Vabariigi Valitsuse määruse „E-toimiku süsteemi asutamine ja e-toimiku süsteemi pidamise põhimäärus“ eelnõu seletuskiri

I. Sissejuhatus

Määruse eelnõu on välja töötatud „Kriminaalmenetluse seadustiku“ (edaspidi KrMS) § 210 ja „Väärteomenetluse seadustiku“ (edaspidi VTMS) § 81^1 alusel ja kooskõlas „Avaliku teabe seaduse“ (edaspidi AvTS) § 43^5 lõikega 1.
KrMS-i ja VTMS-i eelpool nimetatud ning e-toimiku süsteemi volitusnormi sisaldavad paragrahvid jõustuvad 15. juulil 2008. Samal ajal jõustub ka põhimäärus.

E-toimiku süsteem on õiguskaitseasutuste vaheline keskne infosüsteem menetlusinfo hoidmiseks ja edastamiseks. E-toimiku süsteem ühendab erinevad kriminaalasju menetlevad osapooled ja organisatsioonid (politsei, prokuratuur, kohus) ühtsesse inforuumi tagades kehtiva informatsiooni pideva kättesadavuse kõikidele menetlejatele.

E-toimiku süsteem laiemas tähenduses koosneb tsentraalsest andmebaasist e-toimikust, mis sisaldab toimiku informatsiooni ning klientsüsteemidest, kes toimiku informatsiooni manipuleerivad – salvestavad ja muudavad. Igas klientsüsteemis on kirjeldatud ligipääsuõigused vastava ametkonna töötajatele, et kasutada e-toimiku tsentraalseid teenuseid. Klientsüsteemides hoitakse eraldiseisvalt minimaalset informatsiooni, mis ei ole vajalik teistele menetlusosalistele.

Lõppkasutaja jaoks ei ole e-toimik otsene töövahend. Lõppkasutaja jääb kasutama temale harjumuspärast töökeskkonda pea samal viisil nagu praegu. Selles mõttes võib ka väita, et e-toimik on üksnes tehniline projekt ja ei puuduta oma esimestes faasides olemuslikult menetlevate asutuste töökorraldust.

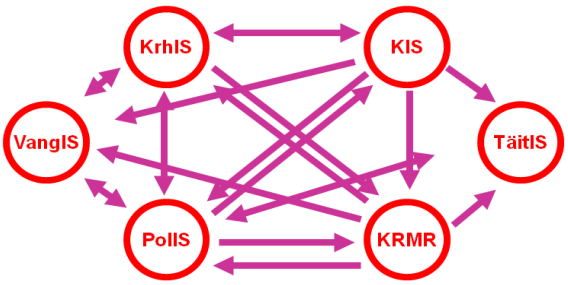
Tsentraalselt hoitakse informatsiooni, mis on vajalik või peab olema menetluse käigus nähtav rohkem kui ühele menetlusosalisele. E-toimiku süsteem hoiab ka piiratud ulatuses äriloogikat – näiteks kehtestab reegleid – milline menetleja millises protsessi etapis saab toimikusse dokumente lisada või toiminguid teha.

E-toimiku süsteem on oma olemuselt radikaalselt uuenduslik infosüsteem kuna põhineb valdkondliku tööloogika teenindamise eesmärgil – toetatakse tervet (kriminaal)menetlusprotsessi läbi mitme eraldiseisva asutuse ja infosüsteemi.

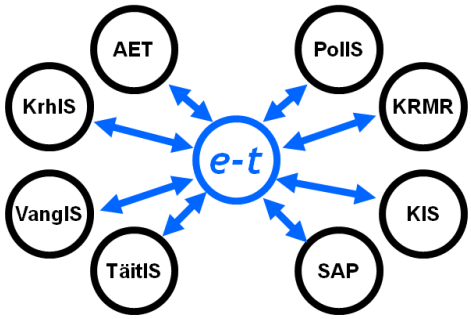
Alternatiiviks e-toimiku süsteemi arendamisele oleks olnud valdkondlike ja organisatsioonikesksete infosüsteemide edasiarendamine sidustades neid läbi eraldiseisvate andmeülekande kanalite, mis tooks kaasa probleemid dokumentide ja andmete autentsuse, usaldusväärsuse ja originaalsusega. E-toimiku süsteem väldib nimetatud probleeme läbi menetluste põhiandmete koondamise kasutamiseks kõikidele menetlusega seotud isikutele ning organisatsioonide. Nimetatud lahendus tagab lõppkokkuvõttes lisaks andmete usaldusväärsusele ka arenduste võrreldava suhtelise odavuse.

Valikuid kahe alternatiivi vahel iseloomustavad järgmised skeemid:

E-toimiku süsteemi eelse süsteemi tulem:



Kavandatud E-toimiku süsteem:



Eelnõu ja seletuskirja on koostanud Justiitsministeeriumi justiitshalduspoliitika osakonna infosüsteemide ja tööprotsesside talituse nõunik Siim Jurkatam (tel: 680 3111; e-post: siim.jurkatam@just.ee) ja Justiitsministeeriumi justiitshalduspoliitika osakonna infosüsteemide ja tööprotsesside talituse juhataja Karl Laas (tel: 680 3142, e-post: karl.laas@just.ee).

II. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb kaheksast peatükist:
1. peatükk Üldsätted
2. peatükk E-toimiku süsteemi töötlejad
3. peatükk Kannete tegemine e-toimiku süsteemi
4. peatükk Juurdepääs e-toimiku süsteemi andmetele
5. peatükk E-toimiku süsteemi järelevalve ja turvameetmed
6. peatükk E-toimiku süsteemi finantseerimine ja likvideerimine
7. peatükk E-toimiku avalik liides
8. peatükk Rakendussätted

1. peatükk Üldsätted

§ 1. E-toimiku süsteemi asutamine: Määrusega asutatakse riigi infosüsteemi kuuluv õiguskaitseasutuste ühine menetluste andmekogu ametliku nimetusega „E-toimik“. Sarnaselt KrMS ja VTMS muutmise eelnõuga on määruses ja seletuskirjas edaspidi E-toimikut nimetatud e-toimiku süsteemiks.

§ 2. E-toimiku süsteemi ülesehitus: E-toimiku süsteemi peetakse ühetasandilise elektroonilise andmekoguna. Oma olemuselt on see tsentraalne andmekogu, millega on andmevahetuskihi X-tee kaudu liidestatud klientinfosüsteemid (klientinfosüsteemi mõiste on avatud järgmises paragrahvis). E-toimiku süsteemi pidamisel kasutatakse automatiseeritud andmetöötlust ja e-toimiku süsteemi andmed säilitatakse digitaalsel kujul.
E-toimiku süsteem ristkasutab teisi andmekogusid vastavalt kokkuleppele nende andmekogude vastutavate töötlejatega. E-toimiku süsteemi rakendamise esimeses etapis saab e-toimiku süsteem lisaks klientinfosüsteemidele andmeid ka Rahvastikuregistrist, Äriregistrist ja Aadressandmete süsteemist. Tulevikus tuleb kindlasti andmevahetus ka Karistusregistri, Täitemenetlusregistri (TäitIS) ja Kinnipeetavate registriga (VangIS).

§ 3. Klientinfosüsteemid: Avab klientinfosüsteemi mõiste. Klientinfosüsteem on e-toimiku süsteemiga liidestatud andmekogu või register, mis edastab e-toimiku süsteemile selle eesmärkide täitmiseks vajalikke andmeid ja võimaldab teostada klientinfosüsteemile vajalikke päringuid menetlustoimingute läbiviimiseks. Klientinfosüsteemide vahendusel andmeid sisestavad kasutajad on e-toimiku süsteemi andmeandjad AvTS § 43^5 lg 2 mõttes. E-toimiku süsteemi rakendamise esimeses etapis on liidestatud klientinfosüsteemideks: e-toimiku avalik liides (AET), kohtute infosüsteem (KIS), politsei menetluse infosüsteem ja kriminaalmenetlusregister (KRMR). Tulevikus lisandub kindlasti ka riigikohtu infosüsteem ja väärteomenetluse infosüsteem.
Natukene eriline on olukord praeguse riikliku kriminaalmenetlusregistriga, milles sisalduvad andmed kantakse kõik üle e-toimiku süsteemi ning register selle praegusel kujul lakkab töötamast. Selle funktsioone hakkab asendama e-toimiku süsteem. Samas kasutajaliides kui selline jääb ning infosüsteemiga hakkavad edaspidi peamiselt tööd tegema prokurörid (aga ka teised KrMR §-s 31 nimetatud uurimisasutused). Sellest tulenevalt on tarvis teha suuremaid muudatusi ka kriminaalmenetlusregistri põhimääruses.
Uute klientinfosüsteemide liitumisel e-toimiku süsteemiga peaks muutma ka käesolevat määrust, et see kajastaks reaalset olukorda.

2. peatükk E-toimiku süsteemi töötlejad

§ 4. E-toimiku süsteemi vastutav ja volitatud töötleja: E-toimiku süsteemi vastutav töötleja on Justiitsministeerium ja volitatud töötleja on Registrite ja Infosüsteemide Keskus (edaspidi RIK). Justiitsministeerium on e-toimiku süsteemi vastutav töötlejana ära nimetatud ka KrMS §-s 210 ja VTMS §-s 81^1.

§ 5. Vastutava töötleja ülesanded: Sätestab e-toimiku süsteemi vastutava töötleja ehk Justiitsministeeriumi ülesanded. Vastutava töötleja peamised ülesanded on kooskõlas AvTS § 43^4 lg 1, mille kohaselt vastutav töötleja korraldab andmekogu kasutusele võtmist, andmekogu pidamist ja andmete töötlemist, vastutab andmekogu haldamise seaduslikkuse ja andmekogu arendamise eest.
Oluline on siinkohal silmas pidada punktis 2 sätestatut, mille kohaselt Justiitsministeerium vastutab e-toimiku süsteemi pidamise ja andmete väljastamise õiguspärasuse ja otstarbekuse eest. See punkt ei tähenda mitte seda, et Justiitsministeeriumil on vaba voli otsustada, millal, mis ulatuses ja kellele andmeid e-toimiku süsteemist väljastatakse vaid see punt sätestab seda, et Justiitsministeerium peab tagama selle, et andmete väljastamine oleks kooskõlas seadusega. Näiteks KrMS § 214 lg 1 kohaselt võib kohtueelse menetluse andmeid avaldada üksnes prokuratuuri loal ja tema määratud ulatuses. Seega on tarvis nimetatud andmete väljastamiseks prokuratuuri luba.

§ 6. Volitatud töötleja ülesanded: Sätestab e-toimiku süsteemi volitatud töötleja ehk RIK-i ülesanded. Volitatud töötleja peamised ülesanded on kooskõlas AvTS § 43^4 lg 3, mille kohaselt volitatud töötleja on kohustatud täitma vastutava töötleja juhiseid andmete töötlemisel ja andmekogu majutamisel ning tagama andmekogu turvalisuse. RIK-il on ka ülesanne tagada kasutajate abistamine e-toimiku süsteemi kasutamisel.

§ 7. Volitatud töötleja kasutajate liigid: Sätestab volitatud töötleja kasutajate liigid ja nende õigused. Volitatud töötleja kasutajate liikideks on: haldur, administraator ja arendaja.
Halduril on õigus teha andmete kohta päringuid ning põhjendatud vajaduse olemasolul e-toimiku süsteemi tõrgeteta töö või andmetervikluse tagamiseks vaadata ja muuta andmeid, kui klientinfosüsteemi kasutajal endal ei ole võimalik parandusi sisse viia. Andmete vaatamine ja

muutmine ei saa toimuda kellegi suva järgi. Selleks peab olema põhjendatud vajadus ning läbima peab teatava menetlusskeemi. Seda skeemi on täpsemalt kirjeldatud §-s 12.
Administraatoril on õigus pääseda ligi kõigile andmetele ja logidele, et tagada süsteemi tõrgeteta töö.
Arendajal on õigus pääseda ligi kõigile e-toimiku andmetele ja logidele, kui süsteemis on tuvastatud tõrge, mille parandamine ei ole administraatori või halduri pädevuses.

§ 8. Volitatud töötleja kasutajate registreerimine: Sätestab volitatud töötleja kasutajate registreerimise menetluse. Uue kasutaja registreerimiseks edastab kasutaja vahetu ülemus volitatud töötleja poolt määratud kontaktisikule (nt haldurile, kes tegeleb kasutajate lisamisega) vastavasisulise taotluse. Kui kasutajale ei laiene kehtivatest õigusaktidest tulenev isikuandmete saladuses hoidmise kohustus, edastab ta veel lisaks kasutaja poolt allkirjastatud määruse lisas 1 toodud isikuandmete saladuses hoidmise kohustuse vormi. Kasutajaliik määratakse vastavalt § 7 lõikele 1.
Kui kasutaja ametinimetuse, volitused või muud andmed muutuvad või kui tekib kasutaja väljaregistreerimise vajadus (nt töösuhte lõppemisel), siis kohustub kasutaja vahetu ülemus esitama vastavad andmed volitatud töötleja poolt määratud kontaktisikule. Kasutusõiguse sulgemise peab volitatud töötleja korraldama viivitamatult, et vältida selleks volitusi mitteomava isiku ligipääsemist e-toimiku süsteemi.

§ 9. Klientinfosüsteemi töötleja ülesanded: Sätestab klientinfosüsteemi töötleja ülesanded. Siinkohal ei ole vahet tehtud klientinfosüsteemi vastutaval ja volitatud töötlejal. Eelkõige sellepärast, et tihti on nendeks sama isik. Siinnimetatud ülesannete täpsem jagamine nende kahe töötlejate vahel (juhul kui on tegemist kahe erineva isikuga) jääb nende enda omavaheliseks kokkuleppeks, mis peaks olema sätestatud ka klientinfosüsteemi põhimääruses.

§ 10. Klientinfosüsteemi kasutajate liigid ja kasutajate registreerimine: Sätestab korra, et klientinfosüsteemi kasutaja registreeritakse ainult klientinfosüsteemis. Täpsema registreerimise korra kehtestab klientinfosüsteemi vastutav töötleja. Samuti määratakse klientinfosüsteemi kasutaja liik kasutaja registreerinud klientinfosüsteemi poolt. Kasutajaliigid ning nende määramise põhimõtted peaksid olema sätestatud klientinfosüsteemi põhimääruses. Tagatud peab olema see, et andmetele juurdepääs võimaldatakse isikule vaid tema ametiülesannete täitmiseks. Klientinfosüsteemi vastutav töötleja vastutab lõppkokkuvõttes selle eest, et vastavast klientinfosüsteemist tehtud päring e-toimiku andmete kohta on tehtud selleks vastavaid õigusi omava isiku poolt.

3. peatükk Kannete tegemine e-toimiku süsteemi

§ 11. E-toimiku süsteemi kanne: Sätestab, mida peetakse silmas e-toimiku süsteemis (eelkõige põhimääruses) mõiste „kanne“ all. E-toimiku süsteemi kanne on menetlust puudutavate andmete sisestamine, lisamine/täiendamine, parandamine, tühistamine või kustutamine. Sisestatud andmeid hoitakse tsentraalselt e-toimiku süsteemis, millele tagatakse klientinfosüsteemidele juurdepääs vastavalt §-le 15. Samuti täpsustatakse, milliseid andmeid kantakse e-toimiku süsteemi kriminaal- ja väärteomenetluse korral. Tulevikus, kui e-toimiku süsteem rakendub ka tsiviil- ja haldusmenetluses, tuleb seda paragrahvi täiendada vastavate menetluste osas. Täpsemad andmed, mida e-toimiku süsteemi kantakse, on kirjas määruse lisades 2 ja 3.
Kuna e-toimiku süsteem sisaldab andmeid, mis on vajalikud rohkem kui ühele menetlusosalisele, siis on oluline, et andmete ja dokumentide sisestamisega ei viivitataks ülemäära kaua. Seepärast on siin kiire ja efektiivse menetluse tagamiseks kehtestatud ka väga

oluline põhimõte, et kanne tehakse ja dokumendid sisestatakse ja salvestatakse e-toimiku süsteemi viivitamata pärast kande tegemise aluseks oleva sündmuse toimumist, sellest teadasaamist, dokumendi vastuvõtmist või loomist klientinfosüsteemis.

§ 12. E-toimiku süsteemi kannete tegemise kord: Sätestab e-toimiku süsteemi kande tegemise korra. Kande tegemine toimub läbi klientinfosüsteemi piisava aluse olemasolul kande tegemise eest vastutava isiku poolt. Kandeid peab teha saama vaid selleks õigustatud isik. Seesama kandeid tegev pädev isik on e-toimiku süsteemi jaoks andmeandja.
Andmed sisestab see menetleja, kes vastavad andmed tuvastab. Kuni andmed ei ole teada, jäetakse vastavad andmeväljad täitmata. Kui sisestatud andmed osutuvad hiljem ebaõigeteks või täpsustuvad, parandab õiged või täpsed andmed tuvastanud menetleja registrikande.
Kohtuväline menetleja kannab enda tuvastatud andmed e-toimiku süsteemi hiljemalt väärteomenetluse lõpetamise või lõpuleviimise, uurimisasutus hiljemalt kriminaalmenetluse lõpetamise või kohtueelse menetluse lõpuleviimise, prokuratuur hiljemalt kriminaalmenetluse lõpetamise või kriminaalasja kohtusse saatmise, kohus hiljemalt kohtulahendi tegemise staadiumis.
E-toimiku halduri poolt tehtavaid kandeid võib tinglikult jagada kahte rühma: kanded, mis on seotud sisulise vea parandamisega ning kanded, mis on seotud tehnilise vea parandamisega. Esimesel juhul tohib haldur kannet teha vaid siis, kui parandust sooviva kasutaja asutuse juhi või tema poolt määratud isik esitab kirjaliku taotluse. See säte ei kohaldu siis, kui kasutajal endal on võimalik paranduskanne ära teha. Eesmärk on vältida olukorda, kus suvaline isik saaks haldurile helistada ning nõuda kande tegemist. Sellist asja ei saa lubada. Tehnilise vea parandamiseks tehtavat kannet tohib haldur teha vaid siis, kui tehniline viga on eelnevalt registreeritud volitatud töötleja tehniliste vigade haldamise süsteemis.
Kande tegija vastutab enda poolt e-toimiku süsteemi kantud andmete õigsuse eest. E-toimiku süsteemi haldur vastutab tema poolt tehtud kande eest vaid juhul, kui ta ei järginud käesolevas paragrahvis kehtestatud korda.

§ 13. E-toimiku süsteemi andmete säilitamise tähtajad: E-toimiku süsteemi sisestatud andmed säilitatakse vastavalt menetlusseadustikes ja nende alusel antud õigusaktides sätestatud korras. Samadest õigusaktidest ning lisaks veel „Arhiiviseadusest“ tulenevad ka juhised, mida andmetega edasi teha. Kas tuleks need arhiveerida või mitte ning kui kauaks peab neid säilitama. Näiteks tuleks siinkohal kindlasti arvestada KrMS § 209 regulatsiooni.

§ 14. E-toimiku süsteemi andmete õiguslik tähendus: Tulenevalt AvTS § 43^6 lõikele 4 antakse õiguslik tähendus andmetele seadusega. Sama põhimõtet on korratud ka määruses. E-toimiku süsteemi rakendamise lõppeesmärgiks on see, et kõikidel andmetel oleks õiguslik tähendus, mis võimaldaks e-toimiku süsteemis pidada täisdigitaalset toimikut.

4. peatükk Juurdepääs e-toimiku süsteemi andmetele

§ 15. Juurdepääs e-toimiku süsteemi andmetele: Volitatud töötleja võimaldab klientinfosüsteemi kasutajale e-toimiku süsteemi andmetele juurdepääsu klientinfosüsteemi vahendusel. Juurdepääsu ulatus määratakse vastavalt kasutaja liigile klientinfosüsteemis arvestades § 16 nimetatud piiranguid. E-toimiku süsteemi teenustaseme tingimused (SLA) ja tehnilised juurdepääsutingimused klientsüsteemidele kehtestab justiitsminister kooskõlastatult klientinfosüsteemide töötlejatega määrusega.
E-toimiku süsteemi kannete ja päringute tegemise õigus on kõikide klientinfosüsteemide peale e-toimiku avaliku liidese kasutajatel vaid tema seadusest ja teistest õigusaktidest tulenevate ülesannete täitmiseks. Vastutaval töötlejal on õigus seda asjaolu kontrollida. Väärkasutuse avastamine võib olla aluseks e-toimiku süsteemile kasutusõiguse piiramiseks,

peatamiseks või lõpetamiseks. Nimetatud kontrolliõiguse puhul tuleks silmas pidada seda, et Justiitsministeeriumil ei ole selle raames võimalik vaadata kande või päringu sisu. Selline võimalus on tehniliselt välistatud. Peamine informatsioon peitub selles, millise menetluse raames on kanne või päring tehtud. Eesmärk on kontrollida seda, et kasutajad ei kasutaks andmekogu enda uudishimu või muude isiklike huvide rahuldamiseks. Taunitavad on süstemaatilised ühe ja sama menetluse (toimiku) vaatamised, kui seda teinud isik ei ole kuidagi menetlusega seotud. Kontrolli teostatakse RIK-i e-toimiku süsteemi halduri poolt Justiitsministeeriumi ametnikule esitatud logide põhjal. Selline lahendus välistab olukorra, kus kolmandal isikul (siinkohal eelkõige halduril ja ametnikul) oleks võimalik ringiga ligi pääseda e-toimikus sisalduvatele andmetele.

§ 16. Klientinfosüsteemi kasutaja juurdepääsu erisused sõltuvalt andmete salastatuse astmest: E-toimiku süsteemis on võimalik eristada kolme liiki andmete salastatuse astet: avalik, piiratud ning salastatud. Salastatuse astet „avalik“ omavatel andmetel puuduvad juurdepääsupiirangud. Need andmed avaldatakse internetis ning neid näevad kõikide klientinfosüsteemide kasutajad. Näiteks kuuluvad siia kategooriasse kohtuistungite toimumise ajad ning jõustunud kohtuotsused.
Salastatuse astet „piiratud“ omavatel andmetel on osaline juurdepääsupiirang. Piiratud andmeid näevad piisavate õiguste olemasolul selle klientinfosüsteemi kasutajad, kus menetletakse või on menetletud asja, milles need andmed sisalduvad. Piiratud andmeid näeb e-toimiku avaliku liidese kaudu üksnes see isik, kelle kohta need andmed on kogutud, kui nende andmete nägemise kohta ei ole ka temale piirangut seatud. Piirangu seadmine tuleb näiteks kõne alla siis, kui isiku suhtes alustatakse menetlus (või toiming), mille objektiivseks läbiviimiseks ei saa isikut sellest asjaolust teavitada (näiteks alustatakse isiku suhtes salajane pealtkuulamine).
Salastatuse astet „kinnine“ omavatel andmetel on täiendavad juurdepääsupiirangud. Neid andmeid näevad rangelt määratletud isikute ring, kes on määruses ka ära loetletud.
Asjaolud, millest tingituna on eelkõige juurdepääsupiirangu seadmine õigustatud, on loetletud punktis 5.
Eelnevalt nimetatud salastatuse astmed sisaldavad asutusekeskseid piiranguid juurdepääsuks menetlusinfole, mis on määratud klientsüsteemi äriloogikaga.

§ 17. Juurdepääs statistiliste andmete väljastamisega: Volitatud töötleja võib õigusaktides ettenähtud juhtudel väljastada e-toimiku süsteemi andmeid statistilistel eesmärkidel kasutamiseks. Andmed väljastatakse kujul, mis ei võimalda isikuid identifitseerida. Täpsema korra kehtestab justiitsminister. Samuti võib justiitsminister kehtestada määrusega statistiliste andmete töötlemise ja väljastamise tasu määrad.

5. peatükk E-toimiku süsteemi järelevalve ja turvameetmed

§ 18. Järelevalve e-toimiku süsteemi pidamise üle: Sätestab e-toimiku süsteemi üle järelevalvet pidavad isikut ning nende pädevuse. Kui Andmekaitse Inspektsiooni ning Majandus- ja Kommunikatsiooniministeeriumi poolt teostatav järelevalve on seaduses juba reguleeritud, siis siin paragrahvis on täpsustatud vastutava töötleja poolt teostatavat järelevalvet.
Kõige olulisem vastutava töötleja õigus on sätestatud lõike 4 punktis 2, mille kohaselt võib vastutav töötleja e-toimiku süsteemi kantud andmete väärkasutamise avastamisel nõuda volitatud töötlejalt või klientinfosüsteemi vastutavalt töötlejalt kasutaja juurdepääsu piiramist, peatamist või lõpetamist e-toimiku süsteemile. Väärkasutamise all on eelkõige tegu juhtumitega, kus kasutaja teeb kandeid või päringuid menetluste kohta, kus tal tööülesannete kohaselt tegelikult neid toiminguid teha ei ole õigus. Nimetatud vastutava töötleja õigus on

vajalik selleks, et välistada pärast olulise ja pideva rikkumise (või rikkumiste) avastamist edasist e-toimiku süsteemi väärkasutamist. Nagu öeldud ei saa selline meede olla tavapäraseks lahenduseks väärkasutamisele. Pigem peaks selle võimaluse kasutamist põhjalikult kaaluma ning nagu igal väärkasutamise avastamise juhul küsima ka kasutaja käest seletusi. Samas kui on tõsiseid kahtlusi kasutaja tegevuse osas ning selliseid väärkasutamise ilmingutega päringuid tuleb väga palju, siis on õigus preventatiivselt kasutusõigus peatada ning alles pärast seda seletusi küsida.

§ 19. E-toimiku süsteemi kaitse: Sätestab olulisemad põhimõtted e-toimiku süsteemi kaitsmisel. Sealhulgas on ära toodud vastavalt Vabariigi Valitsuse 20.12.2007. a määrusele nr 252 „Infosüsteemide turvameetmete süsteem“ e-toimiku süsteemi turvaklass ning klientinfosüsteemide minimaalne turvaklass. Juhul, kui e-toimiku süsteemiga hiljem liituva klientinfosüsteemi turvaklass on oluliselt erinev praegu nimetatud klientinfosüsteemi minimaalselt turvaklassist, tuleb uuesti hinnata ja ühtlustada turvaklass ning vajadusel rakendada lisameetmeid andmete käideldavuse, tervikluse ja konfidentsiaalsuse tagamiseks. Kui liituva klientinfosüsteemi turvaklass on madalam praegusest, siis tuleb kõne alla vaid selle klientinfosüsteemi turvaklassi tõstmine ning mitte olemasolevate klientinfosüsteemide turvaklasside langetamine.
Lõikes 3 on sätestatud volitatud töötleja õigus ühepoolselt piirata või peatada kasutaja juurdepääs e-toimiku süsteemile, kui on reaalne või potentsiaalne oht ohustada e-toimiku süsteemi turvalisust. Tegemist on analoogse õigusega eelmises paragrahvis sätestatuga. Seda võimalust on volitatud töötlejal eelkõige õigus kasutada siis, kui on reaalne alus eeldada, et kolmas isik on saanud juurdepääsu kasutajakontole ja selle kaudu ka e-toimiku süsteemile. Sellisele olukorrale viitaks näiteks massiliste päringute tegemine kasutaja poolt vms. Kasutaja juurdepääsu piiramisest või peatamisest peab volitatud töötleja viivitamatult teatama vastutavat töötlejat. Kooskõlas § 18 lõike 4 punktiga 2 on volitatud töötlejal õigus vastutava töötleja nõudmisel lõpetada kasutaja juurdepääs e-toimiku süsteemile. Kuna kasutusõiguste lõpetamine on väga piirav kasutaja suhtes, siis seda võib otsustada vaid vastutav töötleja.

§ 20. E-toimiku süsteemi logid ja nende hoidmine: E-toimiku süsteemi kasutamise õiguspärasust kontrollitakse tarkvaraliselt. Iga e-toimiku süsteemi tehtud päringu või kande kohta säilitatakse vähemalt kasutaja ees- ja perekonnanimi ja/või isikukood, klientinfosüsteem ning päringu või kande tegemise kuupäev ja kellaaeg. Logitud andmeid konkreetse menetluse kohta säilitatakse menetluse lõppemiseni, kui seadusest ei tulene teisiti. Muid logisid säilitatakse 3 aastat päringu või kande tegemise hetkest arvates.

6. peatükk E-toimiku süsteemi finantseerimine ja likvideerimine

§ 21. E-toimiku süsteemi finantseerimine: E-toimiku süsteemi hooldus- ja arendustöid ning pidamist finantseeritakse riigieelarvest vastutavale töötlejale selleks otstarbeks eraldatud vahenditest.

§ 22. E-toimiku süsteemi likvideerimine: E-toimiku süsteemi likvideerimise otsustab Vabariigi Valitsus. E-toimiku süsteemi likvideerimine toimub kooskõlas „Avaliku teabe seaduse“ ja „Arhiiviseaduse“ nõuetega.

7. peatükk E-toimiku avalik liides

§ 23. Sätete kohaldamine: E-toimiku avaliku liidese suhtes kohaldatakse määruses sätestatut seitsmendast peatükist tulenevate erisustega.

§ 24. E-toimiku avaliku liidese eesmärk: Sätestab e-toimiku avaliku liidese põhilised eesmärgid. Nendest punktis 1 sätestatu on kõige olulisem st avalik e-toimik on loodud just seetõttu, et võimaldada isikule juurdepääs e-toimiku süsteemile ning selles sisalduvatele andmetele tema kohta. Seda juhul kui nende andmete vaatamiseks ei ole seatud talle juurdepääsupiirangut. Tehniliselt on välistatud võimalus, et üks isik näeks teise isiku kohta e-toimikus hoitavat informatsiooni.

§ 25. Juurdepääs e-toimiku avalikule liidesele: E-toimiku avalikule liidesele pääseb ligi vaid isik, kelle isikusamasus on tuvastatud. Isiku tuvastamine toimub isikutunnistusele kantud digitaalset tuvastamist võimaldava sertifikaadi alusel või muu isiku digitaalset tuvastamist võimaldava vahendi abil. Kokkuvõtvalt on juurdepääsuks isikul vajalik ID-kaart, mis tagab vajaliku turvalisuse ja kindluse elektrooniliselt isikusamasuse tuvastamisel.

§ 26. E-toimiku avaliku liidese kaitse ja logid: Sätestab e-toimiku avaliku liidese turvaklassi. E-toimiku avaliku liidese kasutamise õiguspärasust kontrollitakse tarkvaraliselt. Iga õnnestunud või ebaõnnestunud katse kohta e-toimiku avaliku liidesesse siseneda ning e-toimiku avalikus liideses tehtud päringu või kande kohta, mida ei logita e-toimiku süsteemis, säilitatakse vähemalt kasutaja ees- ja perekonnanimi ja/või isikukood ning kuupäev ja kellaaeg. Logitud andmeid säilitatakse 3 aastat päringu või kande tegemise hetkest või sisenemiskatse toimumise hetkest arvates. Põhjus, miks siinkohal on toodud ära erinev regulatsioon §-s 20 sätestatust, seisneb pisut erinevates asjades, mida logitakse. E-toimikul ei ole vaja ning samuti ei saa logida sisenemiskatseid näiteks KRMR-i või KIS-i. Seda teevad klientinfosüsteemid ise. Kui kasutaja on juba KRMR-is, siis on talle tagatud ka ligipääs e-toimiku süsteemile. Sarnaselt teistele klientinfosüsteemidele on seetõttu ka e-toimiku avaliku liidese jaoks teistsugune logimisloogika kui e-toimiku enda jaoks. Vältimaks liigset logimist ei logi e-toimiku avalik liides neid andmeid, mida e-toimik ise juba logib.

8. peatükk Rakendussätted

§ 27. E-toimiku süsteemi andmete kandmine: Sätestab, millisest ajast arvates kantakse e-toimiku süsteemi andmed menetluste kohta. Kuna punktis 1 ja 3 nimetatud andmed on vastavalt riiklikus kriminaalmenetlusregistris ja kohtute infosüsteemis hetkel juba olemas ning need andmed kantakse üle e-toimiku süsteemi, siis on need kuupäevad ka varasemad e-toimiku süsteemi rakendamisest.

§ 28. Määruse jõustumine: Määrus jõustub 15. juulil 2008.a Samal ajal jõustuvad ka KrMS ja VTMS muudatused, mis loovad e-toimiku süsteemile õigusliku aluse.

III. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu ei ole seotud Euroopa Liidu õigusega.

IV. Määruse mõjud

E-toimiku süsteemi kasutuselevõtt võimaldab kriminaal-, tsiviil-, haldus- ja väärteomenetluse (e-toimiku süsteemi rakendamise esimeses etapis vaid kriminaal- ja väärteomenetluse osas) osapooltele operatiivse ülevaate menetluse eri etappidest, toimingutest ja tehtud otsustest. Siiani on õiguskaitseasutused hallanud oma menetlusinfot eraldi. Muudatuse tulemusena

väheneb sama informatsiooni mitmekordne sisestamine, erinevates menetlusetappides vaid lisatakse ja täiendatakse vajadusel teavet.

Praegu sisestatakse igas instantsis uuesti teatav osa kuriteo kohta käivat informatsiooni. E-toimiku rakendumisel lähevad nt politsei sisestatud e-toimikule vajalikud andmed otse e-toimikusse ning järgmine instants pääseb neile oma kasutajaliidese kaudu ligi ning saab samas teavet muuta ja täiendada.

E-toimik annab oma arengu mõnel hilisemal etapil füüsilisele ja juriidilisele isikule õiguskindluse. Ta näeb, kas tema vastu on alustatud mõni menetlus (nt trahvinõue), kuulutatud tagaotsitavaks jne. E-toimiku rakendudes kaovad kurioossed juhtumid, kus inimene saab alles pärast mitut aastat arvestatud viiviseid oma trahvidest teada või kannatab teise samanimelise isiku tagaotsitavaks kuulutamise läbi (seda muidugi juhul, kui isik läbi avaliku liidese aeg-ajalt käib kontrollimas e-toimikut või juhul kui tal on tellitud teavitamise teenus).

Kodanikuliidese (AET) kaudu on võimalik alustada koduarvutist ID-kaardi ja interneti vahendusel kohtuasja (nt taotleda lapsele elatist, esitada maksekäsu avaldus või kaevata keegi kohtusse). Selline võimalus hoiab kokku inimeste aega ning raha, sest enam ei ole vaja nimetatud toiminguteks minna kohtumajja.

E-toimikus näeb kodanik vaid neid kohtuasju, milles on ta menetlusosaline. Sisselogimine r-toimiku kodanikuportaali toimub ID-kaardi ja selle paroolide alusel, olles seega turvalisem kui laialt kasutatavad internetipanga koodikaardid (sisse logida saab vaid juhul kui on olemas ID-kaart ning teada selle paroolid; ID-kaardi kadumisel ei saa ilma paroolideta midagi teha).

Lühidalt võiks e-toimiku süsteemi mõtte sõnastada nii:

1. Õiguskindlus (inimene näeb menetlusi, kus ta on osaline);
2. Suur ajavõit (võimalus oma koduarvutist alustada kohtumenetlust, nõuda lapsele elatist jne);
3. Maksumaksja raha kokkuhoid (palju mõttetut tööd jääb ära, nt topeltsisestus);
4. Menetlusosaliste võrdne juurdepääs infole;
5. Turvaline (andmed pole pabertoimikuga riiulis, vaid paroolidega kaitstult serveris. Kodanik pääseb ligi vaid kasutades ID-kaarti ning selle paroole);
6. Asutuste töö läheb lihtsamaks (andmeid ei sisestata topelt ning kui andmed juba e-toimikus on, saab nendele samal hetkel mõnest teisest seotud infosüsteemist ligi).

V. Määruse rakendamiseks vajalikud kulutused

Vastavalt ministrite komisjonis e-toimiku süsteemiga seoses otsustatule peavad ministeeriumid tagama oma haldusalas valmisoleku ja ressursid e-toimiku süsteemi kasutuselevõtmiseks. Kuna uurimisasutused ja prokuratuur sisestavad ka praegu menetlusdokumente menetlusregistrisse, siis menetlusasutustel lisakulutusi protsessiga seoses kanda ei tule. Küll tuleb menetlusasutustel teha ühekordseid kulutusi krüptimist ja digitaalallkirjastamist võimaldava tarkvara soetamiseks. E-toimiku keskkonna ning kodanikuliidese loomist rahastatakse riigieelarvest.

E-toimiku süsteemi esimesele etapile eraldi finantsanalüüsi ei tehta, küll aga on olemas e-toimiku süsteemi täisversiooni rakendamise esialgne tasuvusanalüüs, mis on koostatud 2006.

aastal kriminaalmenetlusele tehtud kulusid arvestades. Selle analüüsi kohaselt võimaldab e-toimiku süsteemi kasutuselevõtt vähendada kriminaalmenetluse kulusid 13,5 miljoni krooni võrra aastas.

VI. Määruse jõustumine

Määrus jõustub 15. juulil 2008.a.

VII. Eelnõu kooskõlastamine

Eelnõu esitatakse e-õiguse infosüsteemi kaudu kooskõlastamiseks ministeeriumitele. Tulenevalt AvTS § 43^3 lg 3 esitatakse eelnõu kooskõlastamiseks ka Andmekaitse Inspektsioonile ja Statistikaametile.