ANDMEKAITSE INSPEKTSIOON

Valvame, et isikuandmete kasutamisel austatakse eraelu ning et riigi tegevus oleks läbipaistev

Andmekaitse Inspektsiooni menetluskord riigi infosüsteemi haldussüsteemis

Kinnitatud peadirektori 14.08.2013 käskkirjaga

Muudetud peadirektori 19.10.2014 käskkirjaga

See kord on juhtnööriks inspektsiooni ametnikele, kes annavad kooskõlastusi/arvamusi riigi infosüsteemi haldussüsteemi esitatud andmekogudele ja muudele objektidele.

Ühtlasi on see abiks esitajatele, kes saavad siit ülevaate inspektsiooni seisukohtadest ja nõuetest.

Sisukord

1. Mida kooskõlastatakse, mille kohta antakse arvamus?

Andmekaitse Inspektsioon kooskõlastab Riigi Infosüsteemi Ametiga (RIA) riigi infosüsteemi haldussüsteemis (RIHA-s) andmekogu dokumentatsiooni andmekogu elutsükli neljas etapis:

- andmekogu asutamisel
- kasutusele võtmisel
- andmekoosseisu muutmisel
- lõpetamisel (sh. andmekogu jagunemisel, andmekogude ühendamisel).

Kooskõlastused saanud andmekogu registreeritakse RIHA-s ning saab liidestuse andmevahetuskihiga (*x-teega*). Dokumentatsioon esitatakse uuesti kooskõlastamisele, kui seda muudetakse andmekogu kasutuselevõtmise või andmekoosseisu muutmise kooskõlastamise ning selle RIHA-s registreerimise vahelisel ajal.

Kooskõlastamist normivad avaliku teabe seaduse (AvTS) § 43^3 lõiked 3 ja 5, registreerimist § 43^7. Täpsemad asjaolud on sätestatud AvTS § 43^9 lõike 1 punkti 6 alusel kehtestatud valitsuse 28.02.2008 määruses nr 58 „Riigi infosüsteemi haldussüsteem“.

Lisaks kooskõlastavad andmekogu dokumentatsiooni Statistikaamet (AvTS § 43^3 lg 3) ning Maa-amet (ruumiandmete seaduse § 75).

Kooskõlastamine puudutab neid infosüsteeme, millele seadusandja on andnud andmekogu staatuse. Andmekogu staatus antakse infosüsteemile seadusega või seaduse alusel antud õigusaktiga. Seadust võib asendada ka välisleping või Euroopa Liidu otsekohalduv õigusakt. Vt. lähemaid selgitusi Andmekaitse Inspektsiooni andmekogude juhisest.

RIHA-s registreeritakse ka andmekogu staatuseta infosüsteeme, sisemise töökorralduse vajaduseks asutatud andmekogusid, infosüsteemide standardlahendusi ja teenuseid – eeskätt andmevahetuskihiga *X-tee* liidestamiseks.

Kuna kooskõlastamine on reserveeritud üksnes andmekogudele, siis nimetatud objektide dokumentatsiooni suhtes avaldab inspektsioon arvamust.

Selle eesmärk on sama mis andmekogu kooskõlastamisel – probleemide ennetamine ning nõu andmine avaliku teabe ja isikuandmete kaitse alal. Sellega vähendame vajadust probleemide tagantjärgi lahendamiseks järelevalve- või väärteomenetlusena.

Arvamuse andmisel ei tugine inspektsioon mitte AvTS § 43^3 lõikele 3, vaid soovituslike juhiste andmise sätetele: AvTS § 45 lõige 4 ning isikuandmete kaitse seaduse (IKS) § 33 lg 1 punkt 5.

Samas on nende kahe menetluse sisu kattuvad – nii kooskõlastamine kui ka arvamuse andmine toimuvad mõlemad RIHA-sse üleslaetud ühesuguse andmestiku põhjal.

2. Menetlusreeglid

Valitsuse 28.02.2008 määruses nr 58 „Riigi infosüsteemi haldussüsteem“ § 7 lõikes 7 ettenähtud 20-päevast andmekogude kooskõlastamistähtaega kohaldab inspektsioon ka muude objektide kohta arvamuse andmisel.

Selle tähtaja jooksul vaadatakse esitatud dokumentatsioon läbi ning:

1) andmekogu kooskõlastatakse/objekti kohta antakse arvamus (kusjuures kooskõlastus/arvamus võib olla ka tingimuslik) või
2) küsitakse asja läbivaatamiseks vajalikke täiendavaid selgitusi (kooskõlastamise 20-päevase perioodi sees)
3) keeldutakse kooskõlastamisest (ka näiteks juhul kui objekt on AvTS ja IKS seisukohast vähetähtis[1]) või antakse eitav arvamus koos põhjendustega, vajadusel kuulatakse ära dokumentatsiooni esitaja vastuväited

Kui dokumentatsiooni esitaja ei anna asja läbivaatamiseks vajalikke täiendavaid selgitusi või ei esita inspektsiooni küsitud täiendavat dokumentatsiooni RIHA kooskõlastamise perioodil (20 tööpäeva), võib inspektsioon kooskõlastamisest keelduda / anda eitava arvamuse.

Kooskõlastuse /arvamuse annab inspektsioon järgmistes peatükkides ettenähtud asjaolude kontrollimise ja nende põhjal kujundatud hinnangute alusel. Hinnangud sõnastatakse nendes peatükkides toodud vormis.

Kuna Eesti riigiasutuste asjaajamiskeeleks on eesti keel, siis aktsepteerib inspektsioon üksnes eestikeelset dokumentatsiooni (keeleseaduse § 10 lg 1).

Võõrkeelsed andmeväljad, aga samuti arusaamatu sisuga (näiteks üksnes asjaosalistele mõistetavate lühenditega) andmeväljad loetakse läbivaatamisel tühjadeks andmeväljadeks. RIHA ei ole mõeldud üksnes asjassepühendatute kitsale ringile, tegemist on igaühele mõeldud avaliku andmestikuga.

[1] Andmekogu kooskõlastamisest samal põhjusel inspektsioon ei keeldu.

3. Delikaatsete isikuandmete töötlemise registreerituse kontroll ja andmestike võrdlemine

Kontrollitavad RIHA väljad:	- üldandmed/töödeldakse delikaatseid isikuandmeid? - andmete koosseis
Muud allikad:	- Isikuandmete töötlejate ja isikuandmete kaitse eest vastutavate isikute register (DIAT-register)
Asjakohased õigusnormid:	- IKS 5. ptk
Antav hinnang:	Delikaatsete isikuandmete töötlemine on: - registreeritud - registreerimata
Antav hinnang:	Registriandmed ja RIHA andmed: - langevad kokku - on vastuolus

Esimese asjana kontrollib inspektsioon, kas menetluse objekt on delikaatsete isikuandmete töötlemise registreerimise kohustuse täitnud ning kui jah, siis võrdleb mõlemaid andmestikke.

Hiljemalt andmekogu kasutusele võtmisel tuleb:

a) delikaatsete isikuandmete töötlemine registreerida DIAT-registris või

b) alternatiivina määrata ja registreerida isikuandmete kaitse eest vastutav isik (IKS § 27 ja 30).

DIAT-register peab kajastama ka andmestiku hilisemaid muudatusi (IKS § 29 lg 5).

Kuna inspektsioon käsitleb registreerimist teavitusena, reeglina ilma teavitatud asjaolude sisu kontrollimata, siis on DIAT-registri andmed lihtsalt abimaterjaliks andmekogu kooskõlastamisel/arvamuse andmisel. Seda niihästi õiguslike kui andmeturbeliste asjaolude hindamisel järgnevate peatükkide kohaselt.

Kui andmekogu pidaja on delikaatsete isikuandmete töötlemise registreerinud, võrreldakse kummaski menetluses avaldatud teavet:

DIAT-register	**RIHA**
Isikuandmete töötleja (vastutav ja volitatud) Isikuandmete töötlemise kohad	Haldaja, pidaja

Isikuandmete töötlemise õiguslik alus ja eesmärk	Üldandmed
Isikuandmete koosseis	Andmete koosseis
Kellele isikuandmete edastamine on lubatud	Teenused
Turvameetmete kirjeldus	Tehniline kirjeldus

Kui kummaski menetluses avaldatud teave on omavahel sisulises vastuolus, algatab inspektsioon järelevalvemenetluse, sest on alust arvata, et isikuandmete töötleja on jätnud IKS §-s 27, § 29 lõikes 5 või §-s 30 sätestatud kohustuse täitmata.

4. Õiguslik küsimustik

Järgnevat küsimustikku kasutame nii andmekogude kooskõlastamisel kui ka kõigi muude objektide kohta arvamuse andmisel.

4.1) mis on menetluse objekt ning tema eesmärk/ülesanne?

Kontrollitavad RIHA väljad:	- üldandmed - alusdokumendid
Asjakohased õigusnormid:	- AvTS § 43^1 lg 1 ning § 43^3 lg 1 - isikuandmete osas IKS § 10 lg 2 ning § 6 punktid 1 ja 2 (seaduslikkuse ja eesmärgikohasuse põhimõte) - menetluse objekti kohta käivad õigusaktid
Antav hinnang:	- objekt on inspektsiooni hinnangul kooskõlastamisele kuuluv andmekogu - objekt ei ole inspektsiooni hinnangul kooskõlastamisele kuuluv andmekogu, vaid [*andmekogu staatuseta infosüsteem / sisemise töökorralduse vajaduseks asutatud andmekogu / teenus / infosüsteemide standardlahendus*] ning [*inspektsioon annab selle kohta arvamuse / inspektsioon loobub arvamuse andmisest, kuna objekt on isikuandmete kaitse ja avalikule teabele juurdepääsu seisukohalt vähetähtis*]. Objekt ei ole kooskõlastamisele kuuluv andmekogu, kuna [*järgneb põhjendus*]
Antav hinnang:	objekti eesmärke (avalikke ülesandeid) on kirjeldatud: - õigesti - valesti, sest [*järgneb puuduste selgitus – vajadusel koos märkusega, et tegu on ebaseadusliku andmetöötlusega; vajalik sünkroonsus andmete koosseisule antud hinnanguga, vt järgmist alaptk*]
Antav hinnang:	alusdokumendid on kirjeldatud: - õigesti - valesti, sest [*järgneb puuduste selgitus: näiteks viidatakse dokumendile, mis ei anna andmetöötluseks pädevust*]

Objekti määratlemisest sõltub, kas kohalduvad andmekogu kohta käivad erinõuded (AvTS 5^1. ptk) või üksnes avaliku teabe ja isikuandmete alased üldnõuded. Infosüsteemi määratlemisel andmekoguna juhindume „Andmekogude juhendis“ toodud seadusliku aluse kriteeriumist.

Kui ilmneb, et objekt ei kvalifitseeru andmekoguks, muutub kooskõlastamine arvamuse andmiseks. Vastavalt on inspektsiooni tegevuse aluseks:

- kas AvTS § 43^3 lõige 3 koos valitsuse 28.02.2008 määruse nr 58 § 7 lõikega 6 või
- AvTS § 45 lõige 4 ja IKS § 33 lg 1 punkt 5.

Andmekogu asutamise aluseks olevast seadusest (seaduse volitusnormist) tuleneb andmekogu loomise eesmärk (ehk avalik ülesanne). Inspektsioon kontrollib, kas RIHA-sse kantu vastab seadusest tulenevale.

Kui objekt ei ole andmekogu, tuleb kontrollida, kas RIHA-sse kantu vastab

- seaduses või selle alusel sätestatud teabevaldaja avalikele ülesannetele – AvTS § 3 lg 1,
- isikuandmete osas haldusorganile pandud avalikele ülesannetele ning neist tulenevatele kohustustele – IKS § 10 lg 2.

Kui ei vasta, võib tegu olla pädevusevälise andmetöötlusega.

Tuleb arvestada, et avalik ülesanne on määratlemata õigusmõiste. See ei pruugi olla sätestatud *expressis verbis*, vaid võib olla seadusest tervemõistuslikult tuletatav:

- näiteks hallatavad asutused luuakse ja nende tegevus sätestataksegi mitte seaduse, vaid haldusaktidega; avalik ülesanne võib tuleneda nende puhul asutamisakti ning Vabariigi Valitsuse seaduse § 43 koosmõjust,
- õigusest heale haldusele (mille aluseks põhiseaduse § 14) tuleneb vajadus poliitikate kujundamiseks asutusse kogunenud teavet mõistlikus mahus analüüsida, ilma et selle kohta oleks seadusenormi.

Inspektsioon ei ole õiguskantsler ega teosta õigustloovate aktide normikontrolli. Kui aga objekti tegevuse aluseks olev määrus vm haldusakt on seadusega selges vastuolus, on see alus kooskõlastamisest keeldumisele või eitava arvamuse andmisele.

Kui seadusega vastuolus olev andmetöötlus rikub isikute õigusi ja vabadusi, teeb menetleja inspektsiooni-sisese ettepaneku järelevalve- või väärteomenetluse alustamiseks või pakub välja muu sobiva lahenduse (nt. pöördumine andmetöötleja suhtes teenistuslikku järelevalvet teostava asutuse poole, erakorraline ettekanne Riigikogu põhiseaduskomisjonile või õiguskantslerile).

4.2) kas andmekoosseis on kohane?

Kontrollitavad RIHA väljad:	- andmete koosseis - üldandmed
Asjakohased õigusnormid:	- AvTS § 43^5 lg 1, § 43^6, samuti vastavus § 43^1 lõikele 1, § 43^3 lõikele 1; - isikuandmete osas IKS § 10 lg 2 ning § 6 punktid 1 ja 2 (seaduslikkuse ja eesmärgikohasuse põhimõte) - menetluse objekti kohta käivad õigusaktid
Antav hinnang:	andmete koosseisu on kirjeldatud: - kohaselt - ebakohaselt, sest [*järgneb puuduste selgitus – vajadusel koos märkusega, et tegu on ebaseadusliku andmetöötlusega; vajalik sünkroonsus objekti eesmärgile (avalikele ülesannetele) antud hinnanguga, vt eelnevat alaptk*]

Muuhulgas kontrollib inspektsioon selle hinnangu andmiseks, kas:

- kirjeldatud koosseis vastab sellele, mida sätestab AvTS § 43^5 nimetatud dokument;
    - sh eriti, et ei töödeldaks pädevuseväliselt isikuandmeid – pädevuseväline on muuhulgas teist andmekogu (näiteks rahvastikuregistrit) dubleeriv andmete kogumine ja säilitamine (keelatud AvTS §-s 43^6, keelust võib seadusega kõrvale kalduda);
- kas delikaatsed isikuandmed ja isikuandmed on korrektselt määratletud (delikaatsete isikuandmete ammendav loetelu on antud IKS § 4 lõikes 2; andmetöötleja konkreetset töötajat tuvastada võivaid andmeid ei peeta mõnikord ekslikult isikuandmeteks; juriidilise isiku andmed ei ole isikuandmed),
- kas õiguslik tähendus on andmetele omistatud seadusega (AvTS § 43^6 lg 4).

Andmeobjekte tuleb kirjeldada nii, et nad oleksid võrreldavad põhimääruse või seadusega, mis andmete kogumise ette näevad. Kui RIHAs toodud andmeobjekti nimetus erineb põhimääruses toodust, saab lisada selgituse kommentaari lahtrisse. Arusaadav ega võrreldav ei ole näiteks andmeobjekti nimetus „*kuum_kpv,eba_oigus_summa,kas_lind*“. Arusaamatud kirjeldused loeb inspektsioon puudusteks.

4.3) kas säilitustähtajad on kohased?

Kontrollitavad RIHA väljad:	- andmete koosseis - alusdokumendid - teenused [*vajadusel*] - tehniline kirjeldus [*vajadusel*] [*sageli ei saa neist väljadest selgust säilitustähtaegade ega nende määramise alusnormide kohta, sel juhul küsib inspektsioon dokumentatsiooni esitajalt lisaselgitusi*]
Asjakohased õigusnormid:	- IKS § 6 punktid 2 ja 3 (eesmärgikohasuse ja minimaalsuse põhimõtted) - menetluse objekti kohta käivad õigusaktid
Antav hinnang:	säilitustähtajad on: - kohased - ebakohased, sest [*järgneb puuduste selgitus*]

Säilitustähtajad on üks sagedasemaid probleemide allikad. Seda on käsitletud lähemalt „Andmekogude juhendis“.

4.4) kas vastutav/volitatud töötleja on õigesti kirjeldatud?

Kontrollitavad RIHA väljad:	haldaja, pidaja
Asjakohased õigusnormid:	- AvTS § 43^4 - isikuandmete osas IKS § 7 - menetluse objekti kohta käivad õigusaktid
Antav hinnang:	andmetöötleja(d) on RIHA-s kirjeldatud: - õigesti - valesti, sest [*järgneb puuduste selgitus*]

Andmetöötleja ning tema töötaja eristamise ning volitatud töötleja määratlemisega seotud probleeme on kirjeldatud „Andmekogude juhendis“.

4.5) kas juurdepääs teabele on kohaselt kirjeldatud?

Kontrollitavad RIHA väljad:	- teenused - alusdokumendid
Asjakohased õigusnormid:	- AvTS 1.-5. peatükid juurdepääsu võimaldamise ja selle piiramise kohta - isikuandmete osas IKS § 14 - menetluse objekti kohta käivad õigusaktid
Antav hinnang:	juurdepääs teabele on kirjeldatud: - kohaselt - ebakohaselt, sest [*järgneb puuduste selgitus*]

Avalikule teabele juurdepääs tagatakse teabenõude täitmisega (passiivne avalikkus) ja teabe avalikustamisega (aktiivne avalikkus). Avalikustamine hõlmab niihästi teabevaldaja võrgulehel avaldamist, andmekogu kaudu avaldamist kui ka Eesti teabeväravas avaldamist. Teabele juurdepääs hõlmab ka õigust seda taaskasutada.

Muuhulgas jälgib inspektsioon, et:

- teabele juurdepääsu piirangud tuleneksid üksnes AvTS-st või eriseadusest,
    - eriseaduste puhul tuleks piirangut võrrelda piirangute klassifikaatoriga – kas on vajalik klassifikaatori täiendamine,
- andmekogude juurdepääsupiiranguta teave oleks avalikustatud masinloetaval kujul ja tervikliku andmekogumina allalaaditav Eesti teabevärava kaudu (AvTS § 29 lg 4),
- tervikuna ja masinloetaval kujul kättesaadavaks tegemist, samuti avalikustatava teabe kättesaadavaks tegemist indekseerimisele (interneti otsingumootoritele) tuleb hinnata täiendava eraelu riive kontekstis (AvTS § 35 lg 1 p 12).

4.6) kas ja kuidas on andmesubjektile võimaldatud juurdepääs enda andmetele?

Kontrollitavad RIHA väljad:	- teenused, tehniline kirjeldus - alusdokumendid
Asjakohased õigusnormid:	- AvTS § 39 lg 1 - IKS § 19, 20 - erinormid, mis piiravad andmesubjekti õigust saada enda kohta käivaid andmeid

Antav hinnang:	andmesubjekti juurdepääs enda kohta käivatele andmetele on kirjeldatud: - kohaselt - ebakohaselt, sest [*järgneb puuduste selgitus*]

Andmesubjekti õigus olla informeeritud oma isikuandmete töötlemise üksikasjadest on isikuandmete kaitse keskne põhimõte. Olles lubanud privaatsusõiguse riive isikuandmete töötlemisel, on seadusandja ette näinud garantiid, mis kehtestavad ühest küljest ette Andmekaitse Inspektsioonile kohustuse revideerida isikuandmete töötleja tegevuse seaduspärasust, kuid teisalt võimaldavad ka andmesubjektil endal kontrollida, milliseid andmeid, millistel eesmärkidel, kelle poolt ja millal on töödeldud. Viimane meede on oluliselt tõhusam kogutud isikuandmete kvaliteedi ning töötlemise õiguspärase tagamise vahend, kuna inspektsioon ei jõuaks ka parima tahtmise korral iga üksikisiku andmete töötlemise õiguspärasust kontrollida. Andmesubjekti ja isikuandmete töötleja otsene dialoog omakorda on vajalik ka isikuandmete töötlejale, et andmekogusse kogutud andmed oleksid ajakohased, täielikud ning vajalikud seatud andmetöötluse eesmärgi saavutamiseks. See vähendaks jällegi täiendavate päringute tegemise vajadust ning optimeeriks seeläbi ka halduskoormust.

Arvestades tänapäeval saadaolevate tehniliste võimaluste taset, peame juurdepääsuõiguse võimaldamist andmesubjektile elementaarseks nõudeks. Eelistada tuleks eelkõige eesti.ee teabevärava võimalusi, sest sinna saab andmesubjekt siseneda turvalise autentimisvahendi abil. Kui taoline tehniline lahendus puudub, mille kaudu andmesubjekt saaks andmekogust enda kohta käivaid andmeid küsida, tuleb seda põhjendada.

Käesolev nõue ei kohaldu, kui andmekogu sisaldab vaid neid isikuandmeid, mis tekivad kandeid teinud ametiisikute või töötajate ülesannete täitmisel nende endi kohta.

5. Andmeturbeline küsimustik

5.1) kas turvaklass on kohaselt määratud?

Kontrollitavad RIHA väljad:	- üldandmed: turvaklass - teenused [*vajadusel, hindamaks teenustaseme nõudeid*]
Asjakohased õigusnormid:	- AvTS § 43, § 43[9] lg 1 p 4 ja lg 3, valitsuse 20.12.2007 määrus nr 252 „Infosüsteemide turvameetmete süsteem“ - isikuandmete osas IKS § 25 - menetluse objekti kohta käivad õigusaktid
Antav hinnang:	Turvaklass on kirjelduse põhjal määratud: - kohaselt - ebakohaselt, sest [*järgneb selgitus*]

Turvaklass määratakse vastavalt valitsuse 20.12.2007 määrusele nr 252 „Infosüsteemide turvameetmete süsteem“. Erinevatel andmeliikidel võib olla erinev turvaosaklass. Turvaklassile vastavad turvameetmed rakendatakse andmeid töötlevale infosüsteemile või selle osale töödeldava andmestiku alusel. Turvaklassiga määratud turbeastmest tuleneb andmekogu auditeerimise sagedus.

Turvameetmete süsteemi kasutusjuhendi kohaselt määratakse juurdepääsupiiranguta teabe konfidentsiaalsuse turvaosaklassiks S0. Kui teave on juurdepääsupiiranguga, määratakse konfidentsiaalsuse turvaosaklassiks S1, S2 või S3. Delikaatsete isikuandmete töötlemisel tuleks määrata teabe konfidentsiaalsuse turvaosaklassiks vähemalt S2.

Määratud turvaklassi sobivuse hindamiseks vaadatakse vajadusel ka teenustaseme nõudeid.

5.2) kas ISKE on hiljemalt andmekogu kasutusele võtmisel rakendatud?

NB! See küsimus kehtib üksnes andmekogude kooskõlastamisel, mitte muude objektide kohta arvamuse andmisel!

Kontrollitavad RIHA väljad:	- üldandmed: turvaklass
Asjakohased õigusnormid:	- AvTS § 43, § 43[9] lg 1 p 4 ja lg 3, valitsuse 20.12.2007 määrus nr 252 „Infosüsteemide turvameetmete süsteem“ - isikuandmete osas IKS § 25 - menetluse objekti kohta käivad õigusaktid

Antav hinnang:	ISKE on kirjelduse kohaselt: - rakendatud - rakendamata, sest [*järgneb selgitus*]

Avaliku teabe seaduse § 43[9] lg 1 punkti 4 ja lõike 3 ning valitsuse 20.12.2007 määruse nr 252 „Infosüsteemide turvameetmete süsteem“ kohaselt peab kõigi avaliku sektori andmekogude pidamisel rakendama turvameetmete süsteemi (**i**nfo**s**üsteemide **k**olmeastmeline **e**talonturbe süsteem ehk ISKE).

ISKE on meetmete kataloog, millest andmetöötleja valib enda andmekogu parameetritele vastavalt asjakohased meetmed. Hiljemalt andmekogu kasutusele võtmisel peavad olema rakendatud kõik asjakohased meetmed. Osaline rakendamine kasutusele võetud andmekogu suhtes ei anna kindlust turvameetmete piisavuse suhtes.

Inspektsioon aktsepteerib osalist rakendamist üksnes asutamise järgus (tingimusel, et andmekogu kasutusele võtmise järgus on ISKE rakendatud täielikult).

5.3) kas isikuandmete kasutamisest jääb jälg maha?

Kontrollitavad RIHA väljad:	- tehniline kirjeldus [*sageli ei ole selles jälgitavust piisavalt avatud, millest tuleneb lisaselgituste küsimise vajadus*]
Muud allikad:	- isikuandmete töötlejate ja isikuandmete kaitse eest vastutavate isikute register (DIAT-register)
Asjakohased õigusnormid:	- AvTS § 39 lg 2, valitsuse 20.12.2007 määrus nr 252 „Infosüsteemide turvameetmete süsteem“ - isikuandmete osas IKS §-d 24-26 - menetluse objekti kohta käivad õigusaktid
Antav hinnang:	- isikuandmete kasutamisest jääb dokumentatsiooni kohaselt maha piisav jälg - isikuandmete kasutamisest ei jää piisavalt jälge maha, sest [*järgneb puuduste selgitus*]

Isikuandmete töötlemisel peab töötleja tagama, et oleks võimalik tagantjärgi kindlaks teha, millal, kelle poolt ja milliseid andmeid töödeldi ja edastati (IKS § 25 lg 2 punktid 3 ja 5).

See on üldnõue, mille praktilisel rakendamisel tuleb arvestada ka olulisuse põhimõttega. Avalike andmete vaatamine andmekogus on eraelu ebaoluline riive ning selle nimeline fikseerimine ei ole enamasti vajalik. Piiratud juurdepääsuga andmete puhul on aga ka andmete vaatamise logimine määrava tähtsusega. Samas ka avalike isikuandmete andmekogusse sissekandmine, muutmine või kustutamine võib olla isiku õiguste oluliseks riiveks ning andmekogu pidamise oluliseks toiminguks, sellised toimingud tuleb nimeliselt fikseerida.[2]

Nimeline fikseerimine on asutuse-siseseks abinõuks, väljapoole võib seda teavet vajadusel kuvada üldistatumalt, näiteks üksuse-põhiselt.

Lisaks IKS-i üldnormile annab AvTS erinormi: asutuse-siseseks kasutamiseks tunnistatud isikuandmete väljastamise üle peab asutus pidama täpset arvestust – kellele, miks, millal, mil viisil ja mida väljastati (AvTS § 39 lg 2).

Arvestuse pidamiseks võivad sobida ka logifailid.

5.4) kas andmetöötlus on turvameetmete kirjelduse kohaselt piisavalt turvaline?

Kontrollitavad RIHA väljad:	- üldandmed: turvaklass - tehniline kirjeldus - teenused
Muud allikad:	- isikuandmete töötlejate ja isikuandmete kaitse eest vastutavate isikute register (DIAT-register)
Asjakohased õigusnormid:	- AvTS § 43, § 43[9] lg 1 p 4 ja lg 3, valitsuse 20.12.2007 määrus nr 252 „Infosüsteemide turvameetmete süsteem“ - isikuandmete osas IKS § 6 p 6, § 25 ja § 26 lg 3 - dokumendiregistrite osas valitsuse 26.02.2001 määruse nr 80 „Asjaajamiskorra ühtsed alused“ § 24 lg 1 - valitsusasutustes infoturbe juhtimise osas valitsuse 15.03.2012 määrus nr 26 „Infoturbe juhtimise süsteem“ - menetluse objekti kohta käivad õigusaktid

[2] Näide: kinnistusraamatu ja äriregistri kõik kanded on avalikud ja nende vaatamise nimeliseks fikseerimiseks puudub vajadus. Kuid selliste kannete tegemine, muutmine ja kustutamine mõjutab oluliselt omandiõigust ja ettevõtlusvabadust, seega tuleb need toimingud nimeliselt fikseerida.

Antav hinnang:	Andmetöötlus on kirjelduse kohaselt esialgsel hinnangul: - piisavalt turvaline - ebaturvaline

Seda üldhinnangulist küsimust kontrollitakse turvameetmete ebapiisavuse kahtluse korral. Kahtlus võib tekkida ka siis, kui kolmes eelnevas küsimuses on positiivsed hinnangud.

Kooskõlastamise juures tekkinud küsimuste puhul võib Andmekaitse Inspektsioon nõuda esitamiseks Valitsuse 20.12.2007 määrus nr 252 „Infosüsteemide turvameetmete süsteem“ § 4 lg 1 alusel koostatud andmete turvaanalüüsi, milles peaks sisalduma:

- infoturbe kirjeldus (näiteks ISKE), selle eesmärgid ja planeeritud täienduste prioriteetnimekiri;
- infosüsteemi ulatus, analüüsitud ohud ja nõrkused, koos vastumeetmetega loetletud ohtudele ning ohu ilmnemisel rakendatavate kaitsemeetmete loetelu;
- isikuandmete, pere- ja eraelu kaitseks rakendatud turvameetmed;
- andmete turvaanalüüsi tulemusena kindlaks määratud jääkriskid ja turvameetmed nende vähendamiseks;

Inspektsiooni erilise tähelepanu alla kuuluvad andmekogud ja muud objektid:

- millel on või peaks inspektsiooni hinnangul olema turvatase „H“;
- mis töötlevad/sisaldavad delikaatseid või muidu eriti tundlikke isikuandmeid;
- mis muudel põhjustel vajavad inspektsiooni kõrgendatud tähelepanu;

ISKE rakendamiskohustusega objektide puhul jälgib inspektsioon ka ISKE auditeerimisekohustuste täitmist peale RIHAs kooskõlastamist.

Kui turvameetmete ebapiisavuse kahtlus püsib, algatab inspektsioon järelevalvemenetluse.