RIIGI INFOSÜSTEEMI
HALDUSSÜSTEEM

RIHA võrgustiku seminar 16.05.2018

RIA kokkuvõte

RIHA võrgustiku seminaril arutati järgmistel teemadel:

1. Nõuetele vastavuse tõhus dokumenteerimine
2. Andmekoosseisu kirjeldamise lisandunud vajaduste parimal viisil lahendamine
3. Asutuste ja infosüsteemide seoste esitamine

Aruteludeks jaotati 30 osalejat kolme- kuni kuueliikmelisteks rühmadeks.

1. Infosüsteemiga seotud dokumendid

Riigi infosüsteemi nõuete hindamiseks esitatakse RIHAsse informatsiooni nii struktureeritult RIHAs täidetavate väljadena kui ka mittestruktureeritult mitmesuguste dokumentidena.

Kooskõlastajate ühise RIHAs dokumentatsiooni hindamise juhendi põhjal hinnatakse RIHAs 20 sellist nõuet, mille täitmise tõendamiseks tuleb esitada mingi dokument. Lisandub 2 nõuet seoses Euroopa Liidu isikuandmete kaitse üldmääruse rakendamisega. Nende nõuete nimekirja leiab selle dokumendi Lisast 1 ja seminari materjalidest.

Rühmatöö ülesanne oli siduda infosüsteemide arenduses ja halduses loodavad dokumendid RIHAs kontrollitavate ja dokumendi esitamisega seotud nõuetega. Kasutades kaartide sorteerimise meetodit, paluti osalejatel grupeerida RIHAs kontrollitavad ja dokumentidega seotud nõuded, näitamaks millisele nõudele vastavust millises dokumendis oleks mõistlik dokumenteerida. RIA ei soovi, et asutused looksid „RIHA jaoks vajalikku dokumentatsiooni“, vaid et RIHAsse lisatav informatsioon tekiks infosüsteemide normaalsel ning jätkusuutlikul arendamisel ja haldamisel.

Selle rühmatöö eesmärk oli leida optimaalne viis infosüsteemi nõuete hindamiseks vajaliku informatsiooni dokumenteerimiseks ning luua klassifikaator RIHAsse esitatavatele õigusaktidele ja tehnilistele dokumentidele.

Kaks rühma lahendasid ülesande sarnaselt, jaotades kontrollitavad nõuded teemadeks ja alamteemadeks (turvalisus, liidestused ja teenused, õiguslik alus, arhitektuur). Ülejäänud kolm rühma jaotasid nõuded kas:

- kahe dokumendikategooria vahel (põhimäärus ja tehniline dokument) ning pakkusid välja, et osadele dokumentide alusel kontrollitavatele nõutele võiks vastavust esitada küsimustiku täitmise vormis;
- hindajate vahel, kes mida kontrollib;
- või hindaja ja arendaja vahel, kes millelegi peaks RIHAs vastama.

Täiendavalt nimetati muredena järgmist:

1. Mitmed nõuded on üksteisest sõltuvad ja on vajalik täita ainult teatud juhtudel, mistõttu „kõigile infosüsteemidele“ kehtivaid nõudeid ei ole, vaid olenevalt infosüsteemi olemusest kehtib talle eraldi „komplekt“ nõudeid.
2. Paljuski on tekkinud olukord, kus kõige paremini teab infosüsteemi ülesehitusest (ja detailidest) omaniku või haldaja asemel arendaja.
3. Mitme nõude puhul selgus, et infosüsteemi omanikud ei dokumenteerigi oma tavapärase arenduse ja halduse käigus konkreetse nõude täitmist.

Kuna ühist viisi ei avaldunud, siis võib väita, et ükski keskselt pakutav lahendus ei leia kõigi osapoolte heakskiitu. Edasiste valikute puhul lähtub RIA eelkõige võimalikult suurele osale kasutajatele sobivusest ja riigiüleselt summaarse töö mahu vähendamisest. RIA järeldused sellest grupitööst:

1. RIHA kasutajad eristavad kõige selgemalt infosüsteemi omaniku esitatud õigusaktide abil kontrollitavad nõudeid. Nende ilmutatud eristamine tänases (ja tuleviku) RIHAs on põhjendatud.
2. Infosüsteemi omanikud sooviks iga nõude juures teada, kes nõude täitmist hindab. Seda nii arenduse planeerimisel kui ka nõude täitmisel tekkivate küsimuste lahendamiseks. Seega tuleb RIHAsse nõude juurde lisada hindaja kontakt, kes oskab vastata küsimustele.
3. Kuna paljud kasutajad ei erista erinevaid tehnilisi nõudeid ja dokumente, siis teeb RIA koostööd IT-asutuste ja arendusettevõtetega, et koostada nimekiri tehnilistest dokumentidest.
4. Nõude puhul, mida tavaliselt eraldi dokumendina ei kirjeldata, tuleks RIHAsse luua pigem eraldi vabas vormis väli, kuhu kirjeldaja saab lisada pikema selgituse. Vajadusel saab kirjeldaja lisada viite konkreetse dokumendi peatükile/leheküljele.
5. Nõudeid tuleb veelgi täpsustada ning analüüsida, milliseid tööd mugavdavaid automaatseid algoritme saab rakendada, et nõude täitmine ja kontroll sõltuks:
    - teistele nõuetele vastamisest (nt kui ei sisalda aadressiandmeid, siis järgnevaid ADSiga seotud nõudeid ei pea täitma ja selgitama);
    - infosüsteemi olemusest (nt kui süsteem ei ole arhiiviväärtuslik, siis andmete eraldamise funktsionaalsust pole vaja).

2. Infosüsteemi andmekoosseis

Infosüsteemis töödeldava andmekooseisu kirjeldamiseks tuleb RIHAsse esitada andmed kirjeldatuna seitsmes veerus (andmeobjekti nimi, isikuandmeteks olek, põhiandmeteks olek jne). Nõuete hindajad on RIA-le esitanud täiendavad vajadused (nt avaandmeteks olek, juurdepääsupiirangu alus, kasutatav klassifikaator jne) RIHAs registreeritava infosüsteemi andmekoosseisu kirjeldamiseks. Selle tulemusel kasvaks kirjeldatavate veergude arv seitsmelt viieteistkümnele.

Rühmatöö ülesanne oli analüüsida, kas ja milliseid andmeid saaks andmekoosseisu kirjeldamiseks hõlmata automaatselt olemasolevatest analüüsidokumentidest, andmemudelitest, andmebaasistruktuurist jms.

Selle rühmatöö eesmärk oli leida RIHAsse esitatava andmekoosseisu uus struktuur ja andmehõive viisid.

Ühiselt leiti, et uuendatud andmekoosseisu kirjeldamiseks on vaja senisest kaks korda rohkem andmeid. Kahjuks pole võimalik enamik andmeid automaatselt hõivata, palju tuleks teha käsitööd. Põhjuseks on see, et andmekoosseisu kohta pole sellist infot kirjeldatud või pole andmeallikas masinloetav. Andmeid saab hõivata andme- ja infomudelitest (sh andmebaasiskeemist), põhimäärusest, X-tee kasutusstatistikast, avaandmete kirjeldusest ja mõjuhinnangust ning X-tee teenuste või API-de kirjeldustest ainult osaliselt. Avaldati arvamust, et mitmete kirjeldusvajaduste osas oleks mõistlik andmemudeleid täiendada, lisades teabe näiteks andmete isikuandmeteks oleku kohta. See oleneb asutuse senisest küpsustasemest ning asutuseüleselt ühiseid masinloetavaid allikaid ei olnud võimalik tuvastada.

Lõplik andmekoosseisu struktuur ja selgitused tuleb ära tuua RIHA kooskõlastajate eraldiseisvates (ja/või ühises) korras. RIA saab RIHA abimaterjalides infosüsteemi omanikele anda suuniseid vajalike algandmete vaatamiseks/hõlmamiseks.

3. Infosüsteemidega seotud asutused

Asutused tegutsevad riigi infosüsteemis erinevates rollides. Riigi infosüsteemi normivates õigusaktides kasutatakse asutuste rollide nimetamisel mitmesuguseid tähistusi: avaliku teabe seaduses räägitakse vastutavast ja volitatud töötlejast, teenuste korraldamise ja teabehalduse aluste määruses haldajast ja sisestajast, isikuandmete kaitse üldmääruses vastuvõtjast ja kaas-vastutavast töötlejast. RIHAs kasutatakse õigusterminite asemel suupärasemaid selgemalt mõistetavaid termineid (näiteks omanik). Igapäevases suhtluses kasutavad infosüsteemide haldajad asutuste rollide kirjeldamisel mõisteid tähenduses, mis ei pruugi kattuda õigusterminitega.

Rühmatöö ülesanne oli nimetada asutuste rolle, mis on vajalikud infosüsteemi igapäevasel haldamisel, teistega suhtlemisel, teenuste arendamisel jne. Paluti kirjeldada ka iga rolli peamisi ülesandeid ja järjestada rollid igapäevase suhtluse vajaduse järgi.

Selle rühmatöö eesmärk oli leida riigi infosüsteemi haldamiseks vajalikud olulisemad infosüsteemide ja asutuste seosed, mida RIHAs näidata.

Leidis kinnitust arvamus, et asutused kasutavad igapäevases suhtluses asutuste rollide kirjeldamiseks mõisteid teises tähenduses kui õigusaktis (näiteks avaliku teabe seaduse mõistes *volitatud töötleja* puhul kasutatakse mõistet *haldaja*).

Nimetati järgmisi olulisi rolle (paksus kirjas on toodud rohkem mainitud rollid):

- andmeandja
- **arendaja (kõik grupid)**
- hindaja, kui kooskõlastaja ja järelevalve teostaja / kooskõlastaja
- majutaja

- **omanik (kõik grupid)**
- RIHA omanik
- **kasutaja / klient / teenuste kasutaja / teenuse saaja**
- **haldaja / teenusepakkuja**
- vaatleja
- vastutav töötleja

Selgus, et kõik grupid nimetasid vajalike seostena omanikku ja arendajat. Leidus arvamusi, et igapäevasel suhtlemisel pole vajalikud mitte niivõrd asutused kui konkreetsed inimesed nendest asutustest kellega on vaja ühendust saada. Toodi ka välja, et sageli ei piisa (ja polegi mõistlik) konkreetsete rollide nimetustest, vaid oleks vaja kirjeldada rolle tegevuspõhiselt ehk milliseid ülesandeid täidavad nad konkreetse infosüsteemi puhul.

RIA plaanib selle alusel lisada RIHAsse järgnevad rollid:

1. Infosüsteemi omanik (olemas, võrdne vastutava töötleja mõistega).
2. Infosüsteemi haldaja – asutus, kes teostab tegelikku võimu infosüsteemis töödeldavate andmete üle (võrdne volitatud töötleja eriliigiga).
3. Infosüsteemi kasutaja – infosüsteemi andmeid vahetult tarbiv asutus (võrdne volitatud töötleja eriliigiga).
4. Infosüsteemi arendaja – infosüsteemi tarkvaratehniliselt arendanud või arendav asutus/ettevõte.

Iga rolli kirjeldamise (infosüsteemiga seostamise) kohustus peab tulenema vastavast nõudest.

4. Kommentaarid, mõtted ja ettepanekud?

Tagasiside on oodatud RIA kasutajatoele: help@ria.ee

Lisa 1. RIHA dokumentide nõuded[1]

1. Kas andmekogu asutamise eesmärgid on RIHAs kirjeldatud vastavalt alusdokumentidele?
2. Kas põhimääruse eelnõus kirjeldatud andmekogu vastab riigi infosüsteemi nõuetele?
3. Kas andmekogu on liidestatud ADSiga otse või kaudselt?
4. Kas aadressiandmeid hoitakse ajakohasena, st uuendatakse regulaarselt?
5. Kas ja milliseid X-tee teenuseid (vms) ja kui sageli kasutatakse andmete ajakohastamiseks?
6. Kas ja kuidas andmekogus säilitatakse aadresside muutmise ajalugu?
7. Kas andmekogu edastab aadressiandmeid oma teenuste kaudu teistele osapooltele? Millistele andmekogudele ja millise peavõtmega?
8. Kas andmetöötlus on turvameetmete kirjelduse kohaselt piisavalt turvaline?
9. Kas ISKE turvatasemed on määratud andmete turva- ja riskianalüüsi alusel?
10. Kas andmevahetus riigi infosüsteemi kuuluvate andmekogudega toimub X-tee kaudu?
11. Kui asutamisel planeeritakse pakkuda X-tee teenuseid, kas need on tehnilises dokumentatsioonis kirjeldatud?
12. Kas RIHAsse kantud andmekogus jälgitakse riigi infosüsteemi haldamise põhimõtteid?
13. Kas andmekogus töödeldakse isikuandmeid pädevuse piires?
14. Kas isikuandmete kasutamine on logitud ja monitooritud?
15. Kas andmetele on õiguslik tähendus omistatud seadusega?
16. Milliste andmekogudega on liidestused (planeeritud)?
17. Kas säilitustähtajad tulenevad seadusest, põhimäärusest, õigusaktist?
18. Kui andmed on arhiiviväärtuslikud: kas andmete eraldamise funktsionaalsus on olemas?
19. Kas andmeid saab masinloetaval kujul edastada RA digitaalarhiivi?
20. Kas ja kuidas on andmesubjektile võimaldatud juurdepääs enda andmetele?
21. Kas andmekaitseline mõjuhinnang on kohane?
22. Missugune on andmetöötlejate tööjaotus (kes vastutab mille eest)?

[1] Nõuded, mis on seotud konkreetsete dokumentidega (st pole sisestatavad andmeväljad või osa andmekooseisu kirjeldusest)