Andmekaitse Inspektsioon

Isikuandmete kaitse auditi läbiviimise juhend

TALLINN 2010

Isikuandmete kaitse auditi läbiviimise juhend

Versioon 2.2
18.Juuni_2010

Sisukord

1. Sissejuhatus

1.1. Käesolevas juhendis kehtestatakse menetluse kord, mis käsitleb isikuandmete kaitse auditi teostamist.

1.2. Isikuandmete kaitse järelevalve auditi läbiviimise juhendi koostamise eesmärgiks on kirjeldada Andmekaitse Inspektsiooni põhiülesanneteks oleva sõltumatu järelvalve teostamine isikuandmete töötlemise seaduslikkuse ja andmekogude pidamise üle ühelt poolt ja avaliku teabe avaldamisnõuete täitmise üle teiselt poolt.

1.3. AKI järelvalvemetoodikal on kaks ülesannet:

1) olla abivahendiks AKI-le järelevalve läbiviimisel;

2) võimaldada isikuandmete töötlejatel kasutada AKI järelvalvemetoodikat oma isikuandmete töötlemise hindamiseks.

1.4. Juhendi koostamisel kasutatud materjalid:

- Isikuandmete kaitse seadus
- Euroopa Parlamendi ja Nõukogu Direktiiv 95/46/EÜ:
    1. CWA 15262:2005. Invetory of Data Protection Auditing Practices. European Committee for Standardization (Isikuandmete kaitse Auditi Raamistik (EL direktiiv 95/46/EÜ; I osa: Baseline raamistik - Isikuandmete kaitse Euroopa Liidus.
    2. CWA 15499:2006. Personal Data Protection Audit Framework (EU Directive EC 95/46) – Part I ja Part II. European Committee for Standardization (EL direktiiv 95/46/EÜ; II osa: Kontrollnimekiri, küsimustike ja näidete kasutajate raamistik - Isikuandmete kaitse Euroopa Liidus
    3. The Data Protection Audit Manual. UK Information Commissioner. 2001.
- EVS/ISO/IEC 2382, Infotehnoloogia. Sõnastik
- IT-turvahaldust kajastavad standardid nagu
    - EVS-ISO/IEC 27001:2006. Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded
    - EVS-ISO/IEC 27002:2008. Infotehnoloogia. Turbemeetodid. Infoturbe halduse tegevusjuhis (vana nimega EVS-ISO/IEC 17799:2003).
    - EVS ISO/IEC 27005:2009 tühistab ja asendab tehnilised aruanded ISO/IEC TR 13335-3:1998 ja ISO/ICE TR 13335-4:2000 ning on nende tehniline uustöötlus.
    - EVS ISO/IEC 13335 osadega 1–5. Infotehnoloogia. Infoturbe halduse suunised.

1.5. Isikuandmete kaitse auditeerimine ei täida ISKE rakendamise auditi rolli.

2. Mõisted ja lühendid

- **Infosüsteem –** andmeid töötlev, salvestav või edastav tehniline süsteem koos tema normaalseks talituseks vajalike vahendite, ressursside ja protsessidega.
- **Vastavusaudit**, mille eesmärk on hinnata kas dokumenteeritud poliitikad, juhendid, eeskirjad ja protseduurid vastavad isikuandmete kaitse õigusaktides sätestatud nõuetele.

  Nimetatud tüüpi auditi tegevusega tuleb isikuandmete kaitse auditi protsessi alustada ning tavaliselt saab seda läbi viia ilma auditeeritavasse asutusse kohapeale minemata, ainult dokumentatsiooni põhjal.
- **Valmidusauditi** eesmärgiks on kindlaks teha, kas asutuse isikuandmete töötlemise praktika vastab asutuse kehtestatud kirjalikele poliitikatele, juhenditele, eeskirjadele, kordadele ja protseduuridele.

  See osa on kõige tähtsam osa auditi protsessist ning seda saab läbi viia ainult auditeeritava juures kohapeal.

- **Valmidusauditi läbiviimiseks** on kaks põhilist metoodikat, mida saab kasutada kas eraldi või siis kombineeritult:
    - **Funktsiooni audit,**
      metoodika sisu on mingi kindla valdkonna, funktsiooni või osakonna isikuandmete kaitse süsteemi kontrollimine.
      Funktsiooni audit keskendub konkreetse struktuuriüksuse (näiteks osakonna) protsessidele, protseduuridele ja isikuandmetele ja ei ületa struktuuriüksuse piire. (N: *perearst, hambaarst vm väike üksus*)
    - **Protsessi audit,**
      metoodika all mõistetakse konkreetse protsessi algusest lõpuni jälgimist isikuandmete kaitsmisega seotud olukorra välja selgitamiseks. Protsessi audit puutub kokku erinevate valdkondade, funktsioonide ja asutuse osadega ning võimaldab hinnata kuidas asutuses isikuandmete töötlemine terviklikult toimib (N: *E-Tervise IS*).
- **Seaduslikkuse põhimõte** – isikuandmeid võib koguda ausal ja seaduslikul teel;
- **Eesmärgikohasuse põhimõte** – isikuandmeid võib koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning isikuandmeid ei või töödelda viisil, mis ei ole andmetöötluse eesmärkide saavutamisega kooskõlas;
- **Minimaalsuse põhimõte** – isikuandmeid võib koguda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks;
- **Kasutuse piiramise põhimõte** – isikuandmeid võib muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal;
- **Andmete kvaliteedi põhimõte** – isikuandmed peavad olema ajakohased, täielikud ning vajalikud antud andmetöötluse eesmärgi saavutamiseks;
- **Turvalisuse põhimõte** – isikuandmete kaitseks tuleb rakendada turvameetmeid nende tahtmatu või volitamata muutmise, avalikuks tuleku või hävimise eest;
- **Individuaalse osaluse põhimõte** – andmesubjekti tuleb teavitada tema kohta kogutavatest andmetest, talle tuleb võimaldada juurdepääs tema kohta käivatele andmetele ja tal on õigus nõuda ebatäpsete või eksitavate andmete parandamist.
- **Audiitor**: sõltumatu isik, kes omab ettevalmistust, kogemust ja õigust teostada isikuandmete järelevalvemenetlust. Auditeerimisrühma juht on Andmekaitse Inspektsiooni poolt määratud auditi toimimise eest vastutav isikuks.
- **Eriarvamuste protokoll**: on dokument, mille koostab auditeeritav ja milles sisaldub põhjuste loetelu ja vajadusel alternatiivsete lahenduste kirjeldus audiitori poolt esitatud puuduste kohta, mille sisseviimist auditeeritav ei pea vajalikuks või õigeks.

3. Isikuandmete kaitse auditeerimise eesmärgid

3.1. Isikuandmete kaitse auditi definitsioon ja põhjused

3.1.1. Isikuandmete kaitse audit on süsteemne ja sõltumatu ekspertiis, mille eesmärk on teha kindlaks kas isikuandmete töötlemisega seotud tegevused asutuses on vastavuses organisatsiooni isikuandmete kaitse poliitika ja protseduuridega ning kas isikuandmete töötlemine vastab isikuandmete kaitse nõuetele.

3.1.2. Isikuandmete kaitse audit aitab välja selgitada probleemid ja nõrkused asutuse isikuandmete töötlemise juhtimise süsteemis.

3.1.3. Isikuandmete kaitse audit aitab kindlustada ja säilitada vastavust oluliste isikuandmete kaitse nõuetega (leida puudusi ja nõrkusi asutuse isikuandmete kaitse süsteemis ning hankida informatsioon isikuandmete kaitse süsteemi ülevaatuse jaoks).

3.2. Isikuandmete kaitse auditi nõuded (*liigitus ja metoodika*)

Auditeerimise esmane ning oluline nõue on, et isikuandmete kaitse auditi läbiviija või läbiviijad, st AKI töötaja(d) ehk audiitor ei oma huvisid auditi lõpptulemuses.

Teiseks, isikuandmete kaitse auditi tulemus kinnitab, et

- organisatsioon töötleb isikuandmeid järgides isikuandmete kaitse põhimõtteid, mis tulenevad väljapoolt asutuse (seadusandlusest, valdkonna spetsiifilistest kokkulepetest jne.);
- asutuse sisene isikuandmete kaitse meetmete ja protseduuride süsteemi kvaliteet on piisav tagamaks isikuandmete kaitse põhimõtete järgimise.

Auditeerimine ei keskendu ainult väljastpoolt asutuse tulevate isikuandmete kaitse nõuete täitmisega seonduvate riskide maandamisele vaid tegeleb ka asutuse sisemise struktuuri isikuandmete kaitse kohustustega.

3.3. Suhtlemine auditeeritava asutuse töötajatega.

3.3.1. Asutuse töötajatega suhtlemine on oluline, kuna ükskõik kui hästi läbimõeldud ja dokumenteeritud asutuse isikuandmete töötlemise protseduurid ka ei ole, sõltub nende teostamine ikkagi inimestest.

3.3.2. Suhtlemisel asutuse töötajatega on kaks eesmärki.

- selgitada välja kas dokumenteeritud isikuandmete süsteem praktikas toimib;
- selgitada välja asutuse personali isikuandmete kaitse teemaline üldine teadmiste tase ja pühendumus kaitsta isikuandmeid ja andmesubjektide privaatsust.

4. Isikuandmete kaitse auditeerimise protsess

Isikuandmete kaitse auditid järgivad samu protsesse nagu kõik auditid ehk AKI poolt isikuandmete töötlemise järelevalve teostamise etapid on:

- Ettevalmistus (sisaldab auditi plaanimist ja riskide hindamist).
- Läbiviimine (sisaldab vastavusauditi läbiviimist, analüüsi varem kogutud materjalile).
- Auditi tulemuste aruandlus (kontrollakt), raporteerimine ja järeltoimingud.

4.1. Ettevalmistus – planeerimine

1) Audit algab eesmärgi sõnastamisega. Auditi eesmärgi sõnastamise tulemusena koostatakse kirjalik dokument auditi ülesandega.

2) Tähtis on, et mõlemad pooled (nii audiitor kui auditeeritav) saaksid auditi eesmärkidest ühtemoodi aru. Eesmärgi sõnastamine on auditi alguspunkt ning alus auditi plaani loomiseks.

3) Auditi eesmärk peab olema dokumenteeritud ning sisaldama vähemalt alljärgnevaid andmeid:

1. Auditi eesmärkide püstitaja ja püstitatud eesmärkide täitja.
2. Auditi objekt (auditeeritav asutus).
3. Auditi ulatus, mis sisaldab:
    - objekti kirjeldust (*isikuandmete töötlemise protsessi kirjeldus*).
    - auditi aspekte (***k**onfidentsiaalsus, **t**erviklus, **s**-jätkusuutlikus ja auditeeritavus*).

- nõudeid *(millised on isikuandmete kaitse regulatsioonid, standardid ja parimad praktikaid mille põhjal audit läbi viiakse*).

4. Auditi läbiviimise periood.
5. Auditi põhjalikus ja ulatus (*mida ja kui põhjalikult auditeeritakse*).
6. Auditi aruande vorm ja aruande esitamise ajakava.
7. Auditi jaoks plaanitav aeg.
8. Viide kehtivale seadusandlusele.
9. Vastutuse määramine.

4) Selleks, et isikuandmete kaitse audit oleks võimalikult tõhusalt ja efektiivselt sooritatud tuleb enne auditi alustamist läbi mõelda, millist tüüpi tegevused on auditi jooksul vaja läbi viia, et koguda piisavalt tõendeid isikuandmete töötlemise süsteemi kohta arvamuse andmiseks.
5) Auditi plaan on süsteemne ja struktuurne kirjeldus tegevustest, mida audiitor peaks auditi käigus läbi viima, et hinnata isikuandmete töötlemise süsteemi, olemasolu, ülesehitust, efektiivsust ja jätkusuutlikust.
6) AKI audiitori esmane ülesanne on saada auditeeritava asutuse kohta niipalju taustainformatsiooni kui võimalik, selleks on:

4.2. Auditi läbiviimine

1) Hindamaks isikuandmete kaitse üldjuhtimist, tuleb vaadelda kas asutuse struktuur, protsessid ja juhtimisvahendid tagavad, et asutus täidab isikuandmete kaitse kohustusi, kontrollib isikuandmete kaitsmise protsesse, peab arvet ja korraldab järelvalvet isikuandmete kaitse protsesside üle.
2) Hea isikuandmete kaitse üldjuhtimine tähendab:
   1. Selgelt kaardistatud isikuandmete töötlemise operatsioone.
   2. Seadusega pandud kohustuste alusel koostatud isikuandmete kaitse strateegiat.
   3. Juhtkonna pühendumist.
   4. Selgelt määratletud rolle ja kohustusi.
   5. Asutuse pühendumist, mis väljendab isikuandmete kaitse süsteemi järgimises.
   6. Efektiivsete protsesside olemasolu, mis ennetavad ja tegelevad probleemidega.
   7. Isikuandmete töötlemisele kehtivate nõuete järgimise seiret ja nõuete järgimisest kõrvalekaldumiste avastamise korral sobilikke kompensatsiooni mehhanismide olemasolu.
3) Nõuded, mille põhjal isikuandmete töötlemise üldjuhtimist auditeeritakse, on:
   1. Organisatsioon: Asutuse struktuur, peab võimaldama täita isikuandmete kaitsmisega seotud kohustusi ja täitma asutuse enda isikuandmete kaitsmise eesmärke tõhusalt, efektiivselt ja läbipaistvalt;
   2. Protsess: Asutusel peab olema isikuandmete kaitse süsteem, mille olemasolu tagab, et isikuandmete kaitse eesmärgid on sõnastatud, kõigile teada, arusaadavad ja täidetud, eesmärkide täitmise üle toimub seire, eesmärkide täitmist hinnatakse, isikuandmete kaitse probleemide tekkimist üritatakse ennetada ja probleemide tekkimisel leitakse neile lahendused.

      Isikuandmete töötlemise süsteemi hindamise all mõeldakse siin asutuse dokumenteeritud isikuandmete kaitse süsteemi (poliitikad, eeskirjad, juhendid ja protseduurid) kontrollimist, selgitamaks välja kas süsteem vastab väljapoolt asutust tulevatele nõudmistele (siseriiklikud isikuandmete kaitse õigusaktid, direktiivid vms.).

      Isikuandmete töötlemise süsteemi olemasolu ja ülesehituse hindamine järgneb ajaliselt isikuandmete töötlemise süsteemi hindamisele ja kätkeb endas

praktikas rakendatud isikuandmete töötlemise süsteemi võrdlemist dokumenteeritud isikuandmete kaitse süsteemiga.

Isikuandmete töötlemise süsteemi efektiivsust ja jätkusuutlikust hinnatakse kõige viimasena lähtudes eelneva olemasolu ja ülesehituse hindamise tulemustest.

3. Tehnoloogia: Isikuandmete kaitset mitte ei kompromiteerita, vaid toetatakse ja täiustatakse tehnoloogia abil.

5. Isikuandmete kaitse auditi läbiviimise sammud

5.1. I samm

5.1.1. Auditi läbiviimine algab vastavusauditi eelse kokkusaamisega.

5.1.2. Auditi eelse kokkusaamise eesmärk on kohtuda auditeeritava asutuse juhtkonnaga kindlustamaks nende poolse arusaamise sellest, mida audiitor kavatseb ette võtta (AKI poolt teostatava auditi tutvustamine).

5.1.3. Sellel kohtumisel tuleks arutada:

- administratiivseid küsimusi – kas ja kes on isikuandmete kaitse eest vastutav isik asutuses ning milline on dokumentatsioon (isikuandmete töötlemise süsteem), koostöölepingud volitatud töötlejatega mida asutus peaks esitama audiitorile, et viimane saaks vastavusauditi läbi viia jne;
- auditi aspekte - auditi ulatus, ajakava, personal keda kaasatakse, auditi tulemuste esitamise vorm, järeltegevused jne;
- praktilist korraldust – auditeeritava asutuse ruumidesse ligipääs jne.

5.2. II samm

5.2.1. Teise sammu eesmärkideks on:

1. Hinnata millisel määral vastab auditeeritava asutuse isikuandmete kaitse süsteem seadusandluses sätestatud nõuetele (§25 lg 2 ja 3).

2. Välja selgitada kas on mõistlik viia peale vastavusauditit kohe läbi ka valmidusaudit või lükata valmidusauditi läbiviimist edasi ajani, kuni vastavusauditi tulemusel avastatud puudused asutuse isikuandmete kaitse süsteemis on kõrvaldatud.

5.2.2. Vastavusaudit ja küsimustik

Peale auditi eelset kohtumist esitab AKI auditeeritavale asutusele **vastavusauditi küsimustiku**. Dokumendid, mida läbi vaadatakse on selleks ajaks juba kokku lepitud auditi eelsel kohtumisel.

5.2.3. Vastavusauditi käigus hinnatavate dokumentide hulgas peavad kindlasti olema:

1. **Poliitikad**: koopiad isikuandmete kaitse poliitikast, juhendist või muudest kõrgema juhtimise tasandi dokumentidest, mis kirjeldavad kuidas isikuandmete kaitsega seonduvate teemadega asutuses tegeletakse;

2. **Üldised juhendid**: spetsiifilised tööstusharu või sektori jaoks kehtivad juhendid mis sisaldavad isikuandmete kaitse temaatikat;

3. **Juhendid:** Asutuse sisesed juhend ja treeningmaterjalid, mis on tehtud tõstmaks töötajate teadlikust isikuandmete töötlemise teemadel;

4. **Protseduurid**: Asutuse sisesed protseduurid, mis annavad töötajatele detailseid instruktsioone konkreetsete isikuandmete kaitsega seotud tegevuste teostamiseks.

5.2.4. Vastavalt esitatud dokumentatsiooni ja küsimustiku tulemustele teeb AKI audiitor otsuse, kas vastavusauditi tulemused on piisavad jätkamaks auditit valmidusauditiga. Vastavusauditi tulemused fikseeritakse kirjalikult vastavusauditi aruandes ning edastatakse koos kontrollaktiga

auditeeritavale asutusele, et viimane saaks enne valmidusauditit tulemusi kommenteerida ja vajadusel teha täpsustusi.

5.2.5. Vastavusauditi tulemuste põhjal alustatakse valmidusauditi läbiviimise ettevalmistamist, mis tähendab esmalt otsustamist, kas valmidusauditi raames viiakse läbi funktsionaalne audit (ainult osa või väike firma), protsessi (kogu asutuse) audit, mõlemad auditi tüübid või lükatakse otsustamine edasi (näiteks protsessi auditi vajalikkus otsustatakse alles peale funktsionaalse auditi läbiviimist).

5.2.6. Põhjused, mille alusel mitte jätkata valmidusauditiga võivad olla:

1. puudused siseriiklikes õigusaktides sätestatud nõuete täitmisel;
2. auditeeritava asutuse isikuandmete kaitse poliitika puudumine;
3. isikuandmete kaitse poliitika täitmiseks vajaliku asutuse struktuuri, rollide ja kohustuste puudumine;
4. kindlate isikuandmete kaitse teemadega tegelemiseks vajalike protsesside puudulik dokumenteerimine sh volitatud töötlejate kohustuste ja pädevuse piiride puudumine.

5.3. III samm - Valmidusaudit

5.3.1. Järgmiseks alustatakse funktsionaalse- ja/või **protsessi auditi läbiviimiseks küsimustiku koostamisega** so audiitori Spikker.

Küsimustike (spikreid) on soovitatav kasutada kuna need:

1. on abiks auditi plaanimisel ja ettevalmistamisel;
2. on audiitorile auditi ajal nö. „mälu" eest;
3. aitavad audiitoril keskenduda olulisele;
4. aitavad audiitoril juhtida auditi suunda ja säilitada järjepidevust;
5. on koht kuhu saab teha auditi jooksul märkmeid;
6. on auditi järgse kontrollakti ja aruande aluseks.

5.3.2. Valmidusauditi läbiviimisel tuleb koostada kontrollakt mille allkirjastavad osapooled ning seal fikseeritakse mittevastavused või muud märkused.

6. Isikuandmete kaitse auditi tulemuste aruandlus ja järeltegevused

6.1. Auditi aruande eesmärk on:

1) viidata peamisele isikuandmete kaitse auditit puudutavale informatsioonile, nagu kuupäev, ulatus, hinnatud valdkonnad, auditi meeskond jne;

2) võtta kokku põhilised auditi käigus tehtud leiud ning viitata isikuandmete nõuetele mittevastavustele;

3) kirjeldada soovitused isikuandmete kaitse süsteemi parandusteks;

4) panna paika järelkülastuste iseloom ja ajakava.

6.2. Auditi aruanne koosneb järgnevatest osadest:

1) aruande esilehest, mis sisaldab viiteid, auditeeritava asutuse nime, auditeerimise etapp, auditeeritud funktsiooni või protsesside nimesid, auditi teostamise kuupäevad, auditeerimisrühma liikmete nimekiri, kõikide kasutatud lähtematerjalide loetelu;

2) auditi kokkuvõte, mis peab olema faktipõhine ja aus ning kajastama, et tegemist on konkreetsel ajal ja kohas tehtud olukorra väljavõttega;

Kokkuvõte peab olema hinnangut andev, mitte ainult kirjeldav. Auditeeritav üldjuhul teab, milline nende isikuandmete kaitse süsteem on, neid huvitab eelkõige isikuandmete kaitse süsteemi efektiivsus ja vastavus isikuandmete kaitse nõuetele.

3) sisukord;
4) auditeeritav ja audiitori nime koos audiitori allkirjaga;
5) detailset aruannet kus on kirjas:
   - auditi eesmärk;
   - auditi ulatus;
   - nõuded, mille põhjal audit läbi viidi;
   - auditi metoodika, lähenemise viisi ja üksikasjalikust;
   - kuupäevad;
   - piiranguid, mis auditi läbiviimisele seati;
   - arvamust;
   - detailset leidude kirjeldusi ja soovitusi.
6) kokkuvõte mittevastavuste parandamistegevustest, kus loetletakse üles kõik auditi jooksul leitud mittevastavused ning pannakse kirja parandamistegevuse eest vastutav isik, kirjeldatakse parandamistegevust ning märgitakse aeg mis ajaks parandused sisse viiakse;
7) nimekiri kokkulepitud audiitori poolt tehtavatest järeltegevustest, kus on kirjeldatud järeltegevuste ulatus ja ajakava.

6.3. Isikuandmete kaitse auditi aruanne kõige olulisem osa on auditeerimise käigus tehtud märkuste loetelu kontrollaktis. Märkused esitatakse auditi aruandes audiitorite poolt märgatud auditi puuduste loeteluna.

6.4. Kõik märkused auditis, mida auditi aruandes esile tuuakse, peavad olema seotud isikuandmete kaitsega. Isikuandmete kaitsega mitteseotud puudusi ja tähelepanekuid tuleb käsitleda ja auditeeritavale või muule ametkonnale esitada eraldi.

6.5. Audiitorid peavad auditi aruandes tooma välja võimalikud isikuandmete kaitsest kõrvalekalded infoturbe lähteülesandest, tehnilistest tingimustest, normides, standartidest ja eeskirjadest vaid sel määral, kui need kõrvalekalded või puudused mõjutavad audiitori hinnangul andmeturbest.

6.6. Kõiki avastatud puudusi tuleb auditi aruandes käsitleda niivõrd reaalselt, selgelt ja üheselt mõistetavalt kui võimalik.

6.7. Isikuandmete kaitse auditi aruandes loetletud märkused infoturbe kohta peavad olema hinnatud arvestades nende potentsiaalse ohu taset (riski). Probleemide ohutaseme määrab audiitor.

6.8. Järelaudit

Juhul kui auditi jooksul leiti isikuandmete kaitse nõuetele mittevastavusi on soovitav läbi viia auditi järeltegevusi, et veenduda kas väljapakutud parandustegevused on rakendatud ning kas need tegevused on efektiivsed. Ulatus järeltegevuse hindamiseks tuleb valida vastavalt konkreetse mittevastavuse iseloomule ning võib olla:

1. väiksemate muudatuste rakendamise kohta kinnituse saamine e-posti teel;
2. dokumentatsiooni kontrollimine;
3. isikuandmete kaitse auditi osaline (osas, kus mittevastavused leiti) uuesti läbiviimine;
4. terve valdkonna või struktuuriüksuse, kus mittevastavusi esines, uuesti auditeerimine.

Järeltegevuste ajakava tuleb paika panna lähtuvalt konkreetset mittevastavusest, mida järeltegevuse raames kontrollitakse. Olulise mõjuga mittevastavustega tuleb tegeleda

koheselt, vähem olulisi mittevastavusi võib uuesti kontrollida, kui toimub sama struktuuriüksuse või protsessi järgmine audit (eeldusel, et auditeid viiakse läbi regulaarselt). Kui kõik isikuandmete töötlemise mittevastavusi parandavad tegevused on üle kontrollitud kinnitavad auditi aruande auditeeritud asutuse esindaja ja AKI audiitor ning sellega on audit lõppenud.

7. Auditi toimimise vastutava isiku isikuandmete kaitse auditeerimise protseduurid

Isikuandmete kaitse auditeerimise protsess viiakse läbi järgmise skeemi kohaselt:

1	Koostada ja kinnitada auditi kava. Isikuandmete kaitse järelevalvemenetlus (edaspidi audit) algab selle planeerimisega. AKI auditi toimimise eest vastutav isik koostab auditi kava, mis on auditi programmi aluseks.
2	IKS § 33 lg 5 alusel algatada järelevalvemenetlus omal algatusel. Koostada, kinnitada ja esitada auditeeritavale asutusele Teade riikliku järelevalvemenetluse algatamise kohta..
3	Peale auditeeritava asutuse Teabele vastamist leppida kontaktisikuga kokku ning viia läbi vastavusauditi eelne kohtumine, eesmärgiga kohtuda auditeeritava asutuse juhtkonnaga kindlustamaks nende poolse arusaamise sellest, mida audit kavatseb ette võtta (Vt p 5.1.3.).
4	Peale auditi eelset kohtumist esitatakse auditeeritavale asutusele vastavusauditi küsimustiku. (*Dokumentide loetelu, mida küsimustikus esitatakse on selleks ajaks juba auditi eelsel kohtumisel kokku lepitud*).
5	Analüüsida esitatud dokumentatsiooni ja küsimustiku vastuseid ning otsustada, kas vastavusauditi tulemused on piisavad jätkamaks auditit valmidusauditiga.
6	Vastavusauditi tulemused fikseerida kirjalikult vastavusauditi vahearuandes ning edastatakse koos otsusega auditeeritavale asutusele, st kas jätkata auditit valmidusauditiga, mille eesmärgiks on kindlaks teha, kas asutuse isikuandmete töötlemise praktika vastab asutuse kehtestatud kirjalikele poliitikatele, praktikate kirjeldustele, juhenditele ja protseduuridele.
7	Ettevalmistada küsimused (spikker) ja koostada kontrollakt ning viia läbi valmidusaudit. Kontrollaktis fikseeritakse kõik puudused või märkused. Kontrollakti allkirjastab auditeeritava asutuse kontaktisik.
8	Auditi toimimise eest vastutav isik koostab ning esitab auditi lõpparuande (Raporti), mis esitatakse koos Teatisega auditeeritava asutuse juhile.
9	Peale auditi aruande koostamist viia läbi auditit lõpetav kokkusaamine, mille eesmärk on tutvustada auditi tulemusi isikuandmete kaitsega tegelevatele võtmeisikutele. See kokkusaamine peaks olema suhteliselt lühike ja kokkuvõtlik ning soovitavalt sisaldama: 1. auditi kokkuvõtte ja leidude kirjelduse; 2. auditi järgseid kokkuvõtteid; 3. auditi järeltegevuste/soovituste iseloom.
10	Mittevastavuste korral tuleb teostada järelaudit. Eesmärgiks: • määrata kindlaks, kas ja kuivõrd korrektselt, efektiivselt ja õigeaegselt on asutuses ellu rakendatud auditi tulemusel antud soovitusi; • hinnata jätkuvat kooskõla kehtestatud nõuetega; • veenduda, kas juhtkond on hinnanud riske, mis tulenevad auditi käigus

	tehtud soovituste mitterakendamisest.