

Avaliku teabe nõukogu III kohtumine

28.02.2018 kell 10:00 – 14:00

Koht: Andmekaitse Inspeksioon

Osalejad: Urmas Ojamäe (Rahandusministeeriumi infotehnoloogiakeskus), Aila Schmidt (Kultuuriministeerium), Andrea Kivi (Kultuuriministeerium), Kaspar Kala (Sotsiaalministeerium), Evelyn Tohvri (Tallinna Linnakantselei), Triin Nigul (Keskkonnaministeerium), Kertu Nurmsalu (Siseministeerium), Jaan Laidmets (Haridus- ja Teadusministeerium), Aivar Ilves (Maaeluministeerium), Ivika Vutt (Maaeluministeerium), Janno Laas (Majandus- ja Kommunikatsiooniministeerium), Marju Müürisepp (Kaitseministeerium), Elle Vahur (Kaitseministeerium), Risto Rahu (Haridus- ja Teadusministeerium), Eneli Nõmm (Politsei- ja Piirivalveamet), Hille Oidemaa (Välisministeerium), Pille Noodapera (Rahvusarhiiv), Innar Tammiku (Riigi Infosüsteemi Amet), Liivi Karpištšenko (Majandus- ja Kommunikatsiooniministeerium), Kadri Kilp (Riigikantselei), Priit Lello (Tallinna Linnakantselei), Bert Blös (Justiitsministeerium), Viljar Peep (AKI), Elve Adamson (AKI), Raavo Palu (AKI), Merit Valgjärv (AKI), Urmo Parm (AKI), Maarja Kirss (AKI).

1. 10.00-11.45 Vajalikud tegevused isikuandmete kaitse üldmääruses sätestatud nõuete täitmiseks Justiitsministeeriumi näitel – Bert Blös

Bert tutvustas oma arutelus tema koostatud dokumendi, mis on loodud Saksa BSI baasil. Selle dokumendi esmane ning avalik versioon on kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/isikuandmete_tootlemise_oigus_parasuse_tagamise_susteemi_loomine_justiitsministeeriumi_naitel.pdf (lisatud AKI võrgulehele avaliku teabe nõukogu I kohtumise materjalide all).

RIA uuendab ISKE mooduleid, kuid hetkel ei ole selge, millal tulevad muudatused andmekaitsemeetmetena. Siiski peab lisaks ISKE meetmete osas arvestama ka lisaks isikuandmete kaitse üldmääruse (ÜM) nõudeid, mis ei ole juba kaetud nende ISKE nõuetega.

Registrit tuleb pidada kõigi isikuandmete töötlemise toimingute osas – nõue tuleneb ÜM art 30.

Viljar: kui rääkida kaardistustest, mida teevad asutuste IT-üksused, siis on lisaks ÜM art 30 kohane bilansi pidamine, teenuste korraldamise ja teabehalduse määruse järgi teostatav teenuste kaardistamine, RIHA järgi kaardistamine. Samas RIHA ja teenuste kataloog kõiki andmetöötluste kaardistusi ei kata – nt töötajate andmete töötlemine ei ole nendega kaetud.

Hetkel RIHA ei kata andmekogude ja RIHA-kirjetega kõiki neid aspekte, mida ÜM art 30 nõuab – seetõttu ei saa hetkel ühitada andmekogude osas ÜM art 30 järgse andmetöötlustoimingute ülevaate pidamist.

Bert: asutuste tehtav privaatsuspoliitika peab ka lihtsalt ning selgelt selgitama, mida konkreetses asutuses isikuandmetega tehakse – nt kandideerimisprotsessis.

Viljar: need tegevused, mis on püsivad ja konstantsed, võiks ära kirjeldada nõ mõistlikkuse piiri arvestades. Kui tegemist on nõ ühisürituste fotografeerimine, siis see oleks pigem üksik tegevus, mis selle kirjendamise juurde ei käi.

Bert: logimispoliitika aluseks võeti ISKE meetmed ning see toodi sisse sisemistesse eeskirjadesse.

Viljar: õiguskaitseasutuste direktiivist tuleb otse kohustus logida tegevused, kuid isikuandmete kaitse üldmäärusest on logimise kohustus tuletatav ÜM art-test 5 ja 32.

Bert: kehtiva IKS-i kohaselt, kui andmed on seaduse alusel täiesti avalikud andmed, siis neid ei pea logima. Samas, kuidas hakkab toimima ÜM art 32 valguses?

Viljar: kui tegemist on tundlikumate andmetega (karistusandmed) kuid seaduse kohaselt juurdepääsetavad, siis neile juurdepääs on ennekõike päringupõhine ning selles osas on vajalik logida selline juurdepääs.

Logide säilitamine – tuleb eristada, millisest erinormist või seadusest tuleneb logide säilitamise tähtaeg.

Viljar: andmekogude põhimäärustes on enamasti logide säilitamistähtajad juba määratud, kuid ülejäänud osas tuleb arvestada pigem üldisemate seaduste ja nõuetega. See võib sõltuda nt väärtemenetlusliku aegumistähtajaga (2 aastat), distsiplinaarmenetluste läbiviimine (maksimaalselt 2 aasta jooksul) või nt arvutikuritegude uurimine (5 aastat) – ei ole ühtset lähenemist kohe võimalik välja pakkuda.

Bert: kui on kõrgemate turvaosaklassidega seotud andmete kogumid, siis tasuks kasutada tarkvara, et automatiseerituna välja tuua kahtlased andmetöötlustoimingud.

Bert: andmekaitse spetsialist peaks olema infosüsteemi või andmekogu loomise juures, et saaks juba varakult olla nende loomise, toimimise ja lõpetamise juures.

Bert: privaatsuspoliitika võiks teha kõikide andmetöötluste kohta, kuid avaliku sektori osas on paratamatult andmetöötlustoimingud seadusandluses on kaetud, mistõttu tasuks see teha ülejäänud andmetöötluste osas.

Viljar: sellega ei nõustu: AvTS § 28 lõikest 1 ja ÜM art 12 jj sisuliselt nõuavad andmetöötlustingimuste esitamist ning kodulehel kuvamist. Heaks näiteks on AKI enda privaatsuspoliitika – kuidas hoiame teie eraelulist teavet. Andmetöötlustingimustes tuleb ka ära kirjeldada kõik need toimingud, mis on seotud ja toimuvad ka mõne õigusakti alusel.

Bert: õigusliku raamistiku määratlemine ja isikuandmete töötlemise eelkontroll – see on seotud andmekaitsealise mõjuhindangu tegemisega.

Viljar: tegemist on organisatsioonisisese nõustamisega, millest võib välja kasvada ÜM art 35 kohane mõjuhindangu kohustus.

Nii IKS § 25 kui ka AvTS § 43 määratlevad ära, et andmete töötledajad (sh teabevaldajad) peavad kasutusele võtma erinevaid meetmeid andmete tervikluse, käideldavuse ja konfidentsiaalsuse tagamiseks.

Bert: kevadest tuleb ühe eraldiseisva nõudena juurde, et peab olema selge, mis on andmete allikad, kui andmesubjekt küsib seda – nt et mis andmekillu saime andmekogust X.

Bert: töötlemisel osaleva personali teadlikkuse tõstmine – seotud konfidentsiaalsuskohustusega kui ka koolitamisega.

Viljar: ametnike osas tuleb konfidentsiaalsuskohustus avaliku teenistuse seadusest, kuid avaliku sektorite töötajate osas peab tulema mõnest eriseadusest.

Bert: Juurdepääsuõiguste haldus või kasutajaliidesed – tuleks läbi mõelda, kuidas toimuks andmetele juurdepääsu haldus ning kuidas andmesubjekt saaks enda andmetele juurde, sh saaks ka realiseerida oma õigust andmete muutmiseks või kustutamiseks. On arusaadav, et see on seotud ka rahalise toega – ennekõike küsimusega kas see on rahaliselt mõistlik. Soovitav on kasutada ka andmejälgija teenust.

Kui selliseid päringuid ja taotlusi tuleb pidevalt, siis tasuks sel teemal läbi mõelda andmesubjektidele juurdepääsu tegemise lahenduse kasutajaliidesega.

Probleem on ka volikirjade alusel andmetele juurdepääsuõiguste saamisega.

Bert: andmetega ei ole lubatud andmekogusid testida nõ pärisandmetega – selleks tuleb luua nõ test-andmed.

Viljar: samuti ei ole lubatud õppe-eesmärkidel (koolituste jaoks) andmekogudele (sh reaalsele andmetele) juurdepääsu anda. Pärisandmetega testimises osas on AKI varasemalt teinud ka ringkirja.¹

Bert: vastutava ja volitatud töötajate vahel tuleb samuti paika panna töötlemistingimused ja konfidentsiaalsusnõuded – tulenevad ÜM art-st 28.

Bert: kolmandatele isikutele juurdepääsud – sageli on andmekogudes olevatele andmetele õigus oma avalike ülesannete täitmiseks sellist juurdepääsu saada, kuid probleem on siis, kui selline kasutajaõiguste temaatika on vägagi laialt määratletud.

AKI: juurdepääsuõiguste halduse temaatikat oleme sisustanud nii avaliku teabe seaduse üldjuhendis kui andmekogude juhendis.

Bert: X-tee kokkulepped – tuleb sõlmida selline kokkulepe teenuse osutaja ja teenuse kasutaja vahel, kuid ei ole selge, millises vormis ja mida selline kokkulepe peaks sisaldama, sh mis tasemel peaks see olema sõlmitud – selles osas ootaks ennekõike RIA sisendit.

See on osaliselt seotud ka sellega, et anda andmesubjektile infot, millistest andmeallikatest on andmed pärit.

Regulatsioonide kehtestamine alltöövõtulepingute sõlmimisel (volitatud töötajate kasutamine) – seotud samamoodi kolmandate isikutega sõlmitavate lepingutega: nt mh märkida selles konfidentsiaalsuskohustused, nõue võtta vajaminevad (sh vajadusel täpsustada) meetmeid, leppetrahvid, teabe hävitamine, vastutava töötaja võimalus kontrollida alltöövõtjat jne.

Kasulik on kehtestada järelevalveplaani ehk teatud intervalli tagant kontrollitakse andmekogud ja nendes toimuvad andmetöötlused üle – nt võtta eeskujuks ja aluseks turvaosaklasside määratlemise kohaselt + kontrollida teostatud andmetöötlustoiminguid.

Kui soovitakse andmeid anda AvTS-i alusel avaandmeteks mõnele ettevõttele, siis teha ka avaandmete mõjuhindang.

¹ http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ringkiri%20201503%20-%20testimine%20reaalandmetega.pdf.

Andmete kustutamine – kui mingi eesmärk on täidetud, siis tuleb otsustada, mis nendega edasi saab – seadusest tuleneb nõue, et tuleb need andmed kustutada. Andmekogude osas tuleb arvesada säilitamistähtaegadega ning kontrollida, kas Rahvusarhiiv on hinnanud seda teavet arhiiviväärtuslikuks. Säilitamistähtaja osas tuleb ka arvestada võimaliku nõuete esitamise võimalusega.

2. 11.45-12.05 Kohvipaus

3. 12.05- 12.30 IKS-i eelnõu hetkeseis – Viljar Peep

Väga uut informatsiooni ei ole, kuna hetkel ei ole uue isikuandmete kaitse (üld)seaduse regulatsiooni avalikkuse ette toodud – on teada, et see peaks lähiajal Justiitsministeeriumist välja minema, kuid see ei ole ilmselt kindel.

Eraldi teema on eriseaduste pakett – ca 113 seadust muudetakse, osad neist muudatustest on ennekõike vägagi kosmeetilised. Eeldatavasti läheb see eelnõu kooskõlastusringile alles sügisel. Sellest oleneb ka AKI enda juhiste muutmine.

Isikuandmete kaitse üldmäärusega seotud üldjuhendi sisu on sisulist sama, mis on AKI võrgulehel olevad rubriigid ning eeldatavasti ta ei muutu suurel määral.

4. 12.30- 13.10 AKS-de määramise ja üldmääruseks valmistumise hetkeseis asutustes – Viljar Peep

Nõukogu koosolekul osalejad esitasid ülevaate oma asutuses kui ka allasutustes toimuvate asjaolude osas – nii andmekaitse spetsialisti (AKS) määramise kui ka isikuandmete kaitse üldmääruse ettevalmistamise seisust.

Valdavalt on AKS ministeeriumite tasemel juba määratud või toimub see peatselt. Ministeeriumite allasutustele on ka teave AKS-i määramise kohustustest edastatud või tehakse seda peatselt. Samuti tegeletakse ministeeriumi ja/või haldusala üleste töörühmade/koostöövõrgustike tekitamise või sobitatakse olemasolevad töörühmad nii, et see kataks ka selle vajaduse ära.

Andmekaitse üldmääruseks ette valmistamiseks teostavad asutused enda asutuse sees erinevaid kaardistusi, analüüse ja vastavusauditeid nii andmetöötluste, andmekogude põhimääruste kui ka teiste õigusaktide muutmisvajaduste hindamiseks jne. Mõni asutus teostab seda koos teenuste korraldamise ja teabehalduse määrusest tulenevate teenuste kaardistamise nõudega. Samuti tegeletakse organisatsiooni käitumisjuhiste ja privaatsuspoliitikatega ning avaandmete kaardistamisega. Tegeletakse ka koolituste korraldamisega enda asutuse siseselt. Ühena esmastest tegevustest on isikuandmete kaitse üldmääruse art-st 30 tulenev kohustus kaardistada ning luua andmetöötlustoimingute register.

Viljar: soovitame Tallinna LV-sel, JuM-l koos KuM-ga koos tegelda isikuandmete kaitse üldmääruse art 30 kohase andmetöötlustoimingute registri näidise väljatöötamisega. Kui koostöö tulemusena saavutatakse mingi lõppdokument, siis saab selle lisada ka avaliku teabe nõukogu võrgulehele.

5. 13. 10 – 14.00 jooksvad küsimused ja ettepanekud

Järgmine kohtumine toimub aprillis, täpsem kuupäev on kokku leppimisel.

Koostas: Raavo Palu