Avaliku teabe nõukogu IV kohtumine
09.05.2018 kell 10:00 – 14:00
Koht: Andmekaitse Inspektsioon
Osalejad: Urmas Ojamäe (Rahandusministeeriumi infotehnoloogiakeskus), Aila Schmidt (Kultuuriministeerium), Kaspar Kala (Sotsiaalministeerium), Evelyn Tohvri (Tallinna Linnakantselei), Triin Nigul (Keskkonnaministeerium), Kertu Nurmsalu (Siseministeerium), Merit Valgjärv (Tallinna Linnakantselei), Aivar Ilves (Maaeluministeerium), Ivika Vutt (Maaeluministeerium), Janno Laas (Majandus- ja Kommunikatsiooniministeerium), Marju Müürisepp (Kaitseministeerium), Risto Rahu (Haridus- ja Teadusministeerium), Eneli Nõmm (Politsei- ja Piirivalveamet), Hille Oidemaa (Välisministeerium), Kaidi Paju (Riigikantselei), Ragnar Pirk (RIA), Kaidi Vapper (Keskkonnaministeerium), Andrea Kivi (Kultuuriministeerium), Kadri Kilp (Riigikantselei), Bert Blös (Justiitsministeerium), Viljar Peep (AKI), Urmo Parm (AKI), Raavo Palu (AKI), Elve Adamson (AKI), Annika Aavaste (AKI).

1. **10.00-11.00 Mõjuhinnang Tallinna Linnakantselei näitel + arutelu– Evelyn Tohvri**

Evelyn: Tallinna praktika kohaselt on mõjuhinnangu kohustuseks ennekõike infosüsteemid, kus on eriliiki isikuandmed. Näiteks on kavas teha uut infosüsteemi, millesse võib sattuda ka eriliigilisi iskuandmeid. Süstemaatiliste ulatusliku jälgimise all on mõeldud linnas olevad kaamerad: liikluskaamerad, valvekaamerad; eraldi küsitavus on, et kas üksik valvekaamera oleks ulatuslik ja sel puhul oleks vajalik mõjuhinnangut teha.

Viljar: Euroopa andmekaitseasutuste töörühmas olen esitanud soovi ulatuslikkuse teemat sisustada. Üks võimalus seda sisustada on numbriliste väärtusega, kuid kuna AKI-siseselt ei ole veel lõplikule seisukohale jõutud, siis veel avalikkuse ette neid ei tooda.

Ulatuslik alade jälgimune – sel teemal ei ole võimalik öelda, millal üksik kaamera muutub ulatuslikuks alade jälgimiseks.

Kaamerate puhul on ka, et võidakse teha tervikpilt erinevatest kaameratest.

Andrea: Neid kaameraid kasutatakse ennekõike turvalisuse eesmärgil, mitte töötajate enda jälgimiseks.

Viljar: uues IKS-s ei ole turvakaamerate osas ühtegi sätteid, sh kuidas tähistada ning millisel alusel avalik sektor seda kasutada saab.

Evelyn: piletiinfosüsteem oleks ilmselt andmekogude mõistes, mis vajaks mõjuhinnangu tegemist (ulatuslikkuse tõttu).

Viljar: perearste loeme avaliku sektori alla, võttes eeskujuks KüTS-i ehk AKS-i määramine ÜM art 37 kohaselt on vajalik. Mõjuhinnangu osas on jah see erisus, et üksik perearst seda ei pea tegema.

Evelyn: mõjuhinnangu koostamisel võeti eeskujuks Euroopa andmekaitseasutuste töörühma mõjuhinnangu kriteeriumitest;[1] see koosneb kolmest blokist – nt üks osa on andmetöötlusprotsessi kirjeldamine ehk andmetöötlusregistri osa (hinnatakse, kas on eriliigiline, kõrge ulatus jne). Algselt jagati seda 4 linna allasutusega, et testida seda vormi – haridus, finantsinfo, liikluskaamerad, sotsiaalsektor. Tulemus on see, et asutustel endal oli raske seda vormi täita ning seda peaks pigem tegema AKS koos infoturbespetsialistiga.

Linna infoturbespetsialist on välja töötamas lihtsamat lahendust, et ka eriteadmistega isik saaks ise hinnata seda ohtu.

[1] http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/wp248_rev.01_et.pdf.

Raavo: RIHA-s olevate andmekogude muutmisel tuleks teha mõjuhinnang vastavas eelnõu seletuskirjas. Ka praegu AKI-sse tulevate eelnõude korral, mis on seotud andmekogudega, tehakse märkus andmekaitselise mõjuhinnangu vajalikkuse kohta.

Evelyn: mõjuhinnangu koostamisel sai ka rohkem selgemaks, et kas üldse on kogutavad andmed isikuandmed või mitte. Selle põhjal sai ka parema ülevaate, et mis andmeid edaspidiselt enam ei ole vaja või mida enam ei küsita.

RIA: kui keegi küsiks enda kohta andmeid, siis mõjuhinnangu tulemusena sai ka selgemaks, et mis muudatusi oleks vaja andmekogudes teha, et saaks kiiremini vastuseid inimesele anda – nt teha mingi eraldi liides välja arendada.

Viljar: ohtude näidisloetelu isikuandmete kaitse üldmääruse (üldmäärus) põhjenduspunktis 75; samuti on suund mindud sellele, et hinnatakse riske andmesubjektile, mitte asutusele.

Bert: infoturbeliselt lähtudes; tuleks arvestada kas mingi meede või selle kasutamine vähendab riski andmesubjekti jaoks – seda tulebki arvestada.

Kaspar: nt eriliigiliste isikuandmete töötlemine ise on algupäraselt risk.

KeM: kui vaadata riskianalüüsi poolest, siis RIA kodukal on juhend riskihindamise osas – link: https://www.ria.ee/ee/kii-alusdokumendid.html.

RIA: ISKE läheb muutmisele; hetkel on seal sees mõningad meetmed, mis sisaldavad isikuandmete kaitse meetmeid; praegu sakslased ise ka arendavad enda nõudeid edasi.

AKI: Tuleks mõelda sellele, et kuidas majasiseselt isikuandmete kaitse teemalisi teadmisi nö säilitatakse – kas dokumendiregistris mingi elava dokumendina vms.

Urmo: soovitan tutvuda ISO 29134 standardiga – sealt saab ka raamistikku ja lähtekohta, kuidas üles ehitada mõjuhinnangut; link: https://www.evs.ee/tooted/iso-iec-29134-2017.

RIA: peatselt läheb avalikuks ka riskianalüüs elutähtsa teenuse osutajatele.

Evelyn: Tallinnal on mõte teha üks töövahend, mis hakkaks sisaldama üldmääruse art 30 kohast ülevaadet; sinna saab otsa teha mõjuhinnangu osa; samuti sisaldaks infot, andmesubjektile teabe andmise kohta; eraldi on avalike teenuste infosüsteem, kus on sadu teenuseid kirjeldatud; samuti on ka eraldi teavet RIHA-s andmekogude mõttes.

2. 11.00 – 11.30 Andmetöötlusregistri arutelu – Bert Blös

Viljar: üldmääruse art 30 on märgitud „register“, kuid oma olemuselt ei ole see eraldi register, vaid on „isikuandmete töötluse ülevaade“.

Viljar: koostasime ise AKI jaoks ka enda ülevaate, kuid see ei ole lõplikult valmis, kuna majasiseselt on lõpuni vaidlemata selle detailsuse aste. Selle ülevaate koostamisel tekkis ka majasisene vaidlus, et mis on käsitletav kaasvastutavate töötlejatena. Hetkel on meil veebilehel üldmääruse art 12 andmetöötlustingimused avaldatud, kuid üldmääruse art 30 kohase ülevaate avaldame oma veebilehel peale majasisest arutelu.

Bert: kui palju on võimalik üldmääruse art 12-14 teavitamiskohustust täita sellega, et esitatakse see isikuandmete töötluse ülevaade (ehk üldmääruse art 30 kohane ülevaade)?

Andrea: kui võrgulehele pannakse üldmääruse art 30 ülevaade, siis inimene ei pruugi sellest ise aru saada, mis dokumendiga on tegemist ning mida üldse tema andmetega tehakse.

Viljar: ka hetkel on AvTS § 28 lg 1 p 31^1 kohaselt vajalik esitada andmekaitsetingimused (nn privaatsuspoliitika); see on ka seotud üldmääruse art 12-14 – need on avalikud dokumendid. Üldmääruse art 30 on ülevaade ning seda peaks käsitlema erinevalt.

Viljar: kui üldmääruse art 30 ülevaade on osaliselt ka RIHA-s, siis saaks sellele viidata/linkida; iseasi on see, kas hetkel RIHA võimaldaks kogu seda teavet sinna üles anda. See tuleks konkreetsemalt üle hinnata, sest üldmääruse art 30 olevat teavet ei pruugi olla RIHA-s.

Raavo: esmapilgul tundub, et kõik teave RIHA-s olev teave ei kata üldmääruse art 30 ülevaadet.

Bert: ootaks AKI avaldatavat üldmääruse art 30 ülevaadet.

3. **11.30-11.50 Kohvipaus**
4. **11.50- 12.20 vastutava ja volitatud töötleja lepingu tingimustest – Bert Blös**

Bert: JuM-l väga palju selliseid volitatud töötlejaid ei ole, kes on eraõiguslikud juriidilised isikud – üks on nt Medisoft, kes töötleb vangide terviseandmeid. Organisatsioonilised, infotehnilised ja infotehnoloogilised turvameetmed selle lepingu osas on võetud suurel määral kehtivast IKS-st, mis kaob peatselt ära; märkusena olgu öeldud, et kui nüüd IKS kaotab ära, siis peale uue IKS-i peatüki, mis käsitleb õiguskaitseasutuste direktiivi osa, ei ole eraldi nö üldisel tasemel sisustatud samalaadsed nõuded turvameetmete osas. Seda lepingut saaks ka nt kasutada arenduslepingute jaoks – nt kui infosüsteem hakkab sisaldama eriliigilisi isikuandmeid. Tulevikus tuleks ilmselt volitatud töötlejaga sõlmitavas lepingus, et nt tuleb rikkumisest teavitada volitatud töötlejat. Oma olemuselt on infosüsteemi majutaja volitatud töötleja.

Bert: Google Analytics (GA), kui seda kasutatakse ja IP-aadresse kasutatakse maskeerimata viisil – siis kas on isikuandmete töötlemine?

Viljar: jah, GA soovib nö profileerida kasutajaid ning teda tuvastada; nt AKI võrgulehe omanik on RIK, kellelt tellime statistikat võrgulehe kasutatavuse kohta.

RIA: alternatiiv on mitte kasutada GA-d, vaid nö asutuse enda kõhus olevat tarkvara, mis teeks samaväärse töö ära, sh sel juhul ei toimuks ka andmete edastamist kolmandasse riiki ehk USA-sse.

Viljar: GA-l on võimekust ilmselt, et tuvastada selle IP taga olevat isikut; kui asutus ise teeb selle programmirakenduse, siis üldreeglina ei ole tal võimalik tuvastada isikut ehk need ilmselt ei ole isikuandmed.

Bert: kui GA-d ei soovita kasutada, siis tasub oma IT-asutusest selgitada välja, kuidas IP-d maskeerida.

KeM: üks võimalikest alternatiivides GA-le: https://matomo.org/.

Urmo: kui arendajal on juurdepääs isikuandmetele, siis ta on volitatud töötleja

PPA: kui andmekogule saab juurdepääsu eraõiguslik juriidiline isik, kuid ta eraldiseisvalt vastutava töötleja nimel andmeid ei töötle – kes ta siis on?

Viljar: tegemist on vastuvõtjaga.

Bert: kui antakse kellegile juurdepääs mingile andmekogule, siis tuleb ka kontrollida, kas seda juurdepääsu ka kohaselt täidetakse.

Bert: kui soovitakse piirata ülemäära juurdepääsu mõnele andmekogule, siis tuleks kasutada infotehnilisi meetmeid: nt kaupmees ei saaks ilma ID-kaarti kasutamata mingi andmebaasi vastu teha päringut.

Viljar: sellekohane näide on ilmselt ID-kaardi kasutamine hasartmängude korral – nt loto ostmiseks.

RIA: ennetava infotehnilise meetmena võiks mõelda, et kui nt päevas sisestatakse 10 isikukoodi, mille osas tulevad vastetena negatiivsed vastused, siis tekib piirang edasiste päringute tegemiseks.

Viljar: eraldi tasuks mõelda sellistesse lepingutesse lisada ka leppetrahvide teema.

KulMin: tuleks eraldi arutada, et mis RTK üldse on, sh kuidas riigiasutused sellega suhestuvad.
RMIT: hetkel tundub, et RTK korral need, kes kasutatavad andmekogusid/süsteeme, siis selles osas on teised asutused volitatud töötlejad.
Viljar: andmekogu pidamise mõttes võivad teised asutused olla volitatud töötlejad AvTS-i järgi; eraldi teema on, kuidas üldmääruse järgi on RTK ja talle andmeid edastav asutus: leian, et nad on koos kaasvastutavad töötlejad – nt tööandjal ehk asutusel on teatavad õigused ja RTK-l on teatavad õigused andmekogu pidamisel.

Urmo: turvatarkvarad pahavara kontrollimiseks: see toimub kas asutuses endas või selle tarkvarateenuse pakkuja juures; kui need käivad nö majast välja, siis on see teenuse osutaja volitatud töötleja; selle teemaga seonduvalt tuleb pidada meeles, et selles olukorras võib toimuda ka isikuandmete edastamist kolmandatesse riikidesse.
RIA: meil on eraldi veebis üleval üks tarkvara, kuhu saab lisada faili, mida programm hakkab kontrollima viiruste suhtes (http://cuckoo.cert.ee/); sel juhul toimub ka failis olevate isikuandmete töötlemine.
Urmo: sel juhul tuleb üle vaadata, kas selle teenuse juures on selgitavat infot, kuidas selle teenuse puhul isikuandmeid töödeldakse.

5. **12.20-13.00 Jooksvad küsimused (isikuandmete töötlemisest teavitamine art 13 ja 14)- Urmo Parm**

Urmo: AKI enda võrgulehel on juba üleval andmekaitsetingimused - http://www.aki.ee/et/inspektsioon/andmekaitsetingimused; üks võimalikest soovitustest: nt lisada töökuulutuse juurde link juba, et kuidas asutus töötleb isikuandmeid värbamisprotsessis.

6. **13.00-14.00 Andmekaitsespetsialistide (AKS) määramise ja üldmääruseks valmistumise hetkeseis asutustes – Viljar Peep**

Viljar: rakendus äriregistri kaudu AKS-de esitamiseks on juba 16.04. On mõned asutused, kellel veel ei ole määratud nö volitatud isikut, kes saaks iseteeninduspportaalis seda märkida.
Avalikkus näeb AKS-i nime ning kontaktandmeid; isikukoodi ega sünniaega ei nähta.
Viljar: AKI enda osas: AKS on määratud, andmetöötlustingimused on avaldatud; üldmääruse art 30 osas veel on vaidlused, kuid peatselt soovime majasisese aruteluga, peale mida avaldame oma sellekohase ülevaate.

Andrea: kas avaandmete osas on keegi mõjuhinnangut teinud?
PPA: meil on kolm kogumit, mille osas koostati analüüsidokument.
Raavo: 07.05 toimus MKM-s avaandmete teemal koosolek ning edaspidiselt peaks hakkama sellekohane teave koonduma Avaandmete portaali (https://opendata.riik.ee/).
KeM: 25.05 toimub Latitude raames avaandmete teemal üks arutelu, mis on tasuta – link: https://form.jotformeu.com/Tark_e_riik/data-ecosystems-seminar.
Viljar: eraldi oli kokkusaamine MKM-ga seoses SF-taotlustega ning AKI osalusega nende taotluste ülevaatamisel. Mõte oli, et see raha jagamiseks olev bürokraatia oleks lihtsam.

Nõukogu koosolekul osalejad esitasid ülevaate oma asutuses kui ka allasutustes toimuvate asjaolude osas – nii AKS määramise kui ka isikuandmete kaitse üldmääruse ettevalmistamise seisust. Valdavalt on AKS ministeeriumite tasemel juba määratud või toimub see peatselt.

Aktiivselt tegeletakse erinevate kaardistuste ja analüüside tegemisega – olgu selleks üldmääruse art 12-14 kohased andmetöötlustingimused kui ka art 30 kohase ülevaate koostamine. Samuti tegeletakse ka avaandmete temaatikaga ning oma töötajate koolitamisega. Mõned asutused loovad oma siseveebi eraldi rubriigi andmekaitse teema osas ning hakkavad seda järjest uuendama.

Mõned asutused märkisid, et üldmääruse art 30 kohase ülevaate tegemisega sai rohkem selgemaks, mis andmeid üldse töödeldakse ning sellest lähtuvalt saab teha edasisi samme, et oma teenuseid ja protsesse paremini juhtida ja osutada. Tegevusi on palju, kuid ilma seda tegemata poleks see teave välja tulnud.

Samuti tegeletakse erinevate lepingute, sisekordade ja asjaajamiskordade ülevaatamisega. Mitu asutust kavatsevad teha üldmääruse art 30 kohase ülevaate algselt ühe (all)asutuse baasil, et seda mudelit kasutada ka teiste (all)asutuste jaoks. Samuti tegeletakse sellega, et intsidentide korral oleks majasisesed protseduurid tuvastamaks, kas mingi intsident võib olla seotud ka isikuandmetega + kuidas selle intsidendi avastaja kui ka sellele reageerija peaksid toimima.

Viljar: kui ministeeriumitel tekib mingeid dokumente, et mida kõik saaksid kasutada, siis sellekohase teabe vahetamine on teretulnud, sh võiks selle ka nõukogu võrgulehele lisada.

Omavahel tasuks jagada sellised üldisemaid koolitusmaterjale; samuti võiks mõelda mingile veebipõhisele õppekeskkonnale.

Viljar: järgmine kokkusaamine oleks sügisel, kuid konkreetset kuupäeva ei ole veel võimalik öelda.

Koostas: Raavo Palu