siseministeeriumil kavas tellida sõltumatult turvaeksperdilt täiendav turvaaudit, et olla veendunud, et rahvastikuregister vastab seaduses fikseeritud ISKE nõuetele." **Sotsiaalkindlustusameti peadirektor** nõustub soovitusega ning märgib, et „27.01.2006 aasta ministri käskkirjaga nr 22 on IT vara haldamine ja sellega seonduvate dokumentide koostamine üle läinud Sotsiaalministeeriumile. ISKE

Riigikontrolli soovitused	Auditeeritute vastused
	rakendamine on Sotsiaalministeeriumi valitsemisalas jõudnud projekti I etapi lõpetamiseni (infovarade inventar, turvapoolitika koostamise projekt ja turvaklasside määramine). Projekti lõpptähtajaks on märgitud 17.03. 2009 ning siis hakatakse meetmeid rakendama. RIHAsse on SKA oma andmed sisestanud vana korra järgi. Hetkel toimub andmete kaardistamine ning uue korra järgi hakatakse sisestama enne 2009 a saabumist".
Infoturbe dokumentatsioon 26. Korrastada andmekogude dokumentatsioon MKMi soovitustest lähtuvalt. Optimeerida ja viia üksteisega kooskõlla eraldi seisvad IT-korralduslikud dokumendid, arvestades asjaolu, et andmekogu kasutajal oleks hõlbus leida teda puudutavad infoturbealaseid juhendeid. Dokumentide sõnastamisel pidada silmas, et adressaatide ring on IT-valdkonna spetsialistidest laiem. **(p-d 19–25)**	**Majandus- ja Kommunikatsiooniministeerium ja Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega. **Haridus- ja teadusminister** teatab, et vastav dokumentatsioon on ajakohastamisel ning on kättesaadav ministeeriumi autoriseeritud kasutajatele mõeldud veebilehelt. **Kaitseminister** nõustub soovitusega. **Kaitseressursside Ameti peadirektor** teatab, et käesolevaks ajaks on tehtud soovitus rakendatud ning kindlasti arvestab KRA seda ka edaspidi andmekogu dokumentatsiooni täiendamisel. **Maksu- ja Tolliameti peadirektor** jätab soovituse osas oma seisukoha avaldamata. **Kodakondsus- ja Migratsiooniamet** teatab, et Siseministeeriumi haldusala IKT on kavas konsolideerida Siseministeeriumi infotehnoloogia- ja arenduskeskusesse ning lisaks on, tulenevalt KMA liitmisest Politsei- ja Piirivalveameti koosseisu, vajalik korrastada ka haldusalas IT-alased dokumendid. **Regionaalminister** teatab, et 2009. aasta alguses alustatakse olemasolevate infoturbe dokumentide analüüsiga. Analüüsi tulemust ja Riigikontrolli soovitusi arvesse võttes tehakse muudatused ja täiendused olemaolevatesse dokumentidesse. **Sotsiaalkindlustusameti peadirektor** nõustub soovitusega ja teatab, et „uue infoturbepoliitika tegemisel järgitakse soovitust. Lähtuvalt punkti 18 vastusest edastame auditi soovitused Sotsiaalministeeriumile".
27. Kehtestada asutuses infoturbepoliitika. **(p-d 19–25)**	**Sotsiaalkindlustusameti peadirektor** nõustub auditi soovitusega ning märgib, et: „SKAle on koostatud esimene infoturbe kontseptsioon 2000 a AS Cybernetica poolt. Uut infoturbepoliitika dokumenti hakati koostama 2005 a lõpus ning see jäi projekti staadiumisse. Seda ei jõutud peadirektori käskkirjaga kinnitada seepärast, et enne jõuti teatavaks teha plaan infotehnoloogia teenuste halduse konsolideerimisest Sotsiaalministeeriumi valitsemisalas. Uus ja ühtne infoturbe poliitika koostatakse ISKE raames Sotsiaalministeeriumi poolt kõigile oma allasutustele. Auditi soovitused edastame Sotsiaalministeeriumile."
28. Täiendada sisekorraeeskirju või asjaajamiskorda IT osas või kehtestada arvutivõrgu ja infotehnoloogia kasutamise eeskirjad, mis muu hulgas hõlmaksid paroolihaldust ja järelevalve korraldust isikuandmete kaitse aspektist. **(p-d 19–25)**	**Ambla vald** peab otstarbekaks esimesel võimalusel kehtestada ametiasutuse arvutivõrgu ja infotehnoloogia kasutamise eeskirjad, mis muu hulgas hõlmaksid paroolihaldust ja järelevalve korraldust isikuandmete kaitse aspektist, ning ajakohastada asutusesisesed muud dokumendid. **Anija vald** on arvamusel, et vallavalitsuse sisekorraeeskirjas ning Siseministeeriumi ja AS Andmevaraga sõlmitud lepingus RRi kasutamiseks fikseeritud kohustused hoida saladuses salakoode ja paroole puudutav info on piisavad tagamaks isikuandmete töötlemine vastavalt isikuandmete kaitse seaduse nõuetele (valla vastuse täisteksti on võimalik lugeda tabelist lk 54). **Riigikontrolli kommentaar:** Leiame, et sisekorraeeskirjas antud valdkonda reguleeriv lause „samuti tuleb saladuses hoida asutuse turvasüsteeme ning salakoode puudutav informatsioon" ei ole piisav. Lisaks ei laiene rahvastikuregistri kasutamiseks sõlmitud lepingus kajastatud paroolide ja kasutajatunnuste hoidmise reeglid valla üldisele infotöö korraldusele. **Antsla vald** teatab, et kehtestab arvutivõrgu ja infotehnoloogia kasutamise eeskirja. **Audru vald** ei esitanud vastamistähtaja ja täiendava nädala jooksul oma arvamust soovitusele. **Haapsalu linn** peab soovitust asjakohaseks ning valmistab ette vajalike muudatuste sisseviimist sisekorraeeskirjadesse. **Jõhvi vald** teatab, et neil on plaanis koostada arvutivõrgu ja infotehnoloogia kasutamise eeskirjad, mis muu hulgas hõlmaksid paroolihaldust ja järelevalve korraldust isikuandmete kaitse aspektist. Nimetatud eeskirja loodab ta kehtestada 2009. aasta esimesel poolaastal. **Kanepi vald** teatab, et kehtestab arvutivõrgu ja infotehnoloogia kasutamise

Riigikontrolli soovitused	Auditeeritute vastused
	eeskirjad, mis hõlmavad paroolihaldust ja järelevalve korraldust. **Tapa vald** lubab vallavalitsuses viia läbi toimingud hindamaks puudjääke vallavalitsuse seda valdkonda reguleerivas dokumentatsioonis ja arvestab riigikontrolli ettepanekuid nende täiendamisel. **Tõstamaa vald** teatab, et väljatöötamisel on vallavalitsuse arvutivõrgu ja infotehnoloogia kasutamise eeskiri, mis sätestab paroolide kasutamise ning andmekogule juurdepääsu omava ametniku tööülesannete täitmise. **Tartu linn** ja **Viiratsi vald** nõustuvad esitatud soovitusega. **Puka** ja **Vigala vald** teatavad, et täiendavad oma asjaajamiskorda IT osas. **Torma** ja **Jõelähtme vald** ei avalda oma seisukohta soovituse osas.
Alluvussuhted andmekogu haldamisel 35. Leppida kokku vastutus PKRi haldamise, sh isikuandmete õiguspärase kasutamise järelevalve osas ning tagada selge tööjaotus ja infovahetus. Kuni vastutav töötleja on SKA, peaks ka andmekogu haldamisega seotud ametnikud kuuluma SKA koosseisu. **(p-d 29–34)**	**Sotsiaalkindlustusameti peadirektor** nõustub auditi soovitusega ning märgib järgmist: „Juba 08.11.2007 tegi SKA ettepaneku Sotsiaalministeeriumile alustada läbirääkimisi tööjaotuse selgemaks muutmise osas. Hetkel on osapooled alustanud aktiivselt lahenduste otsimist auditiaruandes välja toodud vastutava ja volitatud töötleja märkuste lahendamiseks." **Sotsiaalminister** teatas, et hetkel toimuvad Sotsiaalministeeriumi ja Sotsiaalkindlustusameti vahel töökoosolekud leppimaks kokku riikliku pensionikindlustuse registri tööjaotuse osas.
Kasutajate teavitamine andmekaitse reeglitest 41. Täiendada andmekogu kasutajatele mõeldud juhendeid isikuandmete kaitse reeglitega. Uue kasutaja esmasel sisenemisel andmekogusse on võimalik kuvada andmekogu kasutamisreeglite, sh isikuandmete kaitse alaste reeglite loetelu, millega kasutaja peab edasiste toimingute tegemiseks tutvuma ja nendega nõustuma. Samuti võib igakordsel sisenemisel andmekogusse tutvustada juhendites tehtud muudatusi ja kuvada meeldetuletust, et andmeid tohib kasutada konkreetsete tööülesannete täitmiseks. **(p-d 36–40)**	**Majandus- ja Kommunikatsiooniministeerium** ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega. **Haridus- ja teadusminister** teatab, et Haridus- ja Teadusministeerium lisas andmekogu kasutajaliidese juurde vastava juhendi isikuandmete töötlemise põhimõtetega. Arvestame ettepanekut ning loome vastava funktsionaalsuse menüü valiku ette, kus auditeeritav peab kinnitama teadete lugemist enne funktsionaalsuseni jõudmist. **Kaitseminister** nõustub tehtud soovitusega. **Kaitseressursside Ameti peadirektor** arvestab tehtud soovitusega 2009 aasta KTKR-i arendustööde teostamisel. **Maksu- ja Tolliameti peadirektor** teatab, et „rakendusse logimisel ei ole otstarbekas kuvada põhjalikku selgitust kasutamisreeglite, s.h turvanõuete kohta. Ilmselt on lahenduseks uue töötaja värbamisel talle kohe allkirja vastu "Infosüsteemide kasutamise korra" tutvustamine". **Riigikontrolli kommentaar:** Riigikontroll nõustub, et uue töötaja värbamisel tuleb talle allkirja vastu tutvustada tema tööd puudutavaid eeskirju, kuid leiab, et nende dokumentide väiksemahuliste muudatuste või täienduste tutvustamine ja andmekaitse reeglite perioodiline meenutamine ning nendega tutvumise kohta kinnituste kogumine on kõigile osapooltele lihtsam andmekogusse sisselogimisel, kuna see on nende igapäevane töövahend. **Kodakondsus- ja Migratsiooniamet** teatab, et „2009. a eelarve ja investeeringute vähendamise tõttu on KMAs suunatud arendustööd nendesse valdkondadesse, mis on prioriteetsete põhiülesannetena määratletud (VIS, SIS, biomeetria rakendamine jne), ning lisaks meetmetele, mis on seotud andmebaaside ja infosüsteemide teenustaseme säilitamiseks või olemasolevate lepinguliste kohustuste täitmiseks. Kuid KMA viib regulaarselt läbi andmekaitsealaseid koolitusi, millega tagatakse andmekogu kasutajate teadlikkus andmekaitsealastest reeglitest." **Regionaalminister** teatab, et „vastavalt kasutatavale infotehnoloogilisele lahendusele ilmub rahvastikuregistrile juurdepääsu soovivale kasutajale ekraanile teavitustekst, kus on toodud ära andmete kasutamise ainukese eesmärgina ametiülesannete täitmine, samuti teavitatakse kasutajaid sellest, et registri kasutamise üle teostatakse järelevalvet. Samuti saavad kõik registri uued kasutajad AS-lt Andmevara suulised instruktsioonid enne kasutajaõiguste üleandmist. Uue tarkvara valmimisel on võimalik seda teksti täiendada ja lisada täiendav informatsioon juhendi näol". **Sotsiaalkindlustusameti peadirektor** nõustub soovitusega ning märgib, et „SKAs on määratud isikuandmete kaitse eest vastutav isik, kes teostab järelevalvet isikuandmete kaitse seaduse, avaliku teabe seaduse ja ametis kehtestatud juhendite ning kordade üle. Lisaks teeb ta vähemalt korra aastas igas regioonis ühe andmekaitsealase sisekoolituse. Iga kahe nädala tagant koguneval juhtkonna koosolekul juhib ta juhtide tähelepanu asjaoludele, millele

Riigikontrolli soovitused	Auditeeritute vastused
	tuleb tähelepanu pöörata. Samuti toimub infosüsteemide paroolide kättejagamisel õiguste ja kohustuste tutvustamine. Füüsiliste ja organisatsiooniliste turvameetmete täiustamine leiab aset infoturbepoliitika koostamisel Sotsiaalministeeriumi poolt. Auditi soovitused edastame Sotsiaalministeeriumile."
Delikaatsete isikuandmete töötlemise registreerimine 55. Soovitus AKI-le: ▪ Viia läbi delikaatseid isikuandmeid sisaldavate andmekogude haldajate riskianalüüs ning suurema riskitasemega andmekogude haldajate juures kontrollida isikuandmete kaitse nõuete järgimist ka kohapeal. ▪ Tõhustada teavitustööd ning võtta kasutusele täiendavaid meetmeid (juhendite koostamine, vajaduse korral väärteomenetluse algatamine) selleks, et haridusasutused ning valla- ja linnavalitsused, kes juba töötlevad delikaatseid isikuandmeid, oleksid teadlikud neile kehtivatest isikuandmete kaitse nõuetest, registreeriksid end delikaatsete isikuandmete töötlejatena ning tegelikkuses tagaksid delikaatseid isikuandmeid sisaldavate andmekogude ja nende kasutamise piisava turvalisuse. **(p-d 42–54)**	**Andmekaitse Inspektsiooni peadirektor** teatab, et Andmekaitse Inspektsioon analüüsib põhjalikult talle tehtud ettepanekuid juhendite väljatöötamiseks ja vajaduse korral lülitab need 2009. aasta tööplaani.
Dubleeritud isikuandmed 56. Lõpetada registreerimata dubleeriva andmekogu pidamine ning tagada välistele andmesaajatele nende seadusest tulenevate või seaduse alusel pandud kohustuste täitmiseks vajalik juurdepääs andmetele teiste lahenduste kaudu. **(p-d 51, 53)**	**Sotsiaalkindlustusameti peadirektor** ei nõustu soovitusega ja selgitab, et: „SKA ühines X-teega kui Eesti riigi põhilisi andmebaase ühendava turvalise andmevahetuskihiga juba 2002. a, olles üks esimesi X-teega ühinenud riigiasutusi. X-tee päringute teostamise tehnoloogia realiseeriti selle tarbeks spetsiaalsete andmetabelite moodustamise teel. Sellise tehnoloogia kasutamise eesmärgiks oli võimalikult kiiresti vastata teise ametkonna päringutele, tagamaks sellejuures registri andmete turvalisus. X-teele välja kantud andmeid võiks võrrelda andmeaidaga, kus välja ei kanta kogu online baasi infot, vaid antud eesmärgi huvides korrastatud infot. Nagu andmeait, nii ei ole ka X-teele välja kantud info kasutajate poolt muudetav, vaid ette nähtud üksnes päringute teostamiseks. X-teele andmete väljakandmise puhul ei tehta andmete lisamist, vaid vanad andmed kustutatakse. Sellest nähtub väga täpselt, et ei ole tegemist eraldi andmekoguga, vaid on kuuajalise väljavõttega vahetabelid." **Riigikontrolli kommentaar:** Vastavalt avaliku teabe seaduse § 43¹ nimetatakse andmekoguks korrastatud andmete kogumit, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks. Ka regulaarselt ajakohastatavat väljavõtet PKRi andmebaasist tuleb käsitleda kui andmekogu.
57. Lõpetada reaalsete isikuandmetega dubleeriva keskkonna kasutamine EHISes. **(p-d 52–53)**	**Haridus- ja teadusminister** teatab, et alates 01.11.2008. a on Haridus- ja Teadusministeerium lõpetanud reaalsete isikuandmete töötlemise EHISe arenduskeskkonnas.
Juurdepääsu võimaldamine välistele andmesaajatele 58. Enne andmekogu delikaatsetele isikuandmetele juurdepääsu lubamist kontrollida, kas juurdepääsu taotleja on määranud isikuandmete kaitse eest vastutava isiku või registreerinud end AKIs delikaatsete isikuandmete töötlejana. **(p-d 42–54)**	**Majandus- ja Kommunikatsiooniministeerium** ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega. **Haridus- ja teadusminister** teatab, et täiendab protseduurireegleid uute kasutajate lisamisel. Vastav funktsionaalsus luuakse asutuse administraatori juurde rolli lisamise alla. **Kodakondsus- ja Migratsiooniamet** teatab, et „KMA hinnangul IKS-ist ei tulene, et kõigil andmete töötlejatel on kohustus registreerida delikaatsete isikuandmete töötlemine, vaid selline kohustus on pandud vastutavale töötlejale. IKS-i eelnõu seletuskirjas on selgitatud järgnevalt: „erinevalt kehtinud IKS-ist on eelnõus endise pideva vastutava töötleja ja volitatud töötleja eristamise asemel räägitud üldisest isikuandmete töötlejast. Vastutava ja volitatud töötleja eristamisest siiski täielikult loobuda ei ole olnud võimalik, sest mõningad kohustused IKS-is kehtivad üksnes vastutava töötleja suhtes, nt on delikaatsete isikuandmete töötlemise AKI-s kohustatud registreerima vastutav töötleja, mitte

Riigikontrolli soovitused	Auditeeritute vastused
	aga volitatud töötleja (§ 27 lg 1), kes töötleb isikuandmeid vastutava töötleja järelevalve all, kusjuures vastutav töötleja ei vabane vastutusest nende isikuandmete töötlemise eest.“ IKS § 7 lg 3 annab volitatud töötlejale definitsiooni: 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. Antud selgitus viitab asjaolule, et volitatud/välised töötlejad (sh lepingulised töötlejad) ei ole kohustatud delikaatsete isikuandmete töötlemist registreerima AKI-s.” **Riigikontrolli kommentaar:** Andmekogu vastutaval töötlejal on kohustus registreerida endapoolne delikaatsete isikuandmete töötlemine. Kui vastutav töötleja on andmekogule määranud volitatud töötleja, siis peab eelnimetatud töötlemise taotluse volitatud töötleja eest esitama vastutav töötleja. See ei vabasta delikaatsete isikuandmete registreerimise kohustusest väliseid andmesaajaid ehk IKSi mõistes kolmandaid isikuid, kes peavad ise registreerima delikaatsete isikuandmete töötlemise või määrama isikuandmete kaitse eest vastutava isiku. **Regionaalminister** teatab, et „enne juurdepääsuõiguste andmist delikaatsele isikuandmetele kontrollitakse Siseministeeriumi poolt alati, kas kasutaja vastab selliste andmete töötlemiseks õiguse saamise tingimustele. Kui kasutaja nimetatud tingimustele ei vasta, siis juurdepääsu ei anta enne, kui vastavad õigused on AKI-lt saadud“. **Sotsiaalkindlustusameti peadirektor** nõustub soovitusega ja selgitab, et „delikaatsete isikuandmete päringute puhul, mida ei soorita KOVid, teostab Sotsiaalkindlustusameti andmekaitse peaspetsialist alati kontrolli AKI kodulehel olevast registrist, kas päringut sooritav asutus on end registreerinud delikaatsete isikuandmete töötlejana”.
KOVide registreerimine delikaatsete isikuandmete töötlejana 59. Kindlustada delikaatsete isikuandmete töötlemise vastavus IKSile ja registreerida selleks delikaatsete isikuandmete töötlemine AKIs või määrata isikuandmete kaitse eest vastutav isik. **(p-d 42–54)**	**Ambla vald** teatab, et kindlustamaks delikaatsete isikuandmete töötlemise vastavus IKSile, registreerivad nad esimesel võimalusel KOVi delikaatsete isikuandmete töötlejana AKIs. **Anija vald** teatab, et on vastavalt isikuandmete kaitse seaduse § 27 ja § 30 isikuandmete kaitse eest vastutavaks isikuks määranud registripidaja, mille kohta on vormistatud vallavanema käskkiri 17.11.2008 nr 193. **Antsla vald** nõustub soovitusega ja teatab, et valmistab ette dokumente AKIs registreerimiseks. Lisaks valmistab vald, koostöös maakonna IT spetsialisti abiga kogu maakonna omavalitsustele, ette dokumentatsiooni ISKE nõuete täitmiseks. **Audru vald** ei esitanud vastamistähtaja ja täiendava nädala jooksul oma arvamust soovitusele. **Haapsalu linn** teatab, et on alustatud eeltöid isikuandmete kaitse eest vastutava isiku määramiseks. **Jõelähtme vald** teatab, et on alustanud toiminguid Jõelähtme Vallavalitsuse registreerimiseks AKIs delikaatsete isikuandmete töötlejana. **Jõhvi vald** teatab, et alustas vastava taotluse koostamisega nii vallavalitsuse kui ka hallatavate asutuste registreerimiseks AKIs. Taotluse plaanitakse esitada veel 2008. aastal. **Kanepi vald** teatab, et Kanepi Vallavalitsuse 07.11.2008. a korraldusega nr 228 on määratud isikuandmete kaitse eest vastutav isik. **Tapa vald** teatab, et viib läbi hindamise, kas vallavalitsusele, lähtuvalt vallavalitsuse haldussuutlikkusest ja delikaatsete isikuandmete töötlemise mahust, on otstarbekam registreerida delikaatsete isikuandmete töötlemine AKIs või määrata isikuandmete kaitse eest vastatav isik. Otsuse tegemine IKSi vastava regulatsiooni täitmiseks on võimalik pärast vastava hindamise läbiviimist. **Torma vald** avaldab, et delikaatsete isikuandmete töölemise registreerimine AKIs peaks olema üheselt mõistetav – kas registreerimise taotluse esitab RR kohta KOV või Siseministeerium. **Riigikontrolli kommentaar:** Valla näol on IKSi mõistes tegemist kolmanda isikuga, kellele antakse juurdepääs rahvastikuregistrile. Sel juhul peab delikaatsete isikuandmete töötlemise või isikuandmete kaitse eest vastutava isiku määrama vald. Kui see ülesanne oleks Siseministeeriumil, siis peaks viimane kontrollima kõigi KOVide vastavust IKSi nõuetele. See ei ole kõikide kolmandate isikute osas mõeldav ega otstarbekas.

Riigikontrolli soovitused	Auditeeritute vastused
	Tõstamaa vald teatab, et nad registreerivad isikuandmete töötlemise AKIs vastavalt kehtivale seadusandlusele. **Viiratsi vald** nõustub soovitusega.
Juurdepääsuõiguse ja -vajaduse dokumenteerimine 72. Vaadata üle andmekogude juurdepääsuõigusi ja tööülesandeid kirjeldavad dokumendid asutuses (näiteks ametijuhendid) nii, et neist ilmneks andmekogudele juurdepääsuõiguse vajadus ja selle ulatus. **(p-d 62–71)**	**Majandus- ja Kommunikatsiooniministeerium** ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega. **Haridus- ja teadusminister** nõustub soovitusega. **Kaitseminister** ja **Kaitseressursside Ameti peadirektor** nõustuvad soovitusega. **Maksu- ja Tolliameti peadirektor** teatab, et „andmekogule juurdepääsuõiguse taotluses on ametniku vahetul ülemusel kohustuslik märkida kasutajagrupp (õiguste ulatus), juurdepääsu ajaline periood ja kasutamise põhjendus (vajadus). Ametijuhenditesse andmekogude ja nende kasutajagruppide sissekirjutamist ei pea otstarbekaks, kuna siis tuleks suurema osa ametnike ametijuhendeid suhteliselt sageli muuta“. **Kodakondsus- ja Migratsiooniamet** teatab, et „ametisiseselt on ametnikele ITDAK-le juurdepääsuõiguse andmine reguleeritud käskkirjaga, milles on ette nähtud protsess volituse saamiseks ning lõpetamiseks ja sama käskkirjaga peetakse ka ülevaadet kõigist olemasolevatest ametisisestest volitustest. Ametivälised juurdepääsud avatakse eeldusel, et vastav asutus on teinud taotluse KMA-le ning et neil on olemas seaduslik alus andmete töötlemiseks. Enne andmevahetuse avamist teeb KMA analüüsi, kas taotleval asutusel on õiguslik alus olemas ning kas taotluses soovitud andmehulk vastab eelkõige eesmärgipärasuse ja minimaalsuse põhimõtetele ning milline tehniline lahendus on vajalik/võimalik. Kui kõik eelnev on korras, siis tehakse taotlevale asutusele ettepanek reguleerida andmevahetus lepinguga ning ühtlasi sätestab KMA nõuded andmete töötlemiseks nimetatud lepingus (sh pidada arvestust volituste üle ja ka KMA pädevuse teha järelevalvet andmete töötlemise üle)“. **Regionaalminister** teatab, et Siseministeerium vaatab üle kõigi oma asutuse siseste kasutajate ametijuhendid ja täpsustab neid juurdepääsuõiguste vajaduse ja ulatuse osas. **Sotsiaalkindlustusameti peadirektor** nõustub soovitusega ja märgib, et „SKA teenistujate juurdepääsu dokument viiakse kooskõlla lähtuvalt viimasest struktuurimuudatusest. Punktis 70 ei nõustu auditi soovitusega ja selgitame järgmist. Pensioniameti peaspetsialisti ametijuhendis ei ole sõltumatu järelevalve teostaja rolli. Peaspetsialisti ülesandeks on uue töötaja puhul arvutivõrgu kasutusloa taotluse projekti koostamine.” **Riigikontrolli kommentaar (punkti 70 osas):** Kui peaspetsialisti tööülesannete hulka ei kuulu ametnike juurdepääsuõiguste põhjendatuse hindamine, siis puudub Pensioniametites andmekogudele ligipääsude loomisel taotlejast sõltumatu juurdepääsuulatuse hindamine.
Individuaalse juurdepääsu tagamine ja päringu põhjuse tuvastamine 79. Teha ID-kaart peamiseks autentimisvahendiks andmekogule juurdepääsu andmisel ning välistada seeläbi kasutajakonto jagamine. **(p-d 73–78)**	**Eesti Riikliku Autoregistrikeskuse direktor** nõustub soovitusega. **Sotsiaalkindlustusameti peadirektor** nõustub soovitusega ja märgib, et „ettepanek võetakse arvesse ja katsutakse leida rahalised vahendid ID-kaardiga autentimiseks. Seoses 27.01.2006 a ministri käskkirjaga nr 22 on IT vara haldamine ja sellega seonduvate riigihangete teostamine üle läinud Sotsiaalministeeriumile. SKA pädevusse on jäänud ainult ettepanekute tegemine. Auditi soovitused edastame Sotsiaalministeeriumile“. **Maksu- ja Tolliameti peadirektor** teatab, et „hetkel on MTA rakendustes võimalik autentida ka ID-kaardiga ja see ongi levinuimaks autentimisvahendiks. Samuti on ID-kaardi lugejad kõikidel ametnikel kättesaadavad. Siiski ei ole meil lähiajal plaanis välistada kasutajatunnuste võimalust“.
80. Tagada pikalt kasutamata seisnud kasutajakontode sulgemine ja kustutamine. Sätestada infoturbe dokumentatsioonis ja väliste andmesaajatega sõlmitavates lepingutes tingimused kontode deaktiveerimiseks ja kustutamiseks ning sellega seotud tähtajad. **(p-d 73–78)**	**Majandus- ja Kommunikatsiooniministeerium** ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega. **Haridus- ja teadusminister** teatab, et „EHISe volitatud töötleja on seni sulgenud kõik kontod, mida ei ole kasutatud viimase 12 kuu jooksul. Lisame andmevahetuslepingutes kontode haldamise põhimõtete juurde lisatingimused konto kehtivuse osas. Samuti tuleb luua automaatne kontode sulgemine koos teavitusega konto sulgemisest kasutaja poolt antud meiliaadressile“. **Kaitseminister** nõustub soovitusega. **Kaitseressursside Ameti peadirektor** teatab, et KTKRi osas on soovitus rakendatud.

Riigikontrolli soovitused	Auditeeritute vastused
	Maksu- ja Tolliameti peadirektor teatab, et „MTA siseselt sulguvad pikalt kasutamata kasutajakontod automaatselt. Väliste andmesaajatega sõlmitavatesse lepingutesse peame sellise lisasätte sisseviimist põhjendatuks.” **Kodakondsus- ja Migratsiooniamet** teatab, et „KMA-s peavad osakonnajuhatajad vähemalt kord poole aasta jooksul vaatama üle kõik ametnikele antud volitused ning lisaks võib ka jooksvalt neil tulla ette vajadus vaadata üle oma osakonna ametnikele antud volitused. Välistel töötlejatel on andmevahetuslepingu kohaselt kohustus pidada arvestust antud volituste üle ning KMA-l on õigus kontrollida nende reaalsusega vastavust.” **Regionaalminister** teatab, et „kasutajate õiguste lõpetamine on osaliselt automaatne ja osaliselt tagatud lepingute täiendamise protseduuri käigus. Samuti teostab volitatud töötleja esindaja korrapärast kontrolli kasutajate üle ja kui ilmneb, et mõne asutuse kasutaja ei ole juba mitmel kuul järjest päringuid teinud, siis pöördutakse selgituste saamiseks vastava asutuse poole ja koostöös korrastatakse juurdepääsu andmed. Kasutajate õiguste lõpetamise kord on fikseeritud ka kasutajatega sõlmitavates lepingutes“. **Sotsiaalkindlustusameti peadirektor** nõustub soovitusega ning märgib, et „SKA infosüsteemis on varasemast ajast juba kasutusele võetud süsteem, et kui isik ei ole kaks kuud oma kontot kasutanud, siis see deaktiveeritakse. Juhul kui ISKE raames valmib infoturbe dokumentatsioon, siis sinna lisatakse kontode sulgemise täpne regulatsioon. Auditi soovitused edastame Sotsiaalministeeriumile.”
81. Kui KOVis teevad päringuid andmekogule juurdepääsuõigust omavad ametnikud lisaks oma tööülesannetele ka teiste isikute palvel, siis luua süsteem, millega oleks võimalik tagada päringu algataja ja päringu põhjuse hilisem tuvastamine. **(p-d 73–78)**	**Ambla vald** teatab, et välistab ametiülesannete väliste päringute tegemist töökorraldusega. Nende hinnangul on ametiülesannete väliste päringute tegemine lubamatu. **Anija vald** hindab ettepanekut väga heaks ning teatab, et vallavalitsus on välja töötanud päringu esitamise vormi, milles fikseeritakse päringu esitaja ja päringu esitamise põhjus ning andmete väljastamise kuupäev päringu esitajale. Kirjalikud ja allkirjastatud päringud säilitatakse hilisema tuvastamise võimaldamiseks vastavalt isikuandmete kaitse seaduse nõuetele. **Antsla vald** nõustub ettepanekuga ja teatab, et senini on registreeritud teistele ametnikele tehtavaid päringuid registreerimisraamatus. Lisaks teeb vald ettepaneku, et registrites oleks võimalik enne päringu tegemist lisada päringu põhjus. **Audru vald** ei esitanud vastamistähtaja ja täiendava nädala jooksul oma arvamust soovitusele. **Haapsalu linn** teatab, et on rakendanud rahvastikuregistri päringute registreerimise ainult elektroonilise taotluse alusel. Teiste andmekogude kasutamise vajadust on neil vaja veel monitoorida ning vajaduse korral loovad nad ühtse süsteemi. **Jõelähtme vald** teatab, et on alustanud toiminguid sellise süsteemi loomiseks, millega oleks võimalik tagada päringu algataja ja päringu põhjuse hilisem tuvastamine. **Jõhvi vald** avaldab, et „selline süsteem on koormav igale ametnikule, kes päringuid teostavad, kuid isikuandmete päringute põhjenduse (eesmärgi) suhtes vajalik. Vastava korra kehtestame arvutivõrgu ja infotehnoloogia kasutamise eeskirja osana“. **Kanepi vald** teatab, et väljatöötamisel on taotluse vorm, kus fikseeritakse päringu põhjus. **Puka vald** märgib, et vallavalitsuses kasutavad andmekogusid volitatud isikud personaalselt ja ühist kasutamist ei toimu. Kui ametnik teeb päringuid andmekogudest teiste isikute palvel, siis ta vastutab täielikult andmekogust päringute seaduspärasuse eest. Vallavalitsus kavandab asjaajamiskorra täpsustamist IT osas, et luua päringu algatamise ja päringu põhjuse hilisema tuvastamise võimalused. **Tapa vald** teatab, et esmase lahendusena on viidud sisse süsteem päringute esitamiseks ja säilitamiseks e-mailiga, kus märgitakse ka päringu teostamise põhjus. **Torma vald** märgib, et registritesse logimise registreerimiseks ja hilisemaks järelevalveks võiks toimida ühtne registreerimissüsteem (võimalusena võiks olla registris endas vastava märke tegemise koht). **Tõstamaa vald** teatab, et väljatöötamisel on vallavalitsuse arvutivõrgu ja infotehnoloogia kasutamise eeskiri, mis sätestab lisaks muule ka teiste ametnike algatusel tehtud päringute põhjuste fikseerimise.

Riigikontrolli soovitused	Auditeeritute vastused
	Vigala vald teatab, et vallas on välja töötatud taotluse vorm, kus fikseeritakse taotleja andmed, andmete töötlemise eesmärk, kelle andmeid töödeldakse ning andmete koosseis. **Tartu linn** ja **Viiratsi vald** nõustuvad esitatud soovitusega
Kontroll sooritatud päringute üle 89. Täiendada andmekogude logimisprotseduure nii, et oleks võimalik tuvastada ka päringute sooritaja, päringu tegemise aeg, põhjus ning päringu tulemusena kuvatud isikuandmed. Seeläbi tagada piisavate logide olemasolu isikuandmete töötlemise kohta, et isikul oleks võimalik saada teavet enda andmete töötlemisest ning vastutaval töötlejal oleks võimalik teha järelevalvet andmete töötlemise üle ja kuritarvituse ilmnemisel süüdlane välja selgitada. **(p-d 82–88)**	**Sotsiaalkindlustusameti peadirektor** nõustub osaliselt auditi soovitusega ja selgitab, et sotsiaalmaksu vaatamise andmeid logitakse ja hiljem on võimalik tuvastada, kes ning millal neid andmeid vaatas. **Haridus- ja teadusminister** teatab, et „23.10.2008 a rakendus EHISes täiendav logisüsteem, mis võimaldab tagantjärgi kindlaks teha kes, millal ja milliseid isikuandmeid on vaadanud. Isikuandmete vaatamist sisaldavate logifailide säilitamisaeg on 3 kuud. Isikuandmete salvestamise, muutmise ja kustutamise logifailide arhiveerimisele ajalisi piiranguid ei ole seatud. HTMis tuleb määrata vastutav isik, kellele luuakse võimalus logidega tutvumiseks." **Riigikontrolli kommentaar:** Riigikontroll leiab, et isikuandmete vaatamist sisaldavate logifailide kolmekuuline säilitamistähtaeg on põhjendamatult lühike (vt ka punkti 94). **Eesti Riikliku Autoregistrikeskuse direktor** nõustub soovitusega.
90. Luua võimalused päringulogide hõlpsamaks kontrolliks. X-tee kaudu tehtud päringute analüüsisüsteemi arendamisel on soovitav teha koostööd teiste asutustega, kel on vastavad lahendused olemas või väljatöötamisel. **(p-d 82–88)**	**Majandus- ja Kommunikatsiooniministeerium** ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega. **Haridus- ja teadusminister** teatab, et võtab eesmärgiks logide kättesaadavaks tegemise andmevahetuskanali X-tee kaudu. **Kaitseminister** nõustub soovitusega. **Kaitseressursside Ameti peadirektor** teatab, et käesolevaks ajaks on KRAs kinnitatud vastavasisuline dokumentatsioon ja loodud infotehnoloogiline võimekus päringulogide kontrollimiseks. **Maksu- ja Tolliameti peadirektor** X-tee logide süsteemi peame adekvaatseks, kuid meelsasti oleme valmis tutvuma teiste asutuste lahendustega. **Kodakondsus- ja Migratsiooniamet** teatab, et „2009. a eelarve ja investeeringute vähendamise tõttu on KMA-s suunatud arendustööd nendesse valdkondadesse, mis on prioriteetsete põhiülesannetena määratletud (VIS, SIS, biomeetria rakendamine jne), ning lisaks meetmetele, mis on seotud andmebaaside ja infosüsteemide teenustaseme säilitamiseks või olemasolevate lepinguliste kohustuste täitmiseks." **Regionaalminister** teatab, et päringute kontrollimiseks valmib eraldi tarkvara rahvastikuregistri tarkvara täiendamise projekti käigus. **Sotsiaalkindlustusameti peadirektor** nõustub soovitusega ning edastab soovituse Sotsiaalministeeriumile (vt ka punkti 79 vastust).
Logide säilitamine 96. Kaaluda juhendi loomist, mis sätestab minimaalsed nõuded isikuandmete töötlemise logimiseks ning täpsustab, millisel juhul tuleb isiku taotlusel edastada talle masspäringu toimumise, teostaja ja põhjuse kohta samasugused andmed nagu lihtpäringu puhul (vt p 85). Lisaks peaks juhend selgitama isikuandmete töötlemisest jäävate logide säilitamise vajalikkust ja põhimõtteid, millele tuginedes asutused saavad kehtestada logidele säilitustähtaegu. Ilma vastavate suunisteta võib kujuneda olukord, kus asutustes logide säilitamise tähtaeg võib olla soovitud teabe saamiseks või järelevalvetoimingute tegemiseks liialt lühike. Eelmainitud juhendi koostamisel tuleb muu hulgas arvestada seda, kui suurt kahju on võimalik inimesele tema isikuandmete õigusvastase töötlemisega teha, samuti isikuandmete kuritarvitamisega seotud süütegude aegumistähtaegasid ning andmetöötluse järelevalve korraldust andmekogudes. **(p-d 82–88 ja 91–95)**	**Andmekaitse Inspektsiooni peadirektor** teatab, et Andmekaitse Inspektsioon analüüsib põhjalikult talle tehtud ettepanekuid juhendite väljatöötamiseks ja vajaduse korral lülitab need 2009. aasta tööplaani.

Riigikontrolli soovitused	Auditeeritute vastused
97. Määrata logide säilitamise tähtajad andmekogu põhimääruses. **(p-d 91–95)**	**Majandus- ja Kommunikatsiooniministeerium** ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega. **Haridus- ja teadusminister** teatab, et „on algatanud EHISe põhimääruse muutmise. EHISe põhimäärus on võimalik esitada ministeeriumitevahelisele kooskõlastamisele peale andmekogu registreerimist RIHA-s. Fikseerime põhimääruses isikuandmete päringute logifailide arhiveerimise tähtajad“. **Kaitseminister** ja **Kaitseressursside Ameti peadirektor** nõustuvad soovitusega. **Maksu- ja Tolliameti peadirektor** teatab, et „püüame uurida, millised piiranguid seavad logide hoidmisele EL õigusaktid ja nendest lähtudes kehtestame tähtajad, mida kajastame nii andmekogu põhimääruses kui ka MTA infoturbepoliitikas“. **Kodakondsus- ja Migratsiooniamet** teatab, et KMA on väliste andmetöötlejate puhul sätestamas logide säilitamise tähtaegu lepingutes. **Regionaalminister** teatab, et „tänasel päeval säilitatakse logisid tähtajatult analoogselt rahvastikuregistri andmetele. Toetudes AKI poolt käesoleva auditi alusel antavale seisukohale samas küsimuses, viiakse logide säilitamise kord ja tingimused rahvastikuregistri seadusesse.” **Sotsiaalkindlustusameti peadirektor** nõustub osaliselt soovitusega ja selgitab, et „leiame, et logide säilitamise tähtajad peab paika panema kõikidele ühtlaselt, arvestades töödeldavate isikuandmete koosseisu. Delikaatsetele üks ja tavaandmetele teine säilitamise tähtaeg“.
107. Määrata logide kontrollimise eest vastutavad isikud ning tagada neile võimalused ja vahendid regulaarse riskipõhise kontrolli läbiviimiseks isikuandmete töötlemise eesmärgipärasuse üle. **(p-d 101–106)**	**Haridus- ja teadusminister** teatab, et teeb vastavad muudatused töötajate ametijuhendites ning määrab logide kontrollimise ja isikuandmete töötlemise järelvalve eest (sh väliste andmesaajate osas) vastutavad isikud. **Sotsiaalkindlustusameti peadirektor** nõustub soovitusega ning selgitab, et „SKA teeb Sotsiaalministeeriumile ettepaneku luua selline võimalus SKA isikuandmete kaitse eest vastutava isiku jaoks.” **Eesti Riikliku Autoregistrikeskuse direktor** nõustub soovitusega.
Lepingud väliste andmesaajatega 121. Soovitus auditeeritud andmekogude haldajatele: ■ Kajastada lepingutes väliste andmesaajatega neile mõeldud infoturbe nõuded, sh isikuandmete kaitse, koos nende kinnitusega nõuetele vastavuse kohta ning samuti meetmed puhuks, kui väline andmesaaja lepingut rikub. Samuti peaks leping kajastama, kuidas ja millises mahus peavad välised andmesaajad teostama järelevalvet isikuandmete töötlemise põhjendatuse üle ning kuidas teavitatakse sellealasest tegevusest ja tulemustest andmekogu haldajat. ■ Koostöös Siseministeeriumiga eraldi kindlaks määrata juurdepääsuõigused politseiasutuste ametnikele tulenevalt nende spetsiifilistest tööülesannetest ning asuda koostöös politseiasutustega tegema regulaarselt järelevalvet nende päringute põhjendatuse üle, mille suhtes ei rakendu IKS § 20 piiratud kord. **(p-d 108–120)**	**Majandus- ja Kommunikatsiooniministeerium** ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitustega. **Haridus- ja teadusminister** teatab, et vastavad punktid on väliste andmesaajatega reguleeritud andmevahetuslepingutes. **Riigikontrolli kommentaar:** Asjaolu, et haridusasutustel ning valdadel ja linnadel on seadusest tulenevalt õigus omaenda andmetele juurdepääsuks EHISes, ei taga, et nad täidavad infoturbe ja isikuandmete kaitse tagamisega seotud nõudeid. Kuna HTM ei ole EHISega seoses sõlminud lepinguid KOVide ja haridusasutustega (vt ka punkt 109), siis leiab Riigikontroll, et mitmete väliste andmesaajate osas on HTM jätnud esitamata nõuded infoturbele ja järelevalvele isikuandmete töötlemise põhjendatuse üle. **Kaitseminister** ja **Kaitseressursside Ameti peadirektor** nõustuvad soovitustega. **Maksu- ja Tolliameti peadirektor** teatab, et „X-tee lepingute osas sisaldusid infoturbenõuded ka seni. Muud väliste andmesaajatega sõlmitavad lepingud hakkavad edaspidi läbima kooskõlastust sisekontrolliosakonna poolt, mille käigus jälgitakse infoturbenõuete sisaldumist. Politseiametnike juurdepääsuõiguste osas peab MTA läbi rääkima Politseiameti politseikontrollibürooga.” **Kodakondsus- ja Migratsiooniamet** teatab, et „ITDAK-i andmete töötlemise lepingutes on kajastatud andmekaitsenõuded, lepingu rikkumisega seotud sanktsioonid, järelevalve teostamise ja sellest teavitamise nõuded, andmetöötlemise lõpetamisega seotud nõuded jm nõuded, millest tuleb andmetöötluses kinni pidada. Lisaks andmevahetuslepingu kohaselt peavad ITDAK-i põhimääruses toodud turvaklassile vastavatele organisatsioonilistele, füüsilistele ja infotehnilistele turvameetmetele tähelepanu pöörama ka välised andmetöötlejad. KMA kavandatakse liita alates 2010. a Politsei- ja Piirivalveameti koosseisu, mistõttu tuleb 2009. a üle vaadata kogu andmevahetuse regulatsioon tervikuna tänase Politseiameti ja Piirivalveametiga.” **Regionaalminister** teatab, et „registri kasutajatega sõlmitavates lepingutes on kirjas, mis eesmärgil võib registrisse päringuid teha. Samuti kohustus tagada

Riigikontrolli soovitused	Auditeeritute vastused
	rahvastikuregistri andmete töötlemine vastavalt rahvastikuregistriseadusele, isikuandmete kaitse lokaalvõrgus vastavalt IKSile ning paroolide ja salasõnade salajas hoidmise kohustus. Lisaks on lepingutes kirjas ka loetelu tegevustest, mille eest kasutaja vastutab ning Siseministeeriumi ja AKI poolne järelevalve korraldamine ning õigus katkestada kasutaja ühendus kui on ilmnenud isikuandmete kaitse nõuete rikkumine. Rahvastikuregistri kasutajatel on nendega sõlmitud lepingu kohaselt õigus saada aruandeid andmete töötlejate poolt teostatud päringute kohta ajaperioodide lõikes. Lepingutes ei ole väliste andmesaajate ühest kohustust teostada järelevalvet isikuandmete töötlemise põhjendatuse üle ja teavitada sellest andmekogu haldajat. Rikkumise dokumenteerimise ja rikkumisest teavitamise kord on sätestatud rahvastikuregistri seaduses (§-d 63 ja 64). Täiendades ja ajakohastades rahvastikuregistri töötlemise lepinguid, arvestame ka Riigikontrolli ettepanekuid“. **Sotsiaalkindlustusameti peadirektor** teatab, et „Sotsiaalministeeriumi ja Sotsiaalkindlustusameti andmevahetuslepingud sisaldavad edaspidi lepingu lisa, mis on juba välja töötatud, kuid pole veel rakendamist leidnud. Selles on sätestatud vastaspoole üldised andmeturbenõuded.” SKA peadirektor lisab teise soovituse kohta, et politseiasutuste ametnikel puudub juurdepääs PKRile, kuid nende poolt teostatavatele päringutele on alati lisatud seaduslik alus ning vajalikud põhjendused, miks vastavaid andmeid on vaja.
122. Sõlmida PKRi väliste andmesaajatega lepingud, kus määrata kindlaks osapoolte õigused, kohustused ja vastutus. **(p-d 108–120)**	**Sotsiaalkindlustusameti peadirektor** ei nõustu soovitusega ning selgitab, et „SKA-l on sõlmitud lepingud mitmete PKR-st andmeid päringute baasil saavate asutustega nt Haigekassa, EHIS jne. KOVidega ei sõlmitud lepinguid, kuna seda liitumise ajal ei nõutud. Ettepanek oleks, et RIA võiks luua universaalse lepingu, mis sätestaks X-teele juurdepääsu, kus oleks sätestatud, mis tingimustel ja mis õigustega saadakse teistelt andmekogudelt andmeid.” **Riigikontrolli kommentaar:** KOVid on samasugused andmesaajad nagu nimetatud teised asutused. Andmekogu vastutav töötleja vastutab muu hulgas ka selle eest, et andmekogus olevaid andmeid ei vaadata ebaseaduslikult. Seetõttu on andmekogule juurdepääsu andmisel põhjendatud kahepoolse lepingu sõlmimine. Vastavalt Vabariigi Valitsuse 24.04.2008. a määruse nr 78 „Infosüsteemide andmevahetuskiht” § 20 vastutab X-teega liitunud asutus või isik tema turvaserveri kaudu teenuse kasutaja X-tee keskkonnale juurdepääsuõiguste andmise eest. RIA ülesanne on vastavalt määrusele tagada X-tee haldamine ja arendamine.
123. Võtta kasutusele meetmed, kontrollimaks väliste andmesaajate isikuandmete kaitse nõuete täitmist. Selleks määrata oma asutuses järelevalve eest vastutajad ning arendada infosüsteemides välja järelevalve teostamiseks vajalik funktsionaalsus **(p-d 108–120)**	**Haridus- ja teadusminister** teatab, et teeb vastavad muudatused töötajate ametijuhendites ning määrab logide kontrollimise ja isikuandmete töötlemise järelvalve eest (sh väliste andmesaajate osas) vastutavad isikud. Lisaks kaalutakse võimalust täiendada haridusasutuse välishindamise protseduuri. **Sotsiaalkindlustusameti peadirektor** nõustub soovitusega osaliselt ning selgitab, et „olukord, kus register peab enda väliste kasutajate üle täielikku isikuandmete kontrolli teostama, on üsna suure ja ressursse nõudva kohustuse tekitamine. Välistele kasutajatele lubatakse andmete kasutamist kindlatel alustel, tavaliselt on selleks seadusest tulenev alus/kohustus. Eeldatav on pistelise kontrolli teostamine mõningate isikute/päringute osas. Kui välja töötada infosüsteem, mis hakkaks kontrollima mingitel kindlatel alustel väliste kasutajate päringuid, on see ülemäära kulukas ettevõtmine. Lisaks on Eesti Vabariigis seadustega paika pandud, mis alustel, kes ja mis ulatuses andmeid töödelda tohib. On loodud Andmekaitse Inspektsioon, kes kontrollib isikuandmete töötlemist. Register saab ja peabki võtma endale teatud kohustused väliste kasutajate osas, kuid selle peab ühtlaselt sätestama. Juhendi koostamine, mida üks register oma väliste kasutajate osas inspekteerima peab, võiks tulla AKI-lt koostöös suuremate registrite pidajatega. Ei ole mõtet luua ühtki uut nõuet, mida keegi teostada ei suuda“. **Eesti Riikliku Autoregistrikeskuse direktor** nõustub soovitusega. **Kodakondsus- ja Migratsiooniamet** teatab, et „hetkel on käimas protsess, kus KMA on uuendamas andmevahetuslepinguid. Uutes andmevahetuslepingutest on muu hulgas sätestatud väliste töötlejate endi kohustus teostada regulaarset järelvalvet andmete töötlemise üle ning lisaks nende auditite tulemuste teavitamise kord KMA-le. KMA-s on määratud isik, kes kontrollib eelpool nimetatud auditite KMA-sse jõudmist, nende sisu ning koordineerib ka juhtkonna teavitamist auditite sisust. Lepingus on sätestatud KMA-le õigus teostada järelevalvet (selline õigus on kajastatud ka varasemates lepingutes).”
Inimese kontroll tema isikuandmete töötlemise üle 136. Arendada andmekogude infosüsteeme	**Majandus- ja Kommunikatsiooniministeerium** ja **Eesti Riikliku Autoregistrikeskuse direktor** nõustuvad soovitusega. **Haridus- ja teadusminister** teatab, et arvestab nõudeid iga uue arenduse

Riigikontrolli soovitused	Auditeeritute vastused
nii, et info väljastamine isikuandmete töötlemise kohta oleks edaspidi kiirem ja vähem töömahukas. Arendamisel tuleb silmas pidada, et infot andmete töötlemise kohta kuvataks nii andmebaasi haldaja kui ka andmebaasi väliste andmesaajate toimingute kohta. **(p-d 124–135)**	analüüsi- ja disaini faasist alates. **Kaitseminister** ja **Kaitseressursside Ameti peadirektor** ei väljenda seisukohta soovituse osas. **Maksu- ja Tolliameti peadirektor** teatab, et infosüsteemide arenduse ühe alusdokumendina on MTA-l kavas välja töötada baasnõuded arendajale, mis hõlmavad ka logimist. **Kodakondsus- ja Migratsiooniamet** teatab, et „ITDAK-i puhul on info andmete töötlemise kohta väliste andmetöötlejate poolt kajastatud kodanikuportaalis, muutes seeläbi kodaniku üheks lüliks andmekaitseprotsessis. Edaspidistes arendustöödes juhindub KMA esitatud soovitusest KMA kui töötleja kohta." **Regionaalminister** teatab, et „alates 2009. aasta III kvartalist on igal isikul e-teenusena võimalus saada vastus tema kohta rahvastikuregistrisse tehtud päringute kohta. Päring annab vastuseid alates valmimise hetkest, sest vanade andmete kuvamine ei ole tehniliselt võimalik. Varasemate päringute kohta on võimalik saada teavet, pöördudes rahvastikuregistri volitatud töötleja poole. Pooldame Riigikontrolli seisukohta, et isikule antakse teada tema andmete töötleja asutuse või selle allüksuse täpsusega". **Sotsiaalkindlustusameti peadirektor** nõustub soovitusega ning selgitab, et edastab soovituse Sotsiaalministeeriumile (vt vastus punktile 79).

Auditi iseloomustus

Auditi eesmärk

Auditi eesmärgiks oli hinnata, kas isikuandmete kaitse meetmed on auditeeritud andmekogude puhul kindlaks määratud, kas need on piisavad, et isikuandmetele oleks vaid põhjendatud juurdepääs nii vastutava, volitatud töötleja kui ka väliste andmesaajate juures ning kas nende meetmete rakendamist asutustes kontrollitakse. Samuti antakse hinnang, kas isikuandmete töötlemisega tutvumine on andmesubjekti jaoks võimalik ja piisavalt mugav.

Hinnangu andmise kriteeriumid

Hinnangu andmise põhiküsimus on: kas inimene võib olla kindel oma isikuandmete piisavas kaitstuses?

Jaatavad vastused auditi põhi- ja alaküsimustele annavad kindlustunde, et isikuandmed on kuritarvituste eest kaitstud. Vastus auditi küsimustele antakse auditeeritavate riiklike andmekogude põhjal ning hinnang laiendatakse kogumile. Auditeeritavate hulka kuuluvad mahult suured ja olulisi isikuandmeid sisaldavad riiklikud andmekogud. Kui vaadeldud andmekogude andmeturvalisuse tasemes leitakse sarnaseid olulisi puudujääke, puudub kindlus, et ka teiste riiklike andmekogude isikuandmete kaitse keskmine tase on piisav.

Auditi alaküsimused:

1. Kas andmekogule rakendatakse organisatsioonilisi, infotehnilisi ja füüsilisi turvameetmeid?

1.1. Kas turvameetmete määramisel on aluseks võetud ISKE?
1.2. Kui jah, siis kas asutusele on antud hinnang ISKE rakendatuse kohta (nt vastavusaudit)? Milline?
Organisatsioonilised (sisaldavad käitumist turvaintsidentide korral ning turbe kavandamise ja halduse töökorraldust):
1.3. Kas andmekogu dokumentatsioon sisaldab igapäevast ülesannete jaotust ja toiminguid (kes mida peab tegema)?
1.4. Kas andmekogu dokumentatsioon sisaldab ülesannete jaotust ja toiminguid (kes mida peab tegema) turvaintsidendi korral?
1.5. Kas selline tegutsemise kord on vastavuses isikuandmete kaitse seadusega?
1.6. Kas dokumentatsiooni ajakohastatakse vastavalt vajadusele?
1.7. Kui andmekogu sisaldab delikaatseid isikuandmeid, siis kas töötlemine on AKIs registreeritud?
1.7.1. Kas AKI on enne delikaatsete isikuandmete töötlemise registreerimist kohapeal kontrollinud kavandatavate turvameetmete vastavust IKS § 25 sätestatud nõuetele?
1.8. Kas andmekogu dokumentatsioon määrab kindlaks nõuded infotehnilistele turvameetmetele (nt kasutajalepingutes, turvapoliitikas, riskianalüüsis)?
1.9. Kas kõikidest päringutest (mida vaadati ja mida andmetega tehti) jäävad logid?
1.9.1. Kas logid sisaldavad päringute õigustatuse tagantjärele hindamiseks vajalikku informatsiooni (isik, kuupäev ja kellaaeg jmt)?
1.10. Kas juurdepääsuõigused andmekogule on piisavad ja põhjendatud?
1.10.1. Kas juurdepääsuõigused (sh päringud) on täpselt kindlaks määratud eri kasutajagruppidele?
1.10.2. Kas andmekogu infotehnoloogiline ülesehitus tagab, et eri kasutajagrupid ei pääse ligi muudele kui neile lepingus ettenähtud andmetele ja lubatud mahus?
1.11. Kas asutuses on olemas dokumentatsioon, mis sätestab füüsilised turvameetmed?

2. Kas asutuses on rakendatud piisavad sisekontrolli mehhanismid, et tagada organisatsiooniliste, infotehnoloogiliste ja füüsiliste turvameetmete rakendamine?

2.1 Kas andmeid töötlev asutus (sh andmekogu vastutav/volitatud, muu töötleja, nt KOV) kontrollib turvameetmete täitmist süstemaatiliselt?

2.1.1. Kas andmekogu vastutav/volitatud töötleja kontrollib kasutuslepingutest kinnipidamist, sh väliste andmesaajate päringute põhjendatust?

2.1.2. Kas logisid analüüsitakse jooksvalt?

2.1.3. Kas kontrollimine on mõne ametniku ametijuhendijärgne ülesanne?

2.1.4. Kas nimetatud ametniku järelevalvetegevus põhineb riskianalüüsil või kokkulepitud metoodikal?

2.1.5. Kas nimetatud ametnik on 2007. aastal reaalselt järelevalvet teostanud?

2.1.6. Kas rikkumisi on 2007. aastal avastatud?

2.1.7. Kas avastatud rikkumistele antakse ametlik käik ja määratakse karistused/täpsustatakse ja muudetakse korda?

2.2 Kas infotehniliste puuduste/riskide avastamisel võetakse mõistliku aja jooksul ette tehnilised arendused?

2.2.1. Kas puuduse või riski leidmisest informeeritakse arenduse üle otsustamiseks pädevaid ametnikke?

2.2.2. Kas vajalikud arendusotsused langetatakse viivitamata (2007)?

2.3. Kas andmetöötlejad on teadlikud isikuandmete kaitse nõuetest ja andmetöötluse mõistest?

2.3.1. Kas kõik andmekogus olevaid isikuandmeid töötlevad ametnikud on läbinud isikuandmete kaitse alase väljaõppe?

2.3.2. Kas isikuandmeid töötlevad ametnikud väidavad end teadvat oma õigusi ja kohustusi?

3. Kas andmesubjektil on juurdepääs infole, mis puudutab tema kohta andmebaasis tehtud päringuid?

3.1. Kas andmesubjektil on võimalik näha, millal, millises andmetöötlusprotsessis, kelle poolt ja milliseks otstarbeks tema isikuandmeid kasutatakse?

3.2. Kas seda on võimalik teada saada, esitades teabenõude?

3.3. Kas seda on võimalik teada saada elektrooniliselt infosüsteemi kaudu?

Auditi ulatus ja käsitlusviis

Auditis analüüsiti sisekontrollisüsteemide toimimist isikuandmete kaitsel eri ministeeriumide haldusalas olevate andmekogude näidetel. Auditi valimis olid riiklik liiklusregister, KMA isikut tõendavate dokumentide andmekogu, Eesti Hariduse Infosüsteem, maksukohustuslaste register, riikliku pensionikindlustuse register, kaitseväeteenistuskohustuslike Eesti kodanike riiklik register ja rahvastikuregister (vt tabel 1). Valitud andmekogud sisaldavad suures koguses isikuandmeid, sh delikaatseid isikuandmeid (välja arvatud maksukohustuslaste register) ning enamikul neist on palju kasutajaid ja väliseid andmesaajaid. Isikuandmete kaitse toimimist nimetatud andmekogude kasutamisel vaadeldi andmekogusid haldavates asutustes ning viieteistkümnes valla- ja linnavalitsuses (vt lisa A).

Auditi lõpetamise aeg:

Audititoimingud lõpetati 2008. aasta septembris.

Auditi meeskond:

Auditis osalesid II auditiosakonna peakontrolör Ülle Madise, auditijuht Markko Kard, audiitor Epp Maaten ja vanemaudiitorid Merli Vahar ja Alo Lääne; I auditiosakonna auditijuht Urmet Lee; III auditiosakonna auditijuhid Külli Nõmm ja Liisi Uder; IV auditiosakonna audiitor Marko Palo ning V auditiosakonna audiitorid Marko Seier ja Marit Olesk.

Kontaktandmed

Auditi kohta saab lisainfot Riigikontrolli kommunikatsiooniteenistusest
tel +372 640 0704 või +372 640 0777, e-post riigikontroll@riigikontroll.ee

Auditiaruande elektrooniline koopia (pdf) on saadaval koduleheküljel www.riigikontroll.ee.

Auditiaruande kokkuvõte on saadaval ka inglise keeles.

Auditiaruande number Riigikontrolli asjaajamissüsteemis on OSII-2-1.4/08/77.

Riigikontrolli postiaadress on:

Narva mnt 11a
15013 TALLINN
Tel +372 640 0700
Faks +372 661 6012
riigikontroll@riigikontroll.ee

Riigikontrolli varasemaid auditeid infotehnoloogia ja isiku õiguste valdkonnas

21.12.2007 - **Riikliku statistika asjakohasus ja andmete kogumise tõhusus**

Riigikontroll auditeeris Statistikaameti tegevust riikliku statistika korraldamisel, et hinnata, kas riiklik statistika on asjakohane riigis otsuste tegemiseks ja kui koormav on andmeesitajale statistika tegemiseks andmete kogumine.

Riigikontroll leidis, et Statistikaameti tegevus ei taga riikliku statistika sisulist kujundamist selliselt, et see vastaks Eesti kasutajate ootustele ja vajadustele.

01.11.2007 – **Avaliku teenuse kvaliteet infoühiskonnas**

Riigikontroll auditeeris avalike teenuste kvaliteeti, analüüsides teenuste osutamise kooskõla hea halduse põhimõtetega. Hea halduse põhimõte nõuab inimese võimalikult vähest koormamist suhetes avaliku võimuga: inimene peab saama oma õigust kasutada või kohustust täita võimalikult kiiresti ja mugavalt, üleliigse asjaajamise ja kuluta. Infoühiskonnas tähendab see muu hulgas Interneti kaudu asjaajamise kasutamist, kui see on võimalik ja isikule vastuvõetav.

Olgugi et hea halduse põhimõtete ellurakendamiseks olid riigi- ja kohaliku omavalitsuse asutused pingutusi teinud, ei olnud Riigikontrollil auditi tulemusena võimalik kinnitada, et infoühiskonnas nõutav avalike teenuste kvaliteet on alati tagatud.

29.09.2006 – **Riigi tugi kohalikele omavalitsustele infoühiskonna arendamisel**

Riigikontroll auditeeris 2006. aastal kohalike omavalitsuste toimetulekut infoühiskonna poolt pakutavate väljakutsete ja probleemidega ning riigi tuge omavalitsustele infoühiskonna arendamiseks. Selgus, et infoühiskonna probleemidega tegelemine pole enamikule omavalitsustest jõukohane tegevusala. Vähemalt pooled omavalitsustest vajavad otsest riigi tuge nii infoühiskonna arendamise sisulistes kui ka tehnilistes küsimustes. Omavalitsustele tekitab raskusi veebilehtede pidamist ja veebilehtedel teabe avalikustamist reguleerivate seaduste nõuete täitmine. Riigikontrolli arvates peaks riigi tasandil olema Siseministeerium eestvedajaks ja vastutajaks kohaliku infoühiskonna arengu kavandamise ja koordineerimise eest.

18.03.2005 – **Riigi IT-valdkonna juhtimine ja arendusprojektide tulemuslikkus**

23.02.2001 – **Infosüsteemide arendusprojektide tulemuslikkus**

Kõik aruanded on kättesaadavad Riigikontrolli koduleheküljelt www.riigikontroll.ee

Lisa A: Auditeeritud linnad ja vallad ning nende juurdepääs vaadeldud andmekogudele

KOV	RR	EHIS	PKR	MKR	LR	ITDAK	KTKR
Ambla	+	+	+	+	-	-	-
Anija	+	+	+	+	-	-	-
Antsla	+	+	+	+	+*	-	-
Audru	+	+	+	+	-	-	-
Haapsalu	+	+	+	+	+	-	-
Jõelähtme	+	+	+	+*	-	-	-
Jõhvi	+	+	+	+	+	-	-
Kanepi	+	+	+	+	-	-	-
Puka	+	+	+	+	-	-	-
Tapa	+	+	+	+*	-	-	-
Tartu	+	+	+	-	+	-	-
Torma	+	+	+	+	-	-	-
Tõstamaa	+	+	+	+	-	-	-
Vigala	+	+	+	+	-	-	-
Viiratsi	+	+	+	+	-	-	-

* Tärniga on märgitud kohalikud omavalitsused, kellele on loodud juurdepääs andmekogule, kuid kes pole andmekogusse selle aja jooksul ühtegi päringut teinud.

Lisa B: Aruandes kasutatud lühendid

AKI – Andmekaitse Inspektsioon

ARK – Eesti Riiklik Autoregistrikeskus

EHIS – Eesti Hariduse Infosüsteem

HTM – Haridus- ja Teadusministeerium

IKS – isikuandmete kaitse seadus

ISKE – infosüsteemide kolmeastmeline etalonturbesüsteem

ITDAK – isikut tõendavate dokumentide andmekogu

KMA – Kodakondsus- ja Migratsiooniamet

KOV – kohaliku omavalitsuse üksus

KRA – Kaitseressursside Amet

KTKR – kaitseväeteenistuskohustuslike Eesti kodanike riiklik register

LR – riiklik liiklusregister

MKM – Majandus- ja Kommunikatsiooniministeerium

MKR – maksukohustuslaste register

MTA – Maksu- ja Tolliamet

PKR – riiklik pensionikindlustuse register

REKK – Riiklik Eksami- ja Kvalifikatsioonikeskus

RIHA – riigi infosüsteemide haldussüsteem

RR – rahvastikuregister

SKA – Sotsiaalkindlustusamet