Märgukiri rahvusvahelise paralleelauditi "Isikuandmete kaitse riiklikes andmekogudes" tulemuste kohta

Riigikontroll viis läbi auditi „Isikuandmete kaitse riiklikes andmekogudes“. Audit toimus EUROSAI (Euroopa Kõrgeimate Auditiasutuste Organisatsioon) IT-töörühma algatatud paralleelauditi raames. Paralleelauditis osales kokku neli riiki: auditit juhtis Belgia Riigikontroll ning osalesid Eesti, Ungari ja Moldova.

Auditiga hinnati, kas isikuandmete kaitse on valimisse võetud andmekogudes reguleeritud ja korraldatud kooskõlas isikuandmete kaitset reguleerivate seadustega ja Euroopa Liidu (EL) vastava direktiiviga. Täpsemalt on auditi ulatus kirjeldatud märgukirja lisas 1.

Auditis vaadeldi isikuandmete (sh delikaatsete isikuandmete) kaitseks kehtestatud meetmeid sotsiaalteenuste ja -toetuste andmeregistris (STAR) ja tervise infosüsteemis. Auditeeritud asutused olid Sotsiaalministeerium ja E-tervise Sihtasutus (ETSA). Alates 01.01.2017 läksid ETSA ülesanded uuele valitsemisala asutusele – Tervise ja Heaolu Infosüsteemide Keskusele. Samuti vaadeldi isikuandmete kaitseks rakendatud meetmeid kahes kohalikus omavalitsusasutuses (Tallinna linnas ja Viimsi vallas), kes on sotsiaalteenuste ja -toetuste andmeregistri volitatud töötlejad.

Isikuandmete kaitse tagamist valimisse võetud andmekogudes ja infosüsteemides auditeeriti ajavahemikul 01.06.–31.12.2016, lähtudes sellel ajal kehtinud isikuandmete kaitse õiguskeskkonnast (vt täpsemalt lisa 2).

Auditi märgukiri avalikustatakse koos auditeeritavate vastustega Riigikontrolli veebilehel. Rahvusvaheline auditiaruanne valmib 2017. aasta jooksul. Rahvusvahelises aruandes avaldatakse auditi tulemused üldistatult, s.t eraldi ei tooda välja osalevate riikide ega valimisse võetud infosüsteemide kohta käivat teavet.

Audit näitas, et olulises osas on ELi andmekaitsedirektiivi põhimõtted üle kantud Eesti isikuandmete kaitse seadusesse. Samuti selgus, et auditi valimisse võetud infosüsteemides on isikuandmete kaitsele kaasa aitav riigi infoturbesüsteem ISKE kasutusele võetud ja seda on ka korra auditeeritud (2015. aastal).

Järgnevalt on välja toodud olulisemad probleemid ja soovitused.

1. **Andmekogude vastutavatel töötlejatel puudub kindlus, et kõigis keskset andmekogu kasutavates asutustes (nt KOVid, perearstikeskused) oleks tagatud minimaalne vajalik infoturbe tase.**

Infoturbesüsteemi eduka rakendamise eelduseks on kõigi turvameetmete ühtlane rakendamine kogu infosüsteemi ulatuses, nii et nõutav turbetase oleks tagatud igas infosüsteemi osas. Kui infosüsteemi omanik ei suuda seda tagada, ei vasta infosüsteem kindlaksmääratud infoturbenõuetele ning suureneb oht, et tekivad infosüsteemi tegevust oluliselt mõjutavad turvaintsidendid.

Audit näitas, et STARi vastutaval töötlejal puudus õigus teha järelevalvet infoturbekohustuste täitmise üle volitatud kasutajate (KOVid) juures. Tervise infosüsteemi puhul puudus sama õigus infosüsteemi volitatud töötlejal (ETSA) liidestatud infosüsteemide omanike suhtes. Infoturbe meetmete toimimist KOVides ja infosüsteemiga liidestuvates asutustes ei ole auditeerinud ka väline audiitor. Näiteks ei hõlmanud STARis ja tervise infosüsteemis korraldatud ISKE-auditid ei KOVisid ega liidestuvaid asutusi.

Sellele, et kontrollitud infosüsteemide teatud osades on infoturbe tase nõrgem, osutas näiteks see, et ühel STARi volitatud töötlejal (Viimsi vald) eraldi andmekaitse- või infoturbepoliitikat ei olnud. Samuti oli infoturve (sh andmekaitse) auditeeritud KOVides väga erinevalt reguleeritud ja erineva tasemega.

2. Kohustus ISKE rakendamist KOVides auditeerida on kehtinud alates 25.01.2009, kuid seni ei ole seal auditeid tehtud.

Infosüsteemide turvameetmete süsteemi ISKE rakendamine on kohustuslik kõigi riigi ja kohaliku omavalitsuse andmekogude pidamisel. Kui ISKE rakendamist KOVides ei kontrollita, on ohus KOVide infosüsteemides olevad andmed. Samuti on turvameetmete nõrkuse või puudumise tõttu ohustatud ka need infosüsteemid, mille volitatud kasutajad KOVid on.

Audit näitas, et ISKE-auditeid ei olnud KOVides tehtud. Juhendi kohaselt (vt Vabariigi Valitsuse 20.12.2007. a määrus nr 252 „Infosüsteemide turvameetmete süsteem“, § 9^2 lg 1) ei pea ISKE-auditeid KOVides tellima nad ise, vaid Majandus- ja Kommunikatsiooniministeerium. Seni aga ei ole ministeerium ühtegi KOVides läbi viidavat ISKE-auditit tellinud.

3. Auditeeritud infosüsteemide vastutavad ja volitatud kasutajad ei hoia enamasti ajakohasena oma infoturbepoliitikat, s.t dokumente, mis reguleerivad asutuste tasemel isikuandmete kaitset ja panevad paika strateegilised infoturbe aluspõhimõtted.

Nõutava infoturbetaseme saavutamine on võimalik vaid juhul, kui infoturbe tähtsamate reeglite täitmine tehakse kohustuslikuks. Selleks tuleb turvaeesmärkidest ja -suunistest tulenevate protsesside algatamiseks ning realiseerimiseks paika panna organisatsioonilised ja personaalsed kohustused. Üldjuhul määratakse seesugused reeglid kindlaks organisatsiooni infoturbepoliitikas.

Lisaks tuleb infoturbepoliitikat (vt ISKE kataloogi turvameede M2.192 „Infoturbepoliitika koostamine“) regulaarse ajavahemiku tagant kontrollida (soovitatavalt vähemalt iga 2 aasta tagant), et teha kindlaks, kas see on veel piisavalt ajakohane. Aegunud või puuduliku infoturbepoliitika korral ei suudeta tagada nõutavat infoturbetaset ja reageerida tekkida võivatele ohuolukordadele.

Audit näitas, et neljast asutusest kolmes ei ole infoturbepoliitikat piisava regulaarsusega uuendatud: Sotsiaalministeeriumis uuendati seda 5 aastat tagasi, Tallinna linnavalitsuse infoturbepoliitika on 6 aastat tagasi kinnitatud, Viimsi vallavalitsusel on nn infoturbe vastutuse kinnitamise vorm olnud muutmata kujul kasutusel umbes 10 aastat. Enamasti oli auditeeritud asutustes poliitikat uuendatud ebaregulaarselt. Samuti ei olnud võimalik auditi käigus leida kirjalikku tõendusmaterjali, et infoturbereeglite ajakohasust oleks üleüldse analüüsitud.

Valimisse võetud infosüsteemides korraldatud ISKE-auditite käigus oli ka väline audiitor osutanud tähelepanu sellele, et infoturbepoliitikat tuleks regulaarselt uuendada.

Aegunud infoturbereeglistiku näiteks oli Viimsi valla infoturbe dokument, millelt puudusid mitmed tänapäeval infoturbega seotud teemad, näiteks ID-kaardi või mobiil-ID-ga seotud turvameetmed, andmete krüpteerimise teema.

4. Kõigil juhtudel ei rakendanud auditeeritud infosüsteemide kasutajad ISKEs nõutud tugevusega autentimisvahendeid.

Infosüsteemides, mille terviklusele on kehtestatud kõrgeim turvaklass (T3), on keelatud autentimine viisil, kus kasutatakse ainult üht liiki pääsutõendit, näiteks parooli. Soovitatavaks autentimisevahendiks on Eesti ID-kaart või mobiil-ID, mille puhul kasutatakse kahefaktorilist autentimist (kaart + PIN-kood).

Nõutavast nõrgema autentimisvahendi kasutamine seab ohtu andmete tervikluse ja konfidentsiaalsuse, s.t suurendab võimalusi volitamata juurdepääsuks andmetele, nende andmete pahatahtlikuks muutmiseks või kustutamiseks.

Audit näitas, et tervise infosüsteemi oli kolmandatel osapooltel (perearstid või perearstikeskused) võimalik siseneda ühefaktorilise autentimisvahendiga, s.t tervise infosüsteemiga liidestatud infosüsteemide kaudu on võimalik terviseandmetele juurde pääseda ka vaid kasutajanime ja parooli kasutades ning see ei ole kooskõlas tervise infosüsteemi tervikluse turvaklassiga T3.

5. **STARi infosüsteemi volitatud töötlejad, s.t KOVid ei olnud alati maandanud kõiki kasutajaõiguste haldamisega seotud riske.**

Infoturbe korraldamisel tuleb kasutajaõiguste haldusega tagada, et igal kasutajal oleks võimalik infosüsteemi kasutada ainult vastavalt tema töökohustustele. Töösuhte lõppemisel tuleks töötajalt võtta ära võimalus infosüsteemi kasutada, et vähendada riski volitamata juurdepääsuks isikuandmetele.

Auditi käigus ilmnes, et Tallinna linnas antud STARi kasutusõigused olid viie töötaja lahkumisel muudetud küll mitteaktiivseks, kuid kontosid ei olnud kustutatud (ühe kasutaja puhul isegi 9 kuu jooksul).

6. **Kontrollitud infosüsteemide puhul ei ole korrektselt dokumenteeritud taasteplaane: tervise infosüsteemi puhul on olemas vaid informaalsed taastamisjuhised ja STARi puhul on taastamise kohustus reguleeritud lepingus majutusteenuse pakkujaga. Samuti ei olnud võimalik auditi käigus saada kirjalikke tõendeid infosüsteemide taastamise testimise kohta.**

ISKE rakendamisel kuulub andmete taastamise harjutamine või testimine infoturbemeetmete n-ö baaspaketti ehk see on kohustuslik kõigile. Andmete taastamist tuleb pisteliselt, kuid vähemalt pärast igat andmevarundusprotseduuri muutmist katsetada. Kui seda ei tehta, ei ole kindlust, et andmeid on võimalik taastada ning et valitud andmevarundusmeetod on õige. Samuti ei saa infosüsteemi omanik olla kindel selles, et andmevarundusdokumentatsioon on piisav, s.t näiteks selles, et andmed saaks taastada ka mõni asendustöötaja või et andmete taastamiseks kuluv aeg tagab infosüsteemi kasutavate asutuste põhitegevuse probleemideta jätkumise.

Audit näitas, et ETSA-l puudus üldine infosüsteemide ja andmete taastamise plaan. Tervise infosüsteemi taastamist oli küll testitud, kuid seda ei olnud dokumenteeritud.

STARi taasteplaani on teinud majutusteenuse pakkuja ja seda testitakse Sotsiaalministeeriumi initsiatiivil. Auditi käigus ei saanud Riigikontroll kindlaid tõendeid taasteplaanide regulaarse testimise kohta STARis.

Eelnimetatud probleeme ei ole lahendatud 2015. aasta keskpaigast saadik, mil ISKE-auditite tulemusel olid välja toodud samad puudused. Näiteks soovitati tervise infosüsteemi ISKE-auditi aruandes regulaarselt testida varukoopiate taastamist.

7. **Info saamine selle kohta, kes, millal ja millisel otstarbel on isikuandmeid töödelnud, ei olnud auditeeritud infosüsteemides ei infosüsteemi ega andmesubjekti (s.t isiku, kelle andmeid infosüsteemi kogutakse) jaoks ei kiire ega mugav.**

Isikuandmete töötlemisel peab infosüsteemi omanik andmesubjektile tagama kogu info tema andmete töötlemise kohta, sh avalikustama tema isikuandmete töötlemise eesmärgid; isikud, kes on tema andmeid töödelnud; ning samuti isikud, kellele tema isikuandmeid on edastatud (isikuandmete kaitse seadus, § 19). Kui infosüsteemi omanik ei suuda neid andmeid väljastada, ei ole andmesubjektil võimalik oma eraelu puutumatuses kindel olla.

Audit näitas, et infot isikuandmete töötlemise kohta, s.t selle kohta, kes, millal ja mis eesmärgil infosüsteemides isikuandmeid töötleb, koguvad mõlemad auditeeritud infosüsteemid logidesse. Selleks et edastada andmesubjektile infot tema andmete töötlemise kohta, tuleb STARi puhul iga juhtumiga eraldi tegeleda, s.t info edastamiseks tuleb iga andmetöötlemise episood logidest ükshaaval välja otsida ja süstematiseerida ning andmesubjektile eraldi esitada. Kuna praegu sellisteks päringuteks süsteemset lahendust loodud ei ole, tuleb asutustel teha palju käsitsi tööd ning info kättesaamine ei ole ei mugav ega kiire. Tervise infosüsteemis on kasutajal võimalik patsiendiportaali (www.digilugu.ee) kaudu näha, kes ja millal on tema isikuandmeid töödelnud, kuid mitte töötlemise põhjust.

Sotsiaalministeeriumi sõnul saab STARi puhul nimetatud probleem lähitulevikus lahenduse, sest STAR on kaasatud Riigi Infosüsteemi Ameti andmejälgija pilootprojekti, millega luuakse kodanikele võimalus hõlpsasti jälgida oma andmeid ja nende töötlemist (kasutades ID-kaarti või mobiil-ID-d).

8. Auditeeritud infosüsteemide puhul ei tee vastutavad töötlejad regulaarselt süstemaatilisi logide analüüse, et välistada või avastada isikuandmete väärkasutus.

Isikuandmete kaitse tagamiseks tuleb kontrollida, kas neid kasutatakse eranditult vaid lubatud eesmärkidel. Selleks peaks isikuandmete töötlemise eest vastutav isik (nt infoturbejuht) analüüsima infosüsteemi logidesse kogutavat infot. Logide analüüsimiseta võib jääda märkamata või võidakse liiga hilja avastada olulised turvameetmete nõrkused või turvaintsidendid.

Tervise infosüsteemi oli sisse ehitatud lahendus päringumustrite analüüsimiseks, kuid seda ei ole regulaarselt kasutatud. STARi puhul peab infoturbepoliitika järgi süsteemi- ja võrgulogide revisjone tegema pisteliselt vähemalt kord kuus või pärast turvaintsidente. Auditi käigus ei saanud Riigikontroll kirjalikke tõendeid, et seesuguseid revisjone oleks tehtud.

Ka see probleem on lahenduseta 2015. aastast alates, kui näiteks STARis korraldatud ISKE-auditi aruandes oli üheks läbivaks soovituseks juurutada logiserver ja regulaarselt logifaile analüüsida.

Riigikontrolli soovitus Majandus- ja Kommunikatsiooniministeeriumile:

- Alustada ISKE määruses (Vabariigi Valitsuse 20.12.2007. a määrus nr 252 „Infosüsteemide turvameetmete süsteem“) Majandus- ja Kommunikatsiooniministeeriumile pandud kohustuse täitmist, s.t hakata tellima KOVidele ISKE-audititeid.

Riigikontrolli soovitused Sotsiaalministeeriumile:

- Kasutada tervise infosüsteemis ISKE nõutud kahefaktorilist autentimist, s.t näiteks Eesti ID-kaardi ja mobiil-ID pakutavaid võimalusi; ning tagada selle nõude täitmine ka kõigi tervise infosüsteemiga liidestuvate terviseteenuste osutajate puhul.
- Turvanõrkuste avastamisel STARi ja tervise infosüsteemi kasutavates asutustes tuleks pöörduda Riigi Infosüsteemi Ameti või Andmekaitse Inspektsiooni poole, et need asutused viiksid läbi vajalikud järelevalveprotseduurid.
- Viia regulaarselt läbi andmete taastamise harjutusi ja teste ning dokumenteerida need kirjalikult.
- Viia regulaarselt läbi logifailide süsteemseid analüüse eesmärgiga välja selgitada, kas isikuandmeid on töödeldud vaid seadustes määratud juhtudel ja korras ja/või andmesubjekti nõusolekul.
- Rakendada tulevikus andmejälgija pilootprojekti tulemusi kõigis valitsemisala infosüsteemides, et tagada andmesubjektidele kiire ja lihtne juurdepääs oma andmetele ning infole nende andmete töötlemise kohta.

Riigikontrolli soovitus Sotsiaalministeeriumile, Tallinna Linnavalitsusele ja Viimsi Vallavalitsusele:

- Luua protseduurireeglid infoturbepoliitika ajakohasuse regulaarseks hindamiseks ja kirjalikult dokumenteerida iga hindamine.

/allkirjastatud digitaalselt/

Tarmo Olgo
peakontrolör
tulemusauditi osakond

Riigikontrolli soovitused ja auditeeritu vastused

Riigikontroll andis auditi põhjal Majandus- ja Kommunikatsiooniministeeriumile, Sotsiaalministeeriumile, Tallinna Linnavalitsusele ja Viimsi Vallavalitsusele soovitusi. Ettevõtlus- ja infotehnoloogiaminister Urve Palo (20.04.2017), sotsiaalministeeriumi kantsler Marike Priske (18.04.2017), Tervise ja Heaolu Infosüsteemide Keskuse direktor Katrin Reinhold (19.04.2017), Tallinna abilinnapea linnapea ülesannetes Taavi Aas (19.04.2017) ja Viimsi vallasekretär Kristi Tomingas (11.05.2017) saatsid oma vastused Riigikontrolli soovitustele.

Allpool olevad tabelid annavad ülevaate tehtud soovitustest ja saadud vastustest.

Üldised kommentaarid märgukirja kohta
Sotsiaalministeeriumi kantsler tänab Riigikontrolli põhjaliku auditi läbiviimise eest sotsiaalteenuste ja -toetuste andmeregistris (STAR) ja tervise infosüsteemis ning esitatud probleemkohtade ja soovituste eest. Auditeeritud asutuste hulgas oli ka E-tervise Sihtasutus, mille ülesanded ning osa eelnevatest Sotsiaalministeeriumi ülesannetest läks alates 01.01.2017 üle uuele Sotsiaalministeeriumi valitsemisala asutusele – TEHIK. Vastavalt sotsiaalkaitseministri ning tervise- ja tööministri 11. oktoobri 2016. a käskkirjale nr 104 „Tervise ja Heaolu Infosüsteemise Keskuse moodustamine“ on ka Sotsiaalministeeriumi ning kogu valitsemisala infoturbepoliitika välja töötamine ja rakendamine TEHIKu ülesanne. Sotsiaalministeerium koostöös TEHIKuga võtab teie tähelepanekud teadmiseks ning lähtub nendest edaspidiste tööprotsesside paremal korraldamisel. Sotsiaalministeerium ja TEHIK esitavad enda ühised seisukohad ja tähelepanekud märgukirja eelnõus toodud soovitustele. **Tervise ja Heaolu Infosüsteemide Keskus** andis teada, et nende ülesandeks on Sotsiaalministeeriumi valitsemisala asutuste infosüsteemides ja andmekogudes isikuandmete kaitse parimate meetodite väljatöötamine ja rakendamine. Lähtuvalt sellest koostati vastus koostöös Sotsiaalministeeriumiga ning Tervise ja Heaolu Infosüsteemide Keskuse vastused märgukirja eelnõule kajastusid Sotsiaalministeeriumi poolt Riigikontrollile 18.04.2017 saadetud kirjas. **Tallinna linn** suhtub isikuandmete kaitse tagamisse nii infosüsteemide vastutava kui ka volitatud töötlejana vastutustundlikult. Linn on rohkem kui 30-le riigi infosüsteemi haldussüsteemis registreeritud andmekogule vastutav töötleja, rakendades põhimäärustes toodud ISKE turvaklassidest lähtuvaid turvameetmeid. Volitatud töötlejana täidab linn vastutava töötleja määratud turvaklassist tulenevaid turvameetmeid. Tallinna linn on valmis tegema koostööd infosüsteemide põhimäärustest tulenevate järelevalve- ja auditeerimisnõuete valdkonnas kõigi infosüsteemide puhul, mille volitatud töötleja on linn. Tallinn on omal algatusel läbi viinud infosüsteemide täiemahulise ISKE auditi aastatel 2009–2010. **Viimsi Vallavalitsus** tutvus edastatud märgukirja eelnõuga ning leidis, et viited Viimsi valla puudustele on põhjendatud. Samas pidas vallavalitsus vajalikuks märkida, et 21. detsembril 2016 käskkirjaga nr 25-Ü kinnitas vallavanem Viimsi Vallavalitsuse infoturbepoliitika eeskirja. Selle aasta 13. märtsil toimus kõikidele teenistujatele ISKE-t tutvustav koolitus.

Riigikontrolli soovitused	Auditeeritute vastused
Riigikontrolli soovitus Majandus- ja Kommunikatsiooniministeeriumile: ▪ Alustada ISKE määruses (Vabariigi Valitsuse 20.12.2007. a määrus nr 252 „Infosüsteemide turvameetmete süsteem“) Majandus- ja Kommunikatsiooni-ministeeriumile pandud kohustuse täitmist, s.t hakata tellima KOVidele ISKE audititeid.	**Ettevõtlus- ja infotehnoloogiaministri vastus:** Vastavalt avaliku teabe seaduse § 531 lg-le 1 teostab Riigi Infosüsteemi Ameti (edaspidi RIA) järelevalve haldus- ja riiklikku järelevalvet infosüsteemide turvameetmete süsteemi rakendamise üle. Muudatus jõustus 16.01.2016. ISKE määruse § 92 lg 1 sätestab, et kohalike omavalitsuste andmekogude auditi tellib MKM. 16. mail 2016. a sõlmisid Eesti Vabariigi Rahandusministeerium, MTÜ Eesti Linnade Liit ja MTÜ Eesti Maaomavalitsuste Liit koostöölepingu „Kohaliku omavalitsuse infotehnoloogia keskseks arendamiseks ja kvaliteedi tõstmiseks järgnevaks 3 aastaks.“ Koostöölepingu alusel alustas 01.06.2016 Eesti Maaomavalitsuste Liidu (edaspidi EMOL) koosseisus tööd infotehnoloogia nõunik, kelle peamiseks ülesandeks on omavalitsuste osutatavate, Eesti kodanikele suunatud e-teenuste laialdasem kasutusele võtmine ning parimate infotehnoloogia praktikate levitamine omavalitsustes. Tänaseks on valminud Eesti kohalike omavalitsuste IKT strateegia ja tegevuskava, mis on aluseks ka võimalike struktuurvahendite kasutamiseks (vt majandus- ja taristuministri 12.03.2015. a määrust nr 21 „Nutika teenuste taristu arendamise toetamise tingimused ja investeeringute kava koostamise kord“ § 16 lg 1 p 1). Strateegia kaitsmine MKMis toimub 2017. a augustis. Üheks strateegiliseks eesmärgiks on „KOV IKT taristute turvataseme tõus“ ning koostöös RIA-ga plaanitakse 2018. aasta lõpuks läbi viia ISKE auditid 30%-s KOV-des, kus toimusid IKT taristu korrastustegevused EMOL-i poolt konsulteerituna. MKM ei ole KOV-ide ISKE auditite tellimise kohustuse täitjana optimaalne lahendus, kuna järelevalve kompetents on RIA-s ning MKMi sellise kompetentsi tekitamine ei ole ressursside otstarbeka

Riigikontrolli soovitused	Auditeeritute vastused
	kasutamise vaatest mõttekas. Seetõttu soovime leida kõige mõistlikuma töökorralduse, mis oleks finantside, kompetentsi ja muude ressursside vaates jätkusuutlik. Selleks oleme algatanud läbirääkimised EMOLi, RIA ning MKMi vahel, et leida lahendus, mis toetab kohalike omavalitsuste strateegilisi eesmärke ning on kooskõlas seaduses sätestatud järelevalvepädevustega. ISKE määrus on kehtiv alates 2009. aastast ning oleme valmis arutelude tulemusena ajakohastama ka ISKE määrust. Ootame ka Riigikontrolli ettepanekuid ja soovitusi, milline võiks olla optimaalne lahendus KOVide ISKE auditite tellimiseks.
Riigikontrolli soovitused Sotsiaalministeeriumile: ▪ Kasutada tervise infosüsteemis ISKE nõutud kahefaktorilist autentimist, s.t näiteks Eesti ID-kaardi ja mobiil-ID pakutavaid võimalusi; ning tagada selle nõude täitmine ka kõigi tervise infosüsteemiga liidestuvate terviseteenuste osutajate puhul. ▪ Turvanõrkuste avastamisel STARi ja tervise infosüsteemi kasutavates asutustes tuleks pöörduda Riigi Infosüsteemi Ameti või Andmekaitse Inspektsiooni poole, et need asutused viiksid läbi vajalikud järelevalveprotseduurid. ▪ Viia regulaarselt läbi andmete taastamise harjutusi ja teste ning dokumenteerida need kirjalikult. ▪ Viia regulaarselt läbi logifailide süsteemseid analüüse eesmärgiga välja selgitada, kas isikuandmeid on töödeldud vaid seadustes määratud juhtudel ja korras ja/või andmesubjekti nõusolekul. ▪ Rakendada tulevikus andmejälgija pilootprojekti tulemusi kõigis valitsemisala infosüsteemides, et tagada andmesubjektidele kiire ja lihtne juurdepääs oma andmetele ning infole nende andmete töötlemise kohta.	**Sotsiaalministeeriumi kantsleri vastused:** ▪ Tervise infosüsteemis töödeldakse isikuandmeid, sealhulgas ka delikaatseid isikuandmeid. Tervishoiuteenuse osutajal on õigus tervishoiuteenuse osutamiseks vajalike isikuandmeid, sealhulgas ka delikaatseid, töödelda tervishoiuteenuste korraldamise seaduse (TTKS) § 41 lg 1 alusel ning kohustus dokumenteerimisel kasutada riigi infosüsteemi klassifikaatoreid, loendeid, aadressiandmeid ja tervise infosüsteemi standardeid (TTKS, § 42 lg 1). Sotsiaalministri 18.09.2008. a määruse nr 56 „Tervishoiuteenuse osutamise dokumenteerimise ning nende dokumentide säilitamise tingimused ja kord“ § 3 lg 1 sätestab, et tervishoiuteenuse osutajate loodud andmekogusid peetakse avaliku teabe seadusega (AvTS) ja isikuandmete kaitse seadusega (IKS) kooskõlas. Turvanõuded kõikidele (delikaatsete) isikuandmete töötlejatele on kehtestanud isikuandmete kaitse seadusega. IKS, AvTS ja nende alusel kehtestatud õigusaktides sätestatud nõuete täitmise üle teeb järelevalvet Andmekaitse Inspektsioon. Leiame, et kahefaktorilise autentimise osas teeb järelevalvet Andmekaitse Inspektsioon, kes teeb IKS-is toodud nõuete täimise üle järelevalvet vastavalt asutusele antud delikaatsete isikuandmete töötlemise loale. Ühtlasi kehtestab inspektsioon delikaatsete isikuandmete töötlemise ühe eeldusena kahefaktorilise autentimise, analüüsib seda (delikaatsete) süsteemides ja kehtestab vajadusel ka need nõuded. Siinkohal toome välja, et TEHIK on kahefaktorilise autentimise nõude kehtestanud kõigile infosüsteemiga liidestunud asutustele liidestuslepinguga. ▪ Vastav sisuline koostöö asutuste vahel toimub ja intsidentidest antakse teada. Siinkohal toome välja Andmekaitse Inspektsiooni läbiviidavate järelevalvemenetluste ebamõistlikult pika ajakulu, mis teatud juhtudel võimaldab võimalikul rikkujal jätkata ebaturvaliste tegevustega. ▪ TEHIK-u põhiülesanneteks on Sotsiaalministeeriumi valitsemisala infosüsteemide haldus ja infoturbe korraldamine. TEHIK kinnitab, et andmete taastamise testimist on regulaarselt läbi viidud ja nende läbiviimise dokumenteerimist parandatakse. ▪ Vastava funktsiooni täitmine on TEHIK-u põhimääruse alusel TEHIK-u ülesanne, kus toimub Sotsiaalministeeriumi valitsemisala infoturbealase süsteemi loomine. Valitsemisala infosüsteemide tsentraalse logimise ja nende analüüsimise teenus on plaanis käivitada. Oleme selle teenuse käivitamiseks taotlenud riigieelarvest raha ning teenuse käivitamise aeg on seotud riigieelarve võimalustega. ▪ STAR infosüsteemis on andmejälgija rakendamine planeeritud ja teenus käivitub selle aasta jooksul. TIS infosüsteemi on tehtud investeeringud, mis võimaldasid kodanikel nende andmetöötlemise faktidega tutvuda Patsiendiportaali vahendusel juba enne andmejälgija projekti välja töötamist. Sotsiaalministeerium koostöös TEHIK-uga rakendab keskset andmejälgijat järk-järgult.
Riigikontrolli soovitus Sotsiaalministeeriumile, Tallinna Linnavalitsusele ja Viimsi Vallavalitsusele: ▪ Luua protseduurireeglid infoturbepoliitika ajakohasuse regulaarseks hindamiseks ja kirjalikult dokumenteerida iga hindamine.	**Sotsiaalministeeriumi kantsleri vastus:** TEHIK-u ülesandeks vastavalt põhimäärusele on Sotsiaalministeeriumi valitsemisala infoturbepoliitika välja töötamine ja rakendamine. Sotsiaalministeeriumi valitsemisala infoturbepoliitika uuendamine on võetud TEHIK-u selle aasta tööplaani ja selle ajakohasuse regulaarse hindamise tagab ISKE auditite läbimine.

Riigikontrolli soovitused	Auditeeritute vastused
	Tallinna Linnavalitsuse vastus: Riigikontrolli soovitusega on arvestatud praegu menetluses olevas Tallinna linna infoturbepoliitika uuendamise protsessis, kus peamisteks uuendusteks on turvaintsidentide halduse ja väljasttellimise korraldus, turvameetmete erandite käsitlemine ning lisandunud on uued organisatsiooniülesed meetmed, nagu kontrolljälgede meede, andmekandjate ja arvutivõrkude turve ning infoturbe tagamine asjaomase info jagamisel ja infoturbekoolitused. Infoturbepoliitika muutmise alused on täpsustatud: infoturbepoliitikat muudetakse auditite tulemustest, ISKE versiooniuuendustest ning oluliste tehnilistest, organisatsioonilistest või õiguslikest muudatustest lähtudes. Infoturbepoliitika ajakohasust analüüsitakse vähemalt kord kahe aasta jooksul. Riigikontrolli auditi käigus ilmnenud infosüsteemi kasutajakontode haldamisega seotud riskide maandamiseks on asjaomased sätted reguleeritud Tallinna linna ametiasutuste infotehnoloogiliste vahendite kasutamise reeglitega (linnapea 03.10.2012 käskkiri nr PO-1/195). Oleme nõus, et neis reeglites on vaja täpsustada kasutajakontode haldust, et tagada infosüsteemi kasutamine ainult töökohustustest lähtuvalt ja kontroll infosüsteemide kasutajakontode kustutamise üle töö- või ametisuhte lõppemisel. **Viimsi Vallavalitsuse vastus:** 21. detsembril 2016 käskkirjaga nr 25-Ü kinnitas vallavanem Viimsi Vallavalitsuse infoturbepoliitika eeskirja. Selle aasta 13. märtsil toimus kõikidele teenistujatele ISKE-t tutvustav koolitus.

Lisa 1. Auditi käigus kontrollitud isikuandmete kaitse põhimõtted

Riigikontroll hindas, kas valimisse võetud infosüsteemides ja asutustes on olemas olulisemad isikuandmete kaitset tagavad infoturbemeetmed. Täpsemalt vaadati, kas

- infosüsteemide kasutusõiguste haldamine on korraldatud nii, et isikuandmete kaitse on tagatud;
- infosüsteemidesse sisenemiseks on valitud tehniliselt turvaline autentimisvahend;
- andmete transportimisel kasutatakse tehnilisi meetmeid (nt krüpteerimine), mis tagavad isikuandmete konfidentsiaalsuse;
- valimisse võetud asutustes ja infosüsteemides jälgitakse (nt logifailide analüüsi teel) isikuandmete kasutamist;
- valimisse võetud asutustes on olemas isikuandmete kaitseks vajalik turvaintsidentide käsitlemise kord ja protseduurid, kuidas seda korda ajakohasena hoida;
- asutustes on olemas isikuandmete kaitseks (sh säilimiseks) vajalikud taasteplaanid (*Disaster Recovery Plan ehk DRP*) ja neid hoitakse ajakohasena;
- auditi valimisse võetud infosüsteemid tagavad kodanikule õiguse pääseda oma andmetele ligi ja saada teada, kes on tema andmeid töödelnud (sh vaadanud).

Auditis ei käsitletud muudatusi, mis tulenevad isikuandmete kaitse üldmäärusest (Euroopa Parlamendi ja nõukogu määrus 2016/679, 27. aprill 2016).

Lisa 2. Isikuandmete kaitse ja infoturbe reguleerimine Eesti Vabariigis

Praegu reguleerib Euroopa Liidus andmekaitse valdkonda andmekaitsedirektiiv 95/46/EÜ. 4. novembril 2010 avaldas Euroopa Komisjon dokumendi „Terviklik lähenemisviis isikuandmete kaitsele Euroopa Liidus“, milles teatati, et kehtiv direktiiv vajab uuendamist. Euroopa Parlament kiitis 14.04.2016 lõplikult heaks andmekaitse reformi paketi, millega kõnealune direktiiv asendatakse otsekohalduva isikuandmete kaitse üldmäärusega. Uue andmekaitse määruse peamine eesmärk on anda nutitelefonide, sotsiaalmeedia ja internetipanganduse ajastul kodanikele parem võimalus kontrollida oma andmeid. Määrus jõustus 24.05.2016 ning on avaldatud Euroopa Liidu Teatajas. Määrust hakatakse kohaldama pärast kaheaastast üleminekuaega, s.t alates 25.05.2018. Riigikontroll ei auditeerinud uue määruse kohaldamist Eesti õigusruumis, vaid vaatas praegu kehtivaid andmekaitsereegleid.

Eesti Vabariigis tagab õiguse eraelu puutumatusele üldisemalt põhiseadus ja detailsemalt isikuandmete kaitse seadus. Selle seaduse eesmärk on kaitsta isikuandmete töötlemisel füüsilise isiku põhiõigusi ja -vabadusi, eelkõige õigust eraelu puutumatusele. Seepärast on isikuandmete töötlemine lubatud vaid kas isiku nõusolekul või seaduse alusel. Kui isikuandmete töötlemise alus on olemas, peab andmeid töötlev asutus rakendama seadustest tulenevaid infoturbe meetmeid ning andma ka oma töötajatele selleks piisava väljaõppe.

Kõik riigi andmekogud ja infosüsteemid on kohustatud kasutusele võtma riigi infosüsteemi kindlustavad süsteemid, sealhulgas infosüsteemide turvameetmete süsteemi ISKE. ISKE on loodud riigi ja kohaliku omavalitsuse andmekogude pidamisel kasutatavatele infosüsteemidele ning nendega seotud infovaradele turvalisuse tagamiseks. Seejuures sisaldavad infoturbemeetmed ka andmekaitse tagamise abinõusid, näiteks on neis kirjeldatud, kuidas

- vältida kõrvaliste isikute ligipääsu andmetöötlusseadmetele;
- ära hoida andmete omavolilist lugemist, kopeerimist, kustutamist jms;
- oleks tagantjärele võimalik tuvastada, kes, millal ja millele juurde pääses, mida salvestas, muutis või kustutas ning kellele, millal ja miks isikuandmeid edastati;
- tagada, et igaühel oleks juurdepääs üksnes talle töötlemiseks lubatud andmetele ja töötlemisviisidele;
- töökorraldus kujundada nii, et see võimaldaks täita andmekaitse nõudeid;
- oma alluvuses isikuandmeid töötlevatele isikuile tagada kohane väljaõpe jms.

Kohustuslik infoturbemeetmete süsteem ISKE loob Eesti avalikus sektoris väga soodsa isikuandmete kaitse tagamise kontrollikeskkonna. Siiski tuleb turvameetmete rakendamise üle teha piisavalt järelevalvet ja perioodiliselt ISKE rakendamist auditeerida.

Isikuandmete kaitse seadus jagab riigi andmekogudes isikuandmete töötlejad vastutavateks ja volitatud töötlejateks. Isikuandmete vastutav töötleja määrab kindlaks isikuandmete töötlemise eesmärgid, töödeldavate isikuandmete koosseisu, isikuandmete töötlemise korra ja viisi ning isikuandmete kolmandatele isikutele edastamise lubamise. Volitatud töötleja on isik või asutus, keda vastutav töötleja on haldusakti või lepinguga volitanud isikuandmeid töötlema. Seaduse järgi peab vastutav töötleja andma volitatud töötlejale kohustuslikud juhised, kuidas isikuandmeid töödelda, ja vastutama selle eest, et volitatud töötleja täidab neid nõudeid. Mõlema valimisse võetud infosüsteemi puhul oli vastutavaks töötlejaks Sotsiaalministeerium. Tervise infosüsteemi volitatud töötleja oli Eesti E-tervise Sihtasutus, STARil aga Sotsiaalkindlustusamet, kõik kohalikud omavalitsusasutused ja maavalitsused.

Lisaks võib infosüsteemide ja andmekogude vastutav või volitatud töötleja anda loa liidestuda kolmandate osapoolte infosüsteemidega. Liidestumislepinguid haiglate ja perearstidega sõlmib tervise infosüsteemi volitatud töötleja ETSA.

ISKE nõuete rakendamise eest andmekogudele ja infosüsteemidele vastutab selle vastutav töötleja (Vabariigi Valitsuse 20.12.2007. a määrus nr 252), sealhulgas peab ta korraldama andmekogu andmete turvaanalüüsi, määrama infoturbe eesmärke arvestava turvaklassi ja turvataseme, rakendama sellest lähtudes infoturbemeetmed ning seaduses kehtestatud regulaarsusega korraldama sõltumatu auditi.

Olukorras, kus volitatud töötleja on suur hulk kohalikke omavalitsusasutusi (STARi infosüsteem) või kui infosüsteemiga on liidestatud palju teisi infosüsteeme (tervise infosüsteem), sõltub infoturbemeetmete rakendamine vastutava või volitatud töötleja kehtestatud õigusaktidest või andmekogu kasutamise reeglitest. Samuti võib volitatud töötaja seadustest lähtudes ise endale sisemiselt eelnimetatud reeglid kehtestada.