



ANDMEKAITSE INSPEKTSIOON

AVALIKU TEABE SEADUSE ÜLDJUHEND

Kinnitatud 17. mail 2010

Muudetud ja täiendatud 08.11.2012

Täiendatud 28.02.2013

Muudetud ja täiendatud 19.05.2014, lisatud 8. ptk „Avaliku teabe masinloetav taaskasutamine“

22.10.2014 täiendatud ja muudetud §-e 3, 15, 19, 28, 45 ja 92

11.08.2015 täiendatud 7. peatükki ja lisatud 9. peatükk „Riigihangete avalikkus ja piirangud“

Märtsis 2016 täiendatud §-e 7, 9, 19, 19¹, 42, 45, 55, 71 ja 75. Täiendatud ja muudetud 8. peatükki ja lisatud peatükk 10 „Juurdepääsupiiranguga teabe kaitse“

Septembris 2016 lisatud 11. peatükk

Tallinn 2010-2016

Sisukord

Sissejuhatus.....	6
§ 1. Milleks juhend mõeldud on?.....	6
§ 2. Millele juhend tugineb?.....	6
§ 3. Mida juhend ei asenda?	6
1. Peatükk. Põhilised mõisted ja reeglid	7
§ 4. Mis on avalik teave?	7
§ 5. Kes on teabevaldaja?.....	7
§ 6. Kuidas tagatakse avaliku teabe kättesaadavus?.....	8
§ 7. Kellele antakse avalikku teavet?.....	8
§ 8. Kes on teabevaldaja juht?	8
§ 9. Kas avaliku teabe juurde pääsemiseks on eriregulatsioone?.....	9
§ 9 ¹ . Kas asutus saab esitada teabenõuet?.....	9
§ 10. Mis vahe on teabenõudel ja selgitustaotlusel?	9
§ 11. Kuidas aidata vältida teabenõude ja selgitustaotluse segiajamist?	10
§ 12. Kas üks kiri võib sisaldada nii teabenõuet kui selgitustaotlust?	10
§ 13. Kas iseenda andmete kohta saab esitada teabenõude?	10
2. peatükk. Dokumendiregistri pidamine	11
§ 14. Kuidas näidata dokumendiregistrit asutuse võrgulehel?.....	11
§ 15. Millised dokumendiliigid tuleb registrisse kanda?.....	11
§ 16. Mida arvestada muude dokumendiliikide lisamisel registrisse?.....	11
§ 17. Milliseid dokumendiliike ei pea registrisse kandma?	11
§ 18. Mida dokumendiregistri avalik vaade sisaldab?	12
§ 19. Kuidas näidata saatjat/saajat ja pealkirja registri avalikus vaates?	12
§ 19 ¹ . Kuidas võimaldada dokumendiregistri masinloetavat allalaetavust?	13
§ 20. Miks ei tohi register olla avatud otsingumootoritele?	13
§ 21. Ületekstiotsing – mida see hõlmab?	13
§ 22. Mis dokumente tuleks kokku siduda?	14
§ 23. Kui kaua peab dokumendi andmeid registris näitama?	14
§ 24. Kui kaua peab digitaalset otsejuurdepääsu võimaldama?.....	14
§ 25. Mis ajast alates peab digitaalset otsejuurdepääsu võimaldama?.....	14
3. peatükk. Teabele juurdepääsupiirangu seadmine.....	15
§ 26. Kas juurdepääsupiiranguga dokumendid tuleb registrisse kanda?.....	15
§ 27. Mida näidata piirangu kehtestamise kohta?.....	15
§ 27 ¹ . Sätted, mille alusel ei saa dokumentidele juurdepääsu piirangut kehtestada. 15	

§ 28. Sarjapiirang – millal kasutada, kuidas tähistada?	15
§ 29. Kas eraelulise teabe väljastamisel küsida puudutatud isiku arvamust?	15
§ 30. Kas inimese nimele, sünniajale ja isikukoodile saab kehtestada piirangut?	16
§ 31. Kas isiklikud kontaktandmed vajavad piirangut?	16
§ 32. Kas kinnistu aadress vajab piirangut?	16
§ 33. Mis on ärisaladus?	17
§ 34. Kellelt tuleb algatus ja otsus teabe tunnistamise kohta ärisaladuseks?	17
§ 35. Kas riigihanke pakkumus on juurdepääsupiiranguga teave?	17
§ 36. Millised kohtudokumendid on juurdepääsupiiranguga?	17
§ 37. Kuidas võib väljastada menetlusteavet ja järelevalveotsuseid?	18
§ 38. Kas juurdepääsupiirang piirab juurdepääsu tervele dokumendile?	18
§ 39. Mida panna tähele õigusakti avalikkuse piiramisel?	18
§ 40. Kui kauaks võib piirangu seada?	19
§ 41. Mida teha, kui piirang aegub?	19
§ 42. Kuidas piirangut kohaldada, kui dokument liigub ühest asutusest teise?	19
§ 43. Mida teha, kui teine asutus on unustanud juurdepääsupiirangu seada?	20
§ 44. Kas eraisikule saadetav kiri vajab piirangut?	20
4. peatükk. Kontaktteave asutuse võrgulehel	21
§ 45. Mis kontaktteavet tuleb võrgulehel avaldada?	21
§ 46. Kuhu kontaktteave paigutada?	21
§ 47. Kuidas kontaktteavet kokku lõimida?	21
§ 48. Millised on suure asutuse kontaktteabe erisused?	22
§ 49. Kuidas avaldada asutuse koosseis?	22
§ 50. Kas töötajate ja koosseisuväliste teenistujate nimesid võib avaldada?	22
§ 51. Kuidas avalikustada täitmata ametikohad?	22
§ 52. Kuidas avaldada kontaktteavet peatatud teenistussuhte korral?	22
§ 53. Kuidas avaldada ametijuhendeid?	23
§ 54. Kas ametniku kontaktandmetena peab avaldama otsekontaktid?	23
§ 55. Kuidas võimaldada kontaktteabe masinloetavat allalaetavust?	23
§ 56. Miks ei tohi kasutada menüüpunkti „Avalik teave“?	23
§ 57. Kuidas avaldada asutuse vastuvõtukorraldus?	23
§ 58. Kuidas viidata seotud asutustele?	24
5. peatükk. Asutuse personaliteabe avalikkus ja piirangud	25
§ 59. Kas asutuse personaliteave on avalik?	25
§ 60. Kas piirangu alus saab sisalduda üksnes personalikäskkirjas?	25
§ 61. Kas juurdepääsupiirang piirab juurdepääsu tervele dokumendile?	25

§ 62. Kas teenistuja nimi on juurdepääsupiirangu aluseks?	25
§ 63. Kas teenistuja tööväline kontaktteave on avalik?	25
§ 64. Kas puhkuse põhjus võib olla juurdepääsupiiranguga?	25
§ 65. Mille alusel piirata juurdepääsu terviseandmetele?.....	25
§ 66. Mida pidada silmas lähetusdokumentide puhul?	25
§ 67. Mis tähtajad kehtivad personalidokumentide juurdepääsupiirangutele?	26
6. peatükk. Asutuse palgateabe avalikkus ja piirangud.....	27
§ 68. Mis on avaliku sektori palgaandmete avalikkuse eesmärk?	27
§ 69. Millised on avaliku sektori töötasude läbipaistvuse meetmed?.....	27
§ 70. Keda puudutab korruptsioonivastase seaduse ja avaliku teenistuse seaduse alusel palgaandmete avaldamine?.....	27
§ 71. Kuidas avaldada avaliku teabe seaduse alusel palgaandmeid võrgulehel?	27
§ 72. Kas muul viisil saab palgaandmeid töötaja nõusolekuta avaldada?	28
§ 73. Kas seadusandja on soovinud avaliku sektori palgaandmete avalikkust?	28
§ 74. Milliseid palgaandmeid saab teabenõude korras küsida?	28
§ 75. Kas palgaandmete teabenõude korras küsimist saab piirata?.....	28
7. peatükk. Planeeringute avalikkus ja piirangud	30
§ 76. Miks on planeerimine avalik menetlus?	30
§ 77. Mis seadused reguleerivad planeerimise avalikkust?	30
§ 78. Millist avalikustamist näeb ette avaliku teabe seadus?	30
§ 79. Milliseid piiranguid näeb ette avaliku teabe seadus?	30
§ 80. Millise avalikustamise näeb ette planeerimisseadus?	30
§ 81. Milliseid piiranguid näeb ette planeerimisseadus?.....	31
§ 82. Kas ehitusprojekte saab küsida teabenõudega?.....	31
8. peatükk. Avaliku teabe taaskasutamine	32
§ 83. Mõisted	32
§ 83 ¹ . Millised on taaskasutamise piirangud?	32
§ 84. Milline teave kuulub piiranguteta avalikustamisele taaskasutuseks?	32
§ 84 ¹ Millisele teabe taaskasutamisele tuleb vajadusel seada piirangud?.....	33
§ 84 ² Kas dokumendiregistrid peavad olema masinloetaval kujul tervikuna allalaetavad?	33
§ 85. Kust leida tehnilisi selgitusi?.....	33
§ 86 Kellele ja kus kehtib masinloetava avalikustamise kohustus?	33
(kehtetu märts 2016).....	33
§ 87. Mis on andmekogu?.....	33
§ 88. Kas võib masinloetavana avalikustada lisa-andmeid, mida seadus ei nimeta?.....	34
§ 89. Mis on isikuandmete taaskasutamisel õiguslik alus?	34

§ 90. Kas juurdepääs isikuandmetele tuleb tagada kiirel ja hõlpsal viisil?.....	34
§ 91. Mida peaks arvestama eraelu riive mõjude hindamisel?.....	34
§ 92. Mida eraelu riive mõjude hindamise põhjal otsustada?.....	35
9. peatükk. Riigihangete avalikkus ja piirangud.....	36
§ 93. Miks peavad olema riigihanked läbipaistvad?.....	36
§ 94. Millised dokumendid on hankemenetluses piiranguga?.....	36
§ 95. Kas kvalifitseerimisdokumendid on pakkumuse osa?.....	37
§ 96. Kas riigihanke tulemusena sõlmitud lepingutele saab kehtestada juurdepääsupiirangut?.....	37
10. peatükk. Juurdepääsupiiranguga teabe kaitse.....	38
§ 97. Kas avalikku teavet, millel ei ole juurdepääsupiiranguid, peab ka kaitsma? ...	38
§ 98. Miks jagada piiranguga teavet erinevatesse järkudesse?.....	38
§ 99. Milliseid turvameetmeid peab rakendama andmekogude kaitseks?.....	39
§ 100. Millal rakendada ISO standardeid ja kas nad asendavad ISKE-t?.....	39
§ 101. Millised erinõuded kehtivad valitsusasutustele?.....	39
§ 102. Mis on kõige elementaarsemad organisatsioonilised turvameetmed?.....	40
§ 103. Mis on kõige elementaarsemad füüsilised turvameetmed?.....	40
§ 104. Mis on kõige elementaarsemad infotehnilised turvameetmed?.....	41
§ 105. Kuidas kasutada eemaldatavaid andmekandjaid?.....	41
§ 106. Kuidas edastada piiranguga teavet asutusest välja?.....	41
§ 107. Kas teisele asutusele võib anda otseligipääsu piiranguga teabe juurde?.....	42
11. peatükk. Kriminaal- ja väärteomenetluses kogutud teabe avalikustamine.....	43
§ 108. Kust tulevad piirangu alused?.....	43
§ 109. Kuidas toimub menetlusteabe teabe avalikustamine menetluse ajal?.....	43
§ 110. Mis ajani reguleerivad menetlusteabele juurdepääsu menetlusseadustikud?43	
§ 111. Kuidas toimub menetlusdokumentidele juurdepääsu võimaldamine peale menetluse lõppu?.....	43
§ 112. Kuidas avalikustada kohtuvälises menetluses tehtud väärteootsuseid?.....	43
§ 113. Kuidas avalikustada alaealise süüdlase andmeid?.....	44
§ 114. Kui pikaks ajaks saab piirangu kehtestada?.....	44
§ 115. Kellel on õigus tunnistada dokumente asutusesiseseks kasutamiseks?.....	44
§ 116. Kas kolmandatel isikutel on õigus saada juurdepääsu piiranguga teabele?..	44
§ 117. Kuidas käituda isikuandmetega?.....	44
§ 118. Millal puudub isikul juurdepääsuõigus tema andmeid sisaldavatele dokumentidele?45	

Sissejuhatus

§ 1. Milleks juhend mõeldud on?

1. Juhend on mõeldud asutustele.
2. Juhend selgitab head haldustava avaliku teabe seaduse (AvTS) täitmisel.¹
3. Eraldi juhend on koostatud avaliku teabe eraõiguslikele valdajatele (ühingud, sihtasutused, füüsilised isikud, kes täidavad avalikke ülesandeid).
4. Kriminaal- ja väärteoteabe menetlusjärgset avaldamist selgitatakse juhise 11. peatükis.

§ 2. Millele juhend tugineb?

Juhend tugineb eeskätt:

- a) [avaliku teabe seadusele](#), mille kohaselt võib Andmekaitse Inspektsioon anda soovituslikke juhiseid seaduse rakendamiseks (§ 45 lg 4);
- b) [isikuandmete kaitse seadusele](#), mis annab Andmekaitse Inspektsioonile õiguse anda soovituslikke juhiseid seaduse rakendamiseks (§ 33 lg 1 p 5);
- c) teistele asjasse puutuvatele seadustele;
- d) Vabariigi Valitsuse määrusele „[Asjaajamiskorra ühtsed alused](#)“ (AÜA);
- e) [Riigikohtu lahenditele](#);
- f) [andmekaitse direktiivile 95/46/EÜ](#), [avaliku sektori teabe taaskasutuse direktiivile 2003/98/EÜ](#) koos hilisemate muudatustega;
- g) [Euroopa andmekaitseasutuste töörühma arvamustele](#).

§ 3. Mida juhend ei asenda?

1. Juhend ei asenda asutuse asjaajamiskorda, asutuse võrgulehel avalikustatavaid isikuandmete töötlemise põhimõtteid (AÜA § 3 lg 4 ja AvTS § 28 lg 1 p 31¹) ega muid sisedokumente. Iga asutus peab oma reeglid ise paika panema: kes, millal ja millise juurdepääsupiirangu märke teeb; kuidas piiranguid pikendatakse; kaua logifaile säilitatakse jne.
2. Kindlasti tuleb asutuse sisedokumentides sätestada üksuste ja teenistujate kohustused ja vastutus avaliku teabe seaduse rakendamise eest ning tagada üldine majasisene koordineerimine.
3. Valitsusasutused on kohustatud selleks määrama isiku, kes korraldab asutuses dokumentide avalikustamist ja neis sisalduvate isikuandmete kaitset (AÜA § 3 lg 3). Kohalikes omavalitsustes on selliseks isikuks valla- või linnasekretär (kohaliku omavalitsuse korralduse seadus § 55 lg 4 p 3-4).

¹ Palume siin ja edaspidi meeles pidada, et Riigi Teataja lingid avavad kehtiva tervikteksti viimase sõnastuse.

1. Peatükk. Põhilised mõisted ja reeglid

§ 4. Mis on avalik teave?

1. Põhiseadus annab õiguse küsida asutustelt teavet nende tegevuse kohta.²
2. Selle tagamiseks vastu võetud avaliku teabe seadus peab avalikuks teabeks mistahes viisil mistahes teabekandjale jäädvustatud ja dokumenteeritud teavet, mis on saadud või loodud avalikke ülesandeid täites (AvTS § 3 lg 1). Seega on avalikuks teabeks kogu avaliku sektori valduses olev teave, olenemata sellest, kas teavet tuleb dokumendiregistris registreerida või mitte.

Näiteks on ka raamatupidamise dokumendid avalikuks teabeks, kuigi neid dokumendiregistris registreerima ei pea.

3. Avaliku teabe kättesaadavus avaldab kasulikku mõju:
 - a) ühiskonna tasandil, aidates muuta avaliku võimu teostamist, avalike teenuste osutamist ja eelarveraha kasutamist võimalikult läbipaistvaks;
 - b) üksikisiku tasandil, tagades isiku pääsu talle vajaliku teabe juurde.
4. Avalikku teavet võib teisisõnu nimetada avaliku sektori teabeks.³ See ongi täpsem mõiste, sest avalik teave ei ole alati avalik (osalt kehtivad juurdepääsupiirangud). Küll aga on kogu avalik teave seotud avaliku sektoriga (avaliku võimuga, avalike teenustega, eelarveraha kasutamisega). Avaliku teabe vastand ei ole seega mitteavalik teave, vaid erateave – eraettevõtetele, eraühingutele, eraisikutele kuuluv teave.
5. Avalik teave ei kätke mitte üksnes dokumente/teavet, mis on loodud asutuses või tekib asutuste vahelises suhtluses. Erasisiku kiri asutusele ja asutuse kiri eraisikule on samuti asutuses talletatud avalik teave, kuigi eraelu kaitseks võib sellele kehtida juurdepääsupiirang (vt AvTS-i § 35 lg 1 p 11–15).

§ 5. Kes on teabevaldaja?

1. Teabevaldajaiks (avaliku teabe valdajaiks) on:
 - a) kõik riigi- ja omavalitsusasutused – kogu tegevuse ulatuses,⁴
 - b) kõik avalik-õiguslikud juriidilised isikud – kogu tegevuse ulatuses,
 - c) ühingud, sihtasutused ja füüsilised isikud, kes õigusakti või halduslepingu alusel täidavad avalikke ülesandeid (nt hariduse, tervishoiu vms alal) – avalike ülesannete täitmise alase teabe suhtes.⁵
2. Teabenõudele vastamise kohustuse poolest on teabevaldajaga võrdsustatud (kuigi nad ei ole avaliku teabe valdajad ja neil ei ole veebilehe pidamise kohustust):
 - a) ettevõtjad, kellel on turul valitsev seisund, eri-, ainuõigus või monopol – teabe suhtes, mis puudutab kaupade/teenuste pakkumise tingimusi, hindu ja nende muudatusi;
 - b) ettevõtjad, ühingud, sihtasutused – teabe suhtes, mis puudutab riigi või omavalitsuse eelarvest avalike ülesannete täitmiseks saadud või toetusena antud vahendite kasutamist (AvTS-i § 5, võrgulehe pidamise osas vt § 31).

² [Põhiseaduse](#) § 44 lg 2: „Kõik riigiasutused, kohalikud omavalitsused ja nende ametiisikud on kohustatud seaduses sätestatud korras andma Eesti kodanikule tema nõudel informatsiooni oma tegevuse kohta, välja arvatud andmed, mille väljaandmine on seadusega keelatud, ja eranditult asutusesiseseks kasutamiseks mõeldud andmed.“ Sama paragrahvi lõike 4 kohaselt on sama õigus ka välismaalastel ja kodakondsusetuil, kui seadus ei sätesta teisiti; § 9 lg 2 kohaselt on seda võimalik laiendada ka juriidilistele isikutele.

³ Euroopa Liidu õiguses kasutataksegi *avaliku sektori teabe* mõistet: vt [avaliku sektori valduses oleva teabe taaskasutuse direktiivi 2003/98/EÜ](#). Seevastu Euroopa Nõukogu eelistab *ametlike dokumentide* mõistet: vt nt [2009. a ametlikele dokumentidele juurdepääsu Euroopa Nõukogu konventsiooni](#).

⁴ Teabevaldjaks on ka hallatavad asutused.

⁵ Siinne juhend on mõeldud asutustele. Eraõiguslikele teabevaldajatele ei kehti mitmed asutusest teabevaldaja kohustused, eeskätt võrgulehe pidamine.

§ 6. Kuidas tagatakse avaliku teabe kättesaadavus?

1. Selleks et osata teavet küsida, on vaja teada, mis teavet teabevaldajal üldse on. Sestap on olulised tööriistad, mis tagavad juurdepääsu avalikule teabele:

- a) asutuse dokumendiregister,
- b) asutuse võrguleht,⁶
- c) Eesti teabevärv www.eesti.ee, mis koondab kogu avaliku sektori võrguteavet.

2. Avaliku teabe juurde pääsemiseks näeb AvTS ette neli põhilist teed:

- a) teabenõudja esitab teabevaldajale teabenõude,
- b) digitaaldokumentide „klõpsatav“ otselõigipääs võrgupõhise dokumendiregistri kaudu,
- c) teabevaldaja avalikustab ise teavet oma võrgulehe ja Eesti teabevärava kaudu,
- d) erakorralisi asjaolusid (oht elule, tervisele, varale, keskkonnale), samuti teavet avalikku huvi pakkuvate sündmuste ja faktide kohta avalikustab teabevaldaja ise.

Esimesel juhul on tegu **passiivse avalikustamisega**: teavet antakse, kui seda nõutakse. Teistel juhtudel on tegu **aktiivse avalikustamisega**: teabevaldaja pakub ise teavet või teeb selle kättesaadavaks (vrd AvTS-i § 8).

3. Teabenõuet saab esitada:

- a) suuliselt, pöördudes teabevaldaja poole vahetult või telefoni teel (AvTS § 13 lg 1);
- b) kirjalikult, andes teabenõude üle isiklikult või edastades selle post, faksi või e-postiga (AvTS § 13 lg 2);

Kuna teabenõuetele ja selgitustaotlustele konkreetseid vorminõudeid sätestatud ei ole, siis tuleb asutustel arvestada asjaoluga, et teabenõudeid ja selgitustaotlusi on võimalik esitada ka suhtlusvõrgustike (ühismeedia) kaudu, seda muidugi eeldusel, et asutusel on seal kasutajakonto.

§ 7. Kellele antakse avalikku teavet?

1. Põhiseaduse kohaselt on õigus avalikku teavet saada (st olla teabenõudjaks) Eesti kodanikel ja – kui seadus ei sätesta teisiti – ka välismaalastel ja kodakondsusetuil (§ 44 lg 2 ja 4).

2. Tegelikult on seadusandja selle õiguse andnud igale füüsilisele ja juriidilisele isikule (AvTS-i § 7). Seega on välismaalasel, kodakondsusetul ja juriidilisel isikul avaliku teabe saamisel samad õigused mis Eesti kodanikul.

3. Avaliku teabe saamisel AvTS-i alusel ei pea keegi põhjendama, miks ta seda teavet vajab või mis ta sellega teha tahab. Ühelgi teabenõudjal – sh ajakirjanikul ja advokaadil – ei ole juurdepääsupiiranguta avaliku teabe saamisel teistest suuremaid või väiksemaid õigusi.

4. Isikute erinev kohtlemine ja nõue teabe vajalikkust põhjendada on võimalik vaid piiranguga avaliku teabe saamisel: juurdepääsu võimaldamisel ametialaseks kasutamiseks või õigustatud huvi alusel (vrd AvTS-i § 14 lg 2, § 38 ja 39).

5. Küll aga peab teabenõudja, kui ta taotleb teabele juurdepääsu taaskasutamise eesmärgil, teavitama sellest teabevaldajat. See võimaldab teabevaldajal hinnata teabe üldisele kasutamise piirangute kehtestamise vajadust ning otsustada, kas anda taotletud teave üldiseks kasutamiseks tingimusteta või seda selle üldisele kasutamisele tingimusi litsentside abil (AvTS § 14 lg 21).

§ 8. Kes on teabevaldaja juht?

1. Teabevaldaja juht täidab mitmeid AvTS-is ette nähtud ülesandeid, näiteks:

- a) vastutab teabe passiivse ja aktiivse avalikustamise korraldamise eest, määrates vajadusel vastutajad ja kehtestades töökorraldusreeglid (AvTS-i § 10);
- b) kehtestab juurdepääsupiirangud (AvTS-i § 34 lg 2, § 35, § 41 lg 1 ja 1¹);
- c) lubab erandkorras juurdepääsu juurdepääsupiiranguga teabele (AvTS-i § 38 lg 4).

⁶ AvTS kasutab sõna *veebileht*. Üldkeeles kasutatakse selle vastena ka sõna *koduleht*. Korrektne on rääkida *võrgupaigast* ehk *võrgukohast* (*veebisaidist*). Võrgupaik koosneb eri aadressilaienditega lehtedest. Nii on eraldi lehtedel avaleht, kontaktteave, dokumendiregister jne. Koduleht on tegelikult leht, kuhu võrgulehitseja (veebibrauser) internetikasutaja võrku avades vaikimisi suunab (see ei pea olema asutuse enda võrgupaik). Kuna aga *leht* on meie õiguskeeles võrgupaiga tähenduses paraku võrdlemisi levinud, kasutatakse juhendis sõna *võrguleht*.

2. Kõik need ülesanded on asutuse asjaajamise osa. Kui seadusega on ette nähtud ametiisik, kes juhib asutuse ajaajamist, siis on tema AvTS-i mõttes teabevaldaja juht, näiteks:

- a) ministeeriumis kantsler, ⁷
- b) valla-, linna- ja maavalitsuses valla-, linna- ja maasekretär, ⁸
- c) kohtus kohtudirektor. ⁹

§ 9. Kas avaliku teabe juurde pääsemiseks on eriregulatsioone?

1. Kohtu-, haldus- jm menetluste läbiviimise, andmekogude pidamise ja asutuste tegevuse kohta on palju seadusi. Ka need võivad reguleerida teabe avalikustamist ja teabe küsimist.

2. Kuigi iseenesest võib tegu olla avaliku teabega, kohaldatakse üldseaduse (AvTS) ja eriseaduse vastuolu korral eriseadust (AvTS-i § 2 lg 1 p 2, lg 2).¹⁰

3. Eriseadused võivad teha teabe kättesaadavaks üksnes piiratud isikute ringile (nt menetlusosalistele) ning nõuda, et teabe küsija peab põhjendama oma õigustatud huvi teabe saamiseks. Samuti võivad eriseadused esitada AvTS-ist erinevaid vorminõudeid teabe küsimisele, kehtestada erinevaid tähtaegu teabe väljastamisele ning sätestada tasu teabe väljastamise eest.

§ 9¹. Kas asutus saab esitada teabenõuet?

AvTS § 14 lg 1 p 2 ja § 25 lg-st tulenevalt on õigus teabenõuet esitada ka asutustel. Samas on Riigikohus mitmel korral leidnud, et avaliku sektori asutus ei saa olla põhiõiguste kandja.¹¹ Reeglina küsivad asutused aga teavet oma ülesannete täitmiseks, millisel juhul tuleb teabe saamise õigus mingist eriseadusest, mitte avaliku teabe seadusest.

Näitena võib tuua volikogu liikme õigust saada teavet, mis tuleneb KOKS §-st 26. Kui isik küsib omavalitsuselt teavet sama omavalitsuse volikogu liikmena, ei saa seda käsitleda teabenõudena AvTS-i mõistes. Sellistele juhtudele AvTS ei laiene. Sellisel juhul on tegemist omavalitsuse sisesuhtega, mis tuleb lahendada kohaliku omavalitsuse siseselt. Sellisele seisukohale on asunud Riigikohus lahendis [3-3-1-55-04](#).

Samuti on Riigikohus haldusasjas nr [3-3-1-19-14](#) asunud seisukohale, et avaliku ülesande üleandmisega kaasnevates halduslepingulistest suhetes, mille raames on omavalitsusüksusel avalikule teabele juurdepääsuks halduskoostöö seadusest (HKTS) tulenevad eriõigused, ei saa kohalikku omavalitsusüksust käsitada "iga isikuna" AvTS § 7 mõttes ning nende õigus küsida teavet tuleneb mitte AvTS-st, vaid halduskoostöö seadusest ([HKTS § 18 lg 1 p-d 2 ja 3](#)).

§ 10. Mis vahe on teabenõudel ja selgitustaotlusel?

1. Mitte iga kiri asutusele ei ole teabenõue. Teabenõue puudutab asutuses olemas oleva dokumendi või muu teabe (nii paberil kui digitaalkujul) väljastamist. Teabenõudega võib välja küsida näiteks terve dokumendi sisu või ka üksnes selle väljavõtteid. Samuti näiteks väljavõtteid mingist andmekogust või andmestikust. Seda eeldusel, et vastamiseks ei tule luua uut teabe sisu – sh teha uusi arvutusi.

11. Teabenõudena tuleb ka käsitleda isikute pöördumist, milles soovitakse saada teavet mingi dokumendi olemasolu või selle puudumise kohta, millele on võimalik vastata „jah“ või „ei“ vormis.

2. Aga kui vastamiseks tuleb dokument/teave alles luua? Näiteks küsitakse asutuse seisukohta, hinnangut, kokkuvõtet, palutakse sekkuda, juhitakse tähelepanu puudustele vms. Sellisel juhul on tegu selgitustaotluse või märgukirjaga. Neile vastatakse märgukirjale ja selgitustaotlusele vastamise ning kollektiivse pöördumise seaduse alusel. Samuti võib tegu olla avalduse, kaebuse ja vaidega.

⁷ [Vabariigi Valitsuse seaduse § 53 lg 1](#)

⁸ [Kohaliku omavalitsuse korralduse seaduse § 55 lg 4](#), [Vabariigi Valitsuse seaduse § 91](#). Valla-, linna- ja maasekretäri puhul ei ole küll erinevalt ministeeriumi kantslerist selgesõnalist normi asjaajamise juhtimise kohta, see tuleneb kõigi ülesannete koosmõjust.

⁹ [Kohtute seaduse § 125 lg 1](#), eriti p 1.

¹⁰ Seda õiguspõhimõtet tähistatakse väljendiga *Lex specialis derogat legi generali*.

¹¹ RK nr 3-3-1-19-14 p 25

3. Teabenõudele vastatakse 5 tööpäeva jooksul, märgukirjale ja selgitustaotlusele 30 päeva jooksul.¹² Kui on ilmne, et inimene käsitleb oma märgukirja/selgitustaotlust ekslikult teabenõudena ja ootab sellele vastust 5 tööpäeva jooksul, on heaks tavaks talle 5 tööpäeva jooksul teada anda, et tema kirja käsitletakse märgukirjana/selgitustaotlusena. Automaatvastust kirja kätte saamise kohta ei saa käsitleda kodanikule vastamisena.

§ 11. Kuidas aidata vältida teabenõude ja selgitustaotluse segiajamist?

1. Järjest rohkem teabenõudeid esitatakse asutuse võrgulehe kaudu. Sellepärast on soovitatav lisada teabenõude esitamise vormi juurde lihtne ja arusaadav selgitus, näiteks selline:

„Palume tähele panna, et mitte iga pöördumine ei ole teabenõue. Teabenõudega küsitakse asutuses juba olemas olevat teavet (nt dokumenti või väljavõtet). Teabenõudele vastatakse 5 tööpäeva jooksul. Kui küsite asutuse hinnangut või nõu, juhite tähelepanu puudustele või soovite mingi toimingut tegemist, siis see ei ole teabenõue. Sel juhul on vastamise tähtaeg pikem.“

2. Digitaalselt saabunud pöördumisele on soovitatav saata ka automaateavitus dokumendi kätte saamise kohta. See välistab kodanike täiendavad pöördumised/küsimused dokumendi kohale jõudmise kohta.

3. Eriti soovitatav on infotehniline lahendus, mis võimaldab pöördumise esitajale teatada tema asjaajamisnumbri, millega isik saab oma menetluskäiku dokumendiregistris või muus menetlusregistris ise jälgida.

§ 12. Kas üks kiri võib sisaldada nii teabenõuet kui selgitustaotlust?

1. Kiri võib korruga sisaldada nii teabenõuet kui selgitustaotlust.

2. Sellisel juhul tuleb kohaldada mõlemat seadust. Teabenõue täidetakse AvTS-i alusel 5 tööpäeva jooksul ning selgitustaotlusele vastatakse märgukirjale ja selgitustaotlusele vastamise ning kollektiivse pöördumise esitamise seaduse alusel 30 kalendripäeva jooksul.

§ 13. Kas iseenda andmete kohta saab esitada teabenõude?

1. Isikuandmete kaitse seaduse §-s 19 ettenähtud õigus küsida iseenda kohta kogutud andmeid tuleb põhiseadusest (§ 44 lg-st 3) ja Euroopa Liidu andmekaitse direktiivist.¹³

2. Kuid see õigus on laiem kui AvTS-i kohaldamisala. Õigus küsida iseenda kohta kogutud andmeid hõlmab nii avalikku sektorit (siis küsitakse avalikku teavet) kui ka äri- ja mittetulundussektorit.

3. Olemuselt on isikuandmete kaitse seaduse §-s 19 nimetatud päring tööpoolest teabenõue, või vähemalt sellega väga sarnane.¹⁴ Ka reeglid on sarnased (vastamistähtaeg 5 tööpäeva, paberdokumendi väljastamisel võib võtta paljundustasu kuni 0,19 eurot lehekülje eest alates 21. leheküljest – vt viidatud paragrahvi lõiked 3 ja 4).

4. Kui iseenda kohta kogutud teave on avalik teave, siis saab teabevaldaja kohaldada ka AvTS-i sätet vastamistähtaaja pikendamise kohta 15 tööpäevani (AvTS § 19). Erandina on Politsei- ja Piirivalveametil sellisele päringule vastamiseks aega 30 päeva (politsei ja piirivalveseaduse § 7⁴⁸).

5. Sellise teabenõude puhul ei kehti AvTS-is ette nähtud juurdepääsupiirangud. Aluseid keeldumaks inimesele tema enda kohta kogutud andmete väljastamast on märksa vähem ning need tulenevad üksnes [isikuandmete kaitse seaduse](#) §-st 20.¹⁵

¹² Teabenõudele vastamist võib pikendada kuni 15 tööpäevani, sellest teatatakse 5 tööpäeva jooksul (AvTS § 19). Märgukirjale ja selgitustaotlusele vastamist võib pikendada kuni 2 kuuni ([märgukirjale ja selgitustaotlusele vastamise ning kollektiivse pöördumise esitamise seaduse](#) (§ 6)).

¹³ [Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta](#), vt art 12.

¹⁴ Sellele viitab ka AvTS-i § 14 lg 2.

¹⁵ Nõue tuvastada päringu esitaja isik on elementaarne nii avaliku kui erateabe puhul. Avaliku teabe puhul on see selgesti nimetatud AvTS-i § 14 lg-s 2.

2. peatükk. Dokumendiregistri pidamine

§ 14. Kuidas näidata dokumendiregistrit asutuse võrgulehel?

1. Dokumendiregister on võrgulehe vaadatavamaid osi.¹⁶ See on oluline töövahend tagamaks asutuse tegevuse avalikkust ja ligipääsu avaliku teabe juurde. Soovitav on kuvada register võrgulehe sisukorras esimesel valikutasandil (nn ühe-klõpsu-reegel registri juurde jõudmiseks).
2. Jaotise tähistus peab olema „Dokumendiregister“. Muud tähistused tekitavad segadust, nt tarkvaralahenduse nimi: „Amphora“, „Postipoiss“ vms. Inimesed ei leia sel juhul otsitavat üles.
3. Vajadusel võivad asutused pidada ka ühist dokumendiregistrit (asjaajamiskorra ühtsete aluste § 21 lg 3). Sellisel juhul peab iga asutuse võrguleht sisaldama linki dokumendiregistrile.

§ 15. Millised dokumendiliigid tuleb registrisse kanda?

1. Dokumendiregistrisse kannab asutus andmed dokumentide kohta, mis on loodud või saadud asutuse tegevuse käigus.
2. AvTS annab registrisse kantavate dokumendiliikide minimaalloetelu:
 - a) saabunud ja väljasaadetud dokumendid sh teabenõuded, kui neid ei täideta koheselt (AvTS-i § 12 lg 1 p 1, vt ka AÜA § 28, AvTS § 16 lg 1),
 - b) õigusaktid, sh käskkirjad jm üksikaktid (AvTS-i § 12 lg 1 p 2, vt ka AÜA § 25 ja haldusmenetluse seaduse § 51),
 - c) lepingud (AvTS-i § 12 lg 1 p 3, vt ka AÜA § 27).
3. „Asjaajamiskorra ühtsed alused“ täiendavad seda loetelu, võimaldades ühtlasi asutuse oma asjaajamiskorraga ette näha ka muude dokumendiliikide kandmise dokumendiregistrisse (AÜA § 18).¹⁷
4. Kui mingit liiki dokumendid, mida seadus kohustab dokumendiregistri avalikus vaates näitama, registreeritakse muus andmekogus või infosüsteemis (näiteks personalikäskkirjad), siis tuleb dokumendiregistri juures selgitada, kus ja kuidas on võimalik nende dokumentidega tutvuda ja lisada link vastavale infosüsteemile või andmekogule, kus nende dokumentidega on võimalik tutvuda (AvTS § 29 lg 1).¹⁸

§ 16. Mida arvestada muude dokumendiliikide lisamisel registrisse?

[Kehtetu alates 19.05.2014]

§ 17. Milliseid dokumendiliike ei pea registrisse kandma?

Asutuse avalikku dokumendiregistrisse ei pea kandma:

- a) asutuses edastatud arvamusi, teateid, memosid, õiendeid, nõuandeid jms, mida asutuse juhi otsusel ei ole vaja dokumendiregistrisse kanda (AvTS-i § 35 lg 2 p 3);
- b) raamatupidamisdokumente (AvTS-i § 12 lg 2);¹⁹
- c) riigisaladust ja salastatud välisteavet sisaldavaid dokumente (AvTS-i § 2 lg 2 p 1);
- d) sissetulevaid dokumente, mida vastuvõttev asutus võtab arvele eriseadusega ette nähtud korras ja millele on isiku juurdepääs tagatud (AvTS § 12 lg 21).

Näiteks võib tuua kohtule esitatud menetlusdokumente, mis võetakse arvele kohtuinfosüsteemis või registri-, kinnistus- või laevakinnistuspäevikus.²⁰ Antud näide käib üksnes kohtuasutuse kohta ega

¹⁶ Dokumendiregistri asutuse võrgulehele paigutamise kohustus tuleneb AvTS § 28 lg 1 punktist 31.

¹⁷ AÜA § 18 nimetab täiendavate dokumendiliikidena asutuses koostatud protokolle ja akte, suulisi teabenõudeid (kui neid ei täidetud koheselt), samuti allasutuse/üksuse/töötaja esitatud aruandeid jm dokumente, mille esitamine tuleneb seadusest või on vajalik menetluses oleva asja lahendamiseks.

¹⁸ Asutused, kes on liitunud Riigi Tugiteenuste Keskuse riigitöötajate iseteenindusportaaliga ning kelle puhkuse ja lähetuse käskkirjad avalikustatakse Riigi Tugiteenuste Keskuse [riigitöötajate puhkuste ja lähetuste kinnitusdokumentide registris](#), peavad oma asutuse dokumendiregistri juurde lisama lingi eelnimetatud registrile, mille kaudu lähetuse ja puhkuse käskkirjad on leitavad.

¹⁹ [Raamatupidamise seaduse](#) § 7 (raamatupidamise algdokument, algdokumentide põhjal koostatud koondokument, raamatupidamisõiend) jms

puuduta dokumente saatvat asutust – tema peab väljasaadetud dokumendid ikka oma dokumendiregistrisse kandma.

e) tellimata saadetud reklaami, sest see ei ole avalik teave (asutus ei võta seda vastu avalike ülesannete täitjana, AvTS-i § 3 lg 1).

§ 18. Mida dokumendiregistri avalik vaade sisaldab?

1. Asutuse võrgulehel peab olema ligipääs dokumendiregistri avalikule vaatele koos sisujuhi (dokumendiliikide loetelu), kasutusjuhendi ja ületekstiotsinguga (vt AvTS-i § 12 lg 5).
2. Dokumendiregistri avalikus vaates kuvatakse vähemalt järgmised üldandmed dokumendi kohta (vt AvTS-i § 12 lg 3):
 - a) dokumendi saatja/saaja;
 - b) dokumendi vastuvõtmise/väljasaatmise kuupäev;
 - c) mil viisil dokument tuli/läks (faksi, posti, e-posti või käsipostiga jne);
 - d) dokumendi rekvisiidid:
 - i. dokumendi pealkiri või lühikokkuvõte,
 - ii. koostamise/kinnitamise kuupäev ja vajadusel kellaaeg,
 - iii. dokumendi viit (ehk asjaajamisnumber: asutuse enda ja kui teada, siis ka kirjavahetuspartneri oma);
 - e) dokumendi liik (avaldus, märgukiri, teabenõue, selgitustaotlus vms);
 - f) dokumendi juurdepääsupiirangud (nende kohta vt lähemalt selle juhendi 3. ptk) sh ka piirangute alused ja aeg (AÜA § 23 lg 3).
3. Saabunud ning lahendamist ja vastamist vajavate dokumentide kohta märgitakse ka lahendamise/vastamise tähtaeg, menetleva üksuse ja teenistuja nimi.

§ 19. Kuidas näidata saatjat/saajat ja pealkirja registri avalikus vaates?

1. Kas dokumendi saatjat/saajat tuleks dokumendiregistri avalikus vaates näidata nimeliselt, initsiaalidega või „eraisikuna“? Kui täpne peaks olema dokumendi pealkiri või lühikokkuvõte? Senine praktika on kirev ning mõnikord selges vastuolus seaduse eesmärgiga.
 - 1¹. Alates 16.01.2016 on seadusandja kehtestanud selge keelu, et kui dokumendi saaja/saatja on füüsiline isik, siis ei tohi dokumendiregistri avalikus vaates avalikustada teavet, mis võimaldab füüsilist isikut tuvastada (AvTS § 12 lg 3¹). Eeltoodu tähendab seda, et dokumendiregistri avalikus vaates ei tohi kajastada füüsiliste isikute nimesid, aadresse ega muid füüsiliste isikute otsest tuvastamist võimaldavaid andmeid. Seda nii kirja saaja/saatja andmetes kui ka dokumendi pealkirjades.
 2. (Kehtetu alates 22.10.2014)
 3. (Kehtetu alates 22.10.2014)
 4. (Kehtetu alates 22.10.2014)
 5. (Kehtetu alates 22.10.2014)
 6. (Kehtetu alates 22.10.2014)
 - 6¹ (Kehtetu alates 16.01.2016)
 - 6². (Kehtetu alates 16.01.2016.)
 - 6³. Et dokumendiregister täidaks oma eesmärgi ka initsiaalide või „Eraisik“ kasutamise korral ja füüsilistel isikutel oleks võimalik oma dokumentide liikumist ja menetlusi jälgida, soovitame dokumendi saabumisel saata kodanikule automaatvastus kirja registreerimise kohta koos registreerimisnumbriga, mille kaudu on võimalik menetlust jälgida.
7. Samuti tuleks eraelu kaitse huvides asutuse asjaajamises hoiduda väikesemahuliste, kuid tundliku sisuga sarjade moodustamisest.
8. Ka asutustevahelise kirjavahetuse puhul tuleb vältida saaja/saatjana füüsilise isiku nime kajastamist dokumendiregistri metaandmetes ning kasutada saaja/saatja andmetena asutuse nime.

20 Vt [kohtute seaduse](#) § 8² lg 2, [äriregistri seaduse](#) § 40, [mittetulundusühingute seaduse](#) § 87, [kommertspandiseaduse](#) § 15 lg 1 ja 16 lg 4-4², [kinnistusraamatuseaduse](#) §-d 19, 39, [laeva lipuõiguse ja laevaregistrite seaduse](#) § 37 lg 2 ja 74.

§ 19¹. Kuidas võimaldada dokumendiregistri masinloetavat allalaetavust?

1. Dokumendiregister on samuti selle teabe hulgas, mis tuleb võimalusel avalikustada masinloetaval kujul ja avatud vormingus (AvTS § 31 lg 4 ja § 29 lg 4), mida on pikemalt selgitatud käesoleva juhise §-s 84¹.
2. Dokumendiregistrit, erinevalt teistest andmekogudest, ei pea aga saama alla laadida tervikliku andmekogumina koos metaandmetega.
3. Digitaalne dokumendiregister ongi masinloetav - metaandmed ja digitaalsed dokumendid (nt doc või pdf formaadis) on ka masinloetavad andmed. Masinloetavad ei ole üksnes paberdokumendid.
4. Dokumendiregistrid sisaldavad hulgaliselt juurdepääsupiiranguga teavet ning juurdepääsupiiranguta isikuandmeid. Seetõttu tuleb rakendada käesoleva juhise §-s 20 nimetatud kaitsemeetmeid.

§ 20. Miks ei tohi register olla avatud otsingumootoritele?

1. Avalike otsingumootorite ([Neti](#), [Google](#), [Yahoo](#), [Ixquick](#) jne) abil otsitakse sisestatud nime vms alusel materjale üle kogu interneti, sh asutuse dokumendiregistritest, kui need ei ole otsingumootoritele suletud.
2. Kui inimese igast kontaktist asutustega jääb dokumendiregistri kaudu nimeline avalik jälg internetti, on inimene otsingumootoreid kasutades väga lihtsalt profileeritav. Kogumis võib see oluliselt kahjustada eraelu puutumatust (AvTS-i § 35 lg 1 p 12). See võib inimeses tekitada hirmu avaliku võimuga suhtlemisel.²¹
3. Asutuse dokumendiregister ja eriti dokumendiregistri otselgipäas digitaaldokumentide sisusse tuleb avalikele otsingumootoritele sulgeda. Selleks varustatakse suletav osa näiteks failiga robots.txt või HTML <META> TAG-iga.²²
4. Tegelikult on ka neil sulgemisabinöüdel üksnes piiratud mõju. Enam levinud otsingumootorid tunnustavad võrgulehe valdaja sulgemissoovi viisakusest, hea tahtena. Andmesideteenuste turg areneb aga kiiresti. Alati võib turule tulla vähem viisakaid tegijaid (eriti väljaspool Eestit ja Euroopat) ning viisakas tegija muutuda ebaviisakamaks. Seetõttu ei võta dokumendiregistri otsingumootoritele sulgemine ära vajadust olla tähelepanelik dokumendi pealkirja, saatja/saaja nime ja sarja nimetuse kombinatsiooni suhtes.
5. Erasisikute otse või kaudset äratundmist võimaldava ning tundlikuma sisuga dokumendiregistri sarjade suhtes võiks rakendada ka robotitõket, mis eristab inim- ja automaatpäringuid ning hoiab seega infot masinloetava allalaetavuse eest.²³

§ 21. Ületekstiotsing – mida see hõlmab?

1. Dokumendiregistri ületekstiotsing võib sisaldada täpsustava valiku võimalusi (piirates otsitavat näiteks ajavahemike, dokumendiliikide jms tunnuste abil).
2. Igal juhul peab olema võimalik teha otsingut, mis hõlmab tervet registri avaliku vaate üldandmestikku (vt juhendi § 18 punkti 2) ühekorraga. See peab hõlmama andmestikku vähemalt alates 01.01.2009 (siis jõustus ületekstiotsingu nõue).
3. Otsing Ctrl+F klahvidega ei ole ületekstiotsing AvTS-i mõttes. See ei võimalda korraga otsida eri lehekülgedelt ega mitme parameetri alusel.

21 Ivo Pilving leiab artiklis „Õigus isikuandmete kaitsele“ (Juridica, VIII 2005, lk 532–536), et ühegi erasisiku nime ei tohiks asutuse dokumendiregistris ilma ülekaaluka avaliku huvita avaldada, kuna see võib võtta julguse asutuste poole pöörduda ja pärsib nõnda põhiseaduse §-ga 46 tagatud avalduste esitamise õiguse kasutamist. Seisukohta, et isikuandmete dokumendiregistris avaldamine põhjustab ametiasutusse pöördumise ees hirmu, jagab Liina Kanger artiklis „Kas avalik dokumendiregister või isikuandmete kaitse?“ (Juridica, I 2009, lk 39-46).

22 Vt nt <http://www.robotstxt.org>.

23 Tuntud mõistena CAPTCHA – lühend väljendist *Completely Automated Public Turing test to tell Computers and Humans Apart*.

4. Ületekstiotsing otsib dokumendiregistri avalikust vaatest, mitte dokumentide sisust (vrd AvTS-i § 12 lõikeid 5 ja 3). Vastasel juhul tekib risk, et juurdepääsupiiranguga dokumentide sisu lekib. Samuti võib see oluliselt kahjustada eraelu puutumatust avalikke otsingumootoreid (Neti, Google, Yahoo, Ixquick jne) ning profileerimist arvestades (vt juhendi § 20).

§ 22. Mis dokumente tuleks kokku siduda?

On kasutajasõbralik siduda (linkida) ühe menetlusega või muidu loogiliselt seotud dokumendid (nt selgitustaotlus ja vastus) dokumendiregistri avalikus vaates kokku. Seega kuvatakse dokumendi juures ka seotud dokumentide lingid.

§ 23. Kui kaua peab dokumendi andmeid registris näitama?

1. Dokumente peab registris näitama sama kaua, kui kestab nende säilitustähtaeg. Digitaaldokumentidel on paberdokumentidest erinev säilitustähtaeg üksnes juhul, kui nii on selgesti sätestatud.

2. Säilitustähtajast lühem näitamisaeg kitsendab lubamatult isikute teabeõigust (põhiseaduse § 44 lg 2). Pikem aeg võib aga isikuandmete suhtes olla vastuolus eesmärgikohasuse põhimõttega ([isikuandmete kaitse seaduse](#) § 6 p 2).

§ 24. Kui kaua peab digitaalset otsejuurdepääsu võimaldama?

1. Ka otseligipääs juurdepääsupiiranguta digitaaldokumentidele dokumendiregistri kaudu peab toimima sama kaua, kui kestab dokumendi säilitustähtaeg.

2. Säilitustähtajast lühem otsejuurdepääsu aeg kitsendab lubamatult isikute teabeõigust. Pikem aeg võib aga isikuandmete suhtes olla vastuolus eesmärgikohasuse põhimõttega ([isikuandmete kaitse seaduse](#) § 6 p 2).

§ 25. Mis ajast alates peab digitaalset otsejuurdepääsu võimaldama?

Otselgipääsu dokumendiregistri kaudu ei pea võimaldama enne 01.01.2009 dokumendiregistrisse kantud juurdepääsupiiranguta digitaaldokumentidele, sest otseligipääsu nõue jõustus alles sellest kuupäevast.

3. peatükk. Teabele juurdepääsupiirangu seadmine

§ 26. Kas juurdepääsupiiranguga dokumendid tuleb registrisse kanda?

1. Dokumendiregistrisse kantakse ka juurdepääsupiiranguga dokumendid. Kuid registri avalik vaade ei tohi reeta nende sisu (nt pealkirja ja dokumendi saaja/saatja koosmõjus).
2. Loomulikult ei võimaldata dokumendiregistri kaudu digitaalset otseligi pääsu juurdepääsupiiranguga dokumentide sisusse (AvTS-i § 12 lg 4¹).

§ 27. Mida näidata piirangu kehtestamise kohta?

1. Piirangu korral näidatakse vastavas märkes piirangu kehtestamise aeg, õiguslik alus (viide AvTS-i normile), tähtaeg, piirangu kehtetuks tunnistamine ja muud olulised andmed. Näide:

Andmekaitse Inspektsioon tunnistas selle dokumendi
30.03.2016
ASUTUSESISESEKS KASUTAMISEKS
avaliku teabe seaduse § 35 lg 1 p 1 alusel kuni otsuse
jõustumiseni ning § 35 lg 1 p 12 alusel, kuni möödub
vajadus, kuid mitte kauemaks kui 30.03.2091

Kui dokument sisaldab mitut piirangu alust tuleb dokumendil näidata kõik piirangu alused.

Näiteks kui tegemist on järelevalvemenetluse dokumendiga, mis sisaldab ka juurdepääsupiiranguga isikuandmeid ning piirangu aluseks on ainult AvTS § 35 lg 1 punkt 2, siis peale otsuse jõustumist peaks olema dokument avalik. Dokumendihaldur ei pruugi alati märgata/teada, et dokument sisaldab ka muud piiranguga teavet ning piiranguga teave võib saada avalikuks.

Ugandi Maavalitsus tunnistas selle dokumendi 24.04.2012
ASUTUSESISESEKS KASUTAMISEKS
avalikku teabe seaduse § 35 lg 1 p 2 alusel
kuni otsuse jõustumiseni
ning avaliku teabe seaduse § 35 lg 1 punkti 12 osas kuni möödub
vajadus,
kuid mitte kauemaks kui
24.04.2087

2. Piirangu lõpptähtaeg tuleb näidata kuupäevana (kui see on võimalik).
3. Kui teabekandjale ei ole tehniliselt võimalik märget teha, siis asendab seda hädalahendusena piiranguandmete näitamine dokumendiregistris (sellest lähtub ka AvTS-i § 41 lg 2).

§ 27¹. Sätted, mille alusel ei saa dokumentidele juurdepääsu piirangut kehtestada.

Sätted, mis kohustavad ametnikke, eksperte ning teisi isikuid, kellel on juurdepääs piiranguga teabele, hoidma saladuses neile teatavaks saanud andmeid, ei ole dokumentidele juurdepääsupiirangu kehtestamise aluseks.

Sellisteks säteteks on näiteks [avaliku teenistuse seaduse](#) § 55, [riigikontrolli seaduse](#) § 47 lg 1. Eeltoodud loetelu ei ole ammendav.

§ 28. Sarjapiirang – millal kasutada, kuidas tähistada?

(Kehtetu alates 22.10.2014)

§ 29. Kas eraelulise teabe väljastamisel küsida puudutatud isiku arvamust?

Levinuimaks juurdepääsupiirangu aluseks on saanud AvTS-i § 35 lg 1 p 12 – teave, mille avalikuks tulek kahjustaks oluliselt eraelu puutumatust. Kahtluse korral on heaks tavaks küsida puudutatud isiku (andmesubjekti) enda arvamust – eeldusel, et ta on mõistlike pingutustega kiiresti kättesaadav. Tõsi, isikul ei ole kohustust seisukohta anda ega seda põhjendada, asutus aga ei ole selle seisukohaga seotud. Kuid kuna inimesed tunnetavad eraelu piire erinevalt, siis võib puudutatud isiku arvamus olla

asutusele väärtuslikuks infoks otsuse tegemisel. Ühtlasi annab arvamuse küsimine puudutatud isikule võimaluse oma õiguste kaitseks välja astuda. Näiteks võib ta vaidlustada asutuse tegevuse ja paluda halduskohtul keelata oma eraelu oluliselt kahjustava teabe väljastamine kuni kohtuotsuse jõustumiseni.

§ 30. Kas inimese nimele, sünniajale ja isikukoodile saab kehtestada piirangut?

1. Üksnes inimese nime olemasolu dokumendis ei ole piirangu seadmise põhjuseks AvTS-i § 35 lg 1 p 12 alusel, kui dokument ise ei sisalda eraelu puutumatum oluliselt kahjustavat teavet. Ka sünniaja või isikukoodi lisamine nimele ei saa iseenesest olla piirangu seadmise aluseks.²⁴
2. Mõnel juhul võib olla võimalik väljastada eraelu puutumatum oluliselt kahjustava sisuga dokument nii, et see ei seostuks konkreetse inimesega (eemaldades nime ja teised isikut tuvastada võimaldavad andmed ning jättes alles avalikku huvi pakkuva sisu).
3. AvTS-i § 35 lg 1 p 12 alusel ei saa piirangut kehtestada dokumendi sisule ega ka dokumendi saaja/saatja isikule, kui dokument ei käsitle inimese eraelu, vaid üksnes avalikku tegevust ja ühiskondlikke küsimusi.

Hea näide on siin märgukirjad, mille eesmärk on teha avaliku võimu teostajale ettepanekuid tema töö korraldamiseks või valdkonna arenguks või anda talle teavet. Või on tegemist selgitustaotlusega, kus küsitakse selgitusi asutuses välja töötatud õigusakti kohta ilma oma eraelu kirjeldamata.²⁵ Ka teabenõude enda kui dokumendi puhul puudub selle sisul ja esitaja isikul enamasti eraelu puutumatum oluliselt kahjustav mõju. Kuid loomulikult ei saa otsustada üksnes dokumendi pealkirja järgi. Need dokumendid võivad sellegipoolest sisaldada ka eraelulist teavet (näiteks kontaktandmeid) ja muid AvTS-i § 35 lõikes 1 loetletud piirangu aluseid.

§ 31. Kas isiklikud kontaktandmed vajavad piirangut?

1. Isikliku kontaktteabe (kodune aadress, isiklik e-posti aadress ja telefoninumber jms) sattumine teabenõude korras või dokumendiregistri otseligiipäasu kaudu piiramatult hulga võõraste isikute kätte võib oluliselt kahjustada tema eraelu puutumatum. See võib põhjustada rämpsposti adressaadiks sattumist ja muud soovimatut kontaktivõtmist. Seetõttu tuleb isiklikule kontaktteabele dokumendis seda piirang AvTS-i § 35 lg 1 p 12 alusel.
2. Samas ei saa seda piirangut seada igasuguse kontaktteabe puhul:
 - a) kui inimene osaleb kirjavahetuses juriidilise isiku või asutuse töötajana, ettevõtjana või vaba elukutse esindajana, siis võib eeldada, et ta ei kasuta isiklike kontaktandmeid;
 - b) juriidilisel isikul ja asutusel endal ei ole eraelu, AvTS-i § 35 lg 1 p 12 ei kohaldu,
 - c) AvTS-i § 35 lg 1 p 12 ei kohaldu ka füüsilisest isikust ettevõtja äritegevusele ning vaba elukutse (notari, advokaadi, audiitori, kohtutäituri jt) ameti- või kutsetegevusele. Selline tegevus on suunatud avalikkusele ega ole eraeluline.
3. Erasisiku isiklikule kontaktandmetele piirangu seadmine ei kohaldu ainult kirjavahetusele, vaid ka kõigile teistele dokumentide liikidele, mis sisaldavad erasisikute kontaktandmeid. Sellisteks dokumentideks on näiteks ka erasisikutega sõlmitud lepingud.

§ 32. Kas kinnistu aadress vajab piirangut?

1. Arvestades kinnistusraamatu ja maakatastri avalikkust võib tekkida küsimus, kas kinnistu aadressiga kokkulangevale kontaktaadressile peaks seadma AvTS-i § 35 lg 1 p 12 alusel piirangu? Kirjavahetuses avaldatud postiaadressi võrdlemine sama isiku kinnistusraamatus näidatud aadressiga oleks aga asutusele mõttetu ajaraiskamine. Lisaks peaks arvestama rämpspostiriskiga. Rämpspostitajad ei korja aadressandmeid tavaliselt kinnistusraamatust, kus digitaalne ligipääs on tasuline, vaid eelistavad tasuta ligipääse, sh nt AvTS-i alusel.

²⁴ Isikukoodi kasutamise kohta vt Andmekaitse Inspektsiooni [Isikukoodi kasutamise juhend](#). Juhend selgitab, et isikukood ei ole iseenesest salajasem või tundlikum teave kui inimese nimi, sünniaeg vms isiku tuvastamiseks vajalik põhiteave. Küll aga peab lähtuma minimaalsuse põhimõttest: isikukoodi tuleks kasutada siis, kui seda on tegelikult vaja.

²⁵ [Märgukirjale ja selgitustaotlusele vastamise ning kollektiivse pöördumise esitamise seadus](#) annab nii märgukirja (§ 2 lg 2) kui ka selgitustaotluse definitsiooni (§ 2 lg 3 ja § 3).

2. Samas ei ole vajadust ega põhjust kinnistu/katastriüksuse aadressile AvTS-i § 35 lg 1 p 12 alusel piirangut seada, kui tegu pole lihtsalt dokumendile lisatud isiku kontaktandmetega, vaid aadress on haldusakti oluline osa ja haldusakt ei sisalda iseenesest muud tundlikku teavet. Näiteks võib tuua katastriüksuse sihtotstarbe muutmist või otse aadressi enda muutmist või kinnistu nime muutmist.

§ 33. Mis on ärisaladus?

1. Juriidiliste isikutega peetud kirjavahetuse ja nendega sõlmitud lepingute puhul on levinud piirangu aluseks AvTS-i § 35 lg 1 p 17 (teave, mille avalikuks tulek võib kahjustada ärisaladust). Riigi- ja kohaliku omavalitsusasutustel ega nende hallatavatel asutustel ei saa üldjuhul olla ärisaladust (v.a juhul, kui on tegemist selgelt ärilise teenuse osutamisega).

2. Asutus ja ta lepingupartner ei saa kokku leppida piirangute rakendamises suuremas mahus, kui näeb ette avaliku teabe seadus. Lepingusse pandud punkt, mille kohaselt kogu lepingu sisu on ärisaladus või muul põhjusel konfidentsiaalne, on asutusega sõlmitud lepingu puhul õigustühine.

3. Avaliku teabe seaduse alla kuuluva lepingu kogu sisu ei saa olla täieliku juurdepääsupiiranguga juba sellepärast, et AvTS-i § 36 lg 1 punktid 9 ja 10 keelavad eelarvevahendite kasutamist, eelarvest makstud tasusid ja hüvitsi ning asutuse varalisi kohustusi salastada. Järelikult vähemalt eelarvest raha eraldamist puudutav lepingu osa on igal juhul avalik.

4. AvTS ise ärisaladuse mõistet ei anna. Seda teeb [konkurentsiseaduse](#) § 63 lg 1:

Ärisaladuseks loetakse niisugune teave ettevõtja äritegevuse kohta, mille avaldamine teistele isikutele võib selle ettevõtja huve kahjustada, eelkõige oskusteavet puudutav tehniline ja finantsteave ning teave kulude hindamise meetodika, tootmissaladuste ja -protsesside, tarneallikate, ostu-müügi mahtude, turuosade, klientide ja edasimüüjate, turundusplaanide, kulu- ja hinnastruktuuride ning müügistrateegia kohta. Ärisaladus ei ole avalikustamisele kuuluv või avalikustatud teave /.../.

5. Kuigi [konkurentsiseaduse](#) § 63 lg-s 1 toodud ärisaladuse mõiste on hinnangulise sisuga, on ilmne, et eelarveraha eraldamist käsitleva lepinguosa kõrval on muidki andmeid, millele ärisaladust laiendada ei saa: näiteks lepingu ese kui selline (mida telliti), leppetrahvid ja muud sanktsioonid lepingu mittetäitmise korral jms.

§ 34. Kellelt tuleb algatus ja otsus teabe tunnistamise kohta ärisaladuseks?

1. [Konkurentsiseadus](#) lähtub sellest, et ettevõtja ise on aktiivne, märkides ära, millist teavet ta loeb ärisaladuseks ja seda vajadusel põhjendades (§ 63 lg 2). Sellest võib lähtuda ka avaliku teabe seaduse kohaldamisel.

2. Kui ettevõtja ise ei väljenda, et tegu on ärisaladusega, siis asutus peaks AvTS-i § 35 lg 1 punkti 17 omal algatusel kohaldama vaid siis, kui ärisaladuse sisaldumine dokumendis on täiesti ilmne.

3. Asutus küsib vajadusel ettevõtjalt põhjendusi, kuid piirangu seab ta (või keeldub seadmisest) omaenda kaalutusotsusena.

§ 35. Kas riigihanke pakkumus on juurdepääsupiiranguga teave?

[*Kehtetu alates 19.05.2014, sisu üle viidud Riigihangete peatükki*]

§ 36. Millised kohtudokumendid on juurdepääsupiiranguga?

1. Kohtuasutustes olevate dokumentide/teabe avalikkus ja piirangud on täpsemalt sätestatud kohtumenetluse seadustes ja kohtute seaduses.²⁶

2. Tsiviilkohtumenetluses osalev asutus võib enda kui menetlusosalise huve kahjustada võivale teabele piirangu seada kuni kohtulahendi tegemiseni (AvTS § 35 lg 2 p 4).²⁷

26 Vt nt [tsiviilkohtumenetluse seadustiku](#) § 59, 60¹ ja 61, [halduskohtumenetluse seadustiku](#) § 88, 89, [kriminaalmenetluse seadustiku](#) §-id 214, 408¹, [väärteomenetluse seadustiku](#) § 2 ja 62, [kohtute seaduse](#) § 34.

27 AvTS-i § 35 lg 2 p 4 räägib küll üksnes riigiasutustest teabevaldajast, kuid sätte eesmärki arvestades on ilmne, et seda saab laiendada ka omavalitsusasutustele ning avalik-õiguslikele juriidilistele isikutele.

§ 37. Kuidas võib väljastada menetlusteavet ja järelevalveotsuseid?

1. Riikliku, haldus- ja teenistusliku järelevalve menetluses, väärteomenetluses ja kriminaalmenetluses kogutud teave on tavaliselt kuni otsuse jõustumiseni mitteavalik (AvTS-i § 35 lg 1 p 1 ja 2).
2. Erandina võib otsuse või avaliku arutelu eel menetlusteavet avaldada, kui selleks on väga mõjuvad põhjused (AvTS-i § 30 lg 3 ja 4 koosmõjus § 38 lõikega 1, [kriminaalmenetluse seadustiku](#) § 214, [väärteomenetluse seadustiku](#) § 62).
3. Üheks avalikustamise põhjuseks võib olla ülekaalukas vajadus anda selgitusi selle kohta, mida asjaosaline isik on avalikkusele teatavaks teinud. Kui juurdepääsupiirangu eesmärk on kaitsta menetluse osapoolt, kes aga ise menetluse kohta avalikkuses sõna võtab, siis peab ka asutusel teatud juhul olema võimalik oma tegevust avalikkuse ees nendes piirides selgitada ja võimalikke väärarusaamu kummutada. Siiski peaks asutus jääma nendesse piiridesse, mida asjaosaline on ise avalikkuse ette toonud. Menetlusandmete avalikustamine ei tohi olla kättemaksuakt!
- 3¹. Järelevalvealased otsused võib asutuse seisukohtade läbipaistvuse huvides avaldada pärast allkirjastamist ja piiranguga teabe puhastamist. Järelevalve käigus kogutud teabe avaldamise piirangu (AvTS § 35 lg 1 p 2) mõte on mitte anda välja vastuolulist teavet (algmaterjale) enne järelevalveasutuse lõpliku seisukoha kujundamist. Kui aga otsus on tehtud, siis on seisukoht kujundatud ning see ei muutu- sõltumata sellest, mis hetkel otsus jõuab adressaadini ja jõustub. Asutuse seisukohtade läbipaistvus on hüve, mis kaalub üles kättetoimetamata otsuse problemaatilisuse.
4. Muud asutused peavad arvestama, et kohtueelse kriminaalmenetluse teabe avaldamine enne kohtulikku arutelu on lubatud üksnes prokuröri loal (kriminaalmenetluse seadustiku § 214). Väärteomenetluse teavet võib kuni otsuse jõustumiseni avaldada menetleva ametniku loal (väärteomenetluse seadustiku § 2 ja 62).
5. Menetlusjärgset kriminaal- ja väärteoteabe avaldamist on selgitatud juhise 11. peatükis.

§ 38. Kas juurdepääsupiirang piirab juurdepääsu tervele dokumendile?

1. Juurdepääsupiirang seatakse igale dokumendile eraldi. Kui piiranguga teave on näiteks põhidokumendi lisa(de)s, siis on lihtne märkida piirang üksnes lisa(de)le. Kui piirangu seadmisel ei ole võimalik dokumente niimoodi jagada, siis seatakse piirang tervele dokumendile, kuigi piirangu põhjus võib puudutada vaid väikest osa tervest dokumendist.
2. Teabenõude täitmisest ei saa keelduda ainuüksi põhjusel, et küsitud dokument/teave sisaldab muu hulgas piiranguga teavet (vt ka Riigikohtu 23.10.2003. a otsust nr 3-3-1-57-03, RT III 2003, 32, 324, punkt 20). Kui on võimalik, siis tagatakse juurdepääs üksnes sellele osale küsitud dokumendist/teabest, mida piirang ei puuduta (AvTS-i § 38 lg 2).
3. Alati ei ole võimalik eristada piiranguga ja piiranguta osasid:
 - a) kui asutus annab vastuse eraisiku selgitustaotlusele mingi õigusakti kohaldamise kohta, siis võib ka muu huviline esitada selle kohta teabenõude. Eelduslikult on piirang üksnes vastuskirja saaja kontaktteabel (vt selle juhendi § 31), seda on lihtne kinni katta;
 - b) kui aga teabenõue puudutab selgitustaotlust ennast, võib asi olla keerulisem. Selgitustaotlus sisaldab näiteks tihti viiteid taotluse esitaja eraelule (terviseandmetele, pereelu üksikasjadele, isiklikele kannatustele vms).²⁸ Sel juhul võib olla ebamõistlikult raske eristada teabenõudega küsitud selgitustaotlusest sellist teavet, mida piirang ei puuduta.

§ 39. Mida panna tähele õigusakti avalikkuse piiramisel?

1. Kui eriseadus ei sätesta teisiti, kehtib õigusakti (nii üld- kui üksikakti, sh määruse, korralduse, otsuse, käskkirja) puhul üldine juurdepääsupiirangute seadmise kord (AvTS-i § 35).
2. AvTS-i §-s 35 ette nähtud üldisi piiranguluseid kohaldatakse ka õigusakti aktiivsel ja passiivsel avaldamisel, kui eriseadusest ei tulene teisiti. Kui õigusakti avaldamise nõue (nt kohaliku

²⁸ Näites toodud asjaoludele kohalduvad juurdepääsupiirangud AvTS § 35 lg 1 punktide 11, 13 ja 15 alusel.

omavalitsuse korralduse seaduse §-d 23 ja 31) läheb vastuollu teabele juurdepääsu piiramisega, avaldatakse õigusakt osaliselt.

Näiteks sotsiaalkorterite üürile andmise puhul [sotsiaalhoolekande seaduse](#) alusel võib kohaliku omavalitsuse õigusakt sisaldada nii üürniku kui ka tema pereliikmete andmeid ning neist väljaloetavat kooseluset, üürileandmise motiive kui lõpuks ka nende kontaktteavet. Üürileandmise fakt ja objekt (korterite aadress) on kindlasti avalik (tegemist on avaliku vara kasutamisega, vt ka AvTS § 36 lg 1 p 11), kuid pereliikmete isikuandmete osas on kohane rakendada AvTS § 35 lg 1 p 12 alusel juurdepääsupiirangut.

§ 40. Kui kauaks võib piirangu seada?

1. AvTS-i § 40 lg 1 alusel kehtestatakse juurdepääsupiirang kuni vajaduse möödumiseni või mingi kindla sündmuse saabumiseni (näiteks dokumendi kinnitamiseni siseauditi aruannete puhul AvTS § 35 lg 1 p 18 või dokumendi allkirjastamiseni AvTS § 35 lg 2 p 2), kuid mitte kauemaks kui 5 aastaks. Põhjuse püsimisel võib seda samas paragrahvis lubatud raamides pikendada.

2. Sama paragrahvi lõike 3 alusel kehtestatakse isikuandmeid sisaldavale asutusesisesele teabele juurdepääsupiirang 75 aastaks.²⁹ Seda sätet on mõnikord mõistetud valesti: nagu puudutaks see igasugust isikuandmeid sisaldavat teavet. Tegelikult tuleb sätet vaadata mitte seadusest välja rebituna, vaid tõlgendada süstemaatiliselt kui seaduse komponenti.

3. Säte on osa AvTS-i 5. peatüki („Piiratud juurdepääsuga teave“) regulatsioonist. Sama peatüki § 34 lg 2 lubab asutuse juhil tunnistada teabe asutusesiseseks kasutamiseks üksnes seaduse alusel. Aluste loetelu annab järgmine paragrahv (35). See võimaldab isikuandmetega seoses kehtestada piiranguid teabele, mis sisaldab:

- a) delikaatseid isikuandmeid,³⁰
- b) isikuandmeid, millele juurdepääs kahjustab oluliselt eraelu puutumatust,
- c) sotsiaalabi või -teenuste osutamise taotlemist,
- d) perekonnaelu üksikasjade kirjeldust,
- e) isiku vaimsete ja füüsiliste kannatuste kirjeldust (AvTS-i § 35 lg 1 p 11–15).

4. Niisugusele teabele saab tõepoolest kehtestada AvTS-i § 40 lg-s 3 nimetatud pika tähtajaga juurdepääsupiirangu. Kuid tuleb arvestada, et see piirangualus ei laiene muule isikuandmeid sisaldavale teabele, millele AvTS-i § 35 alusel piirangut kehtestada ei saa (nt personalidokumendid, mis sisaldavad teenistuja nime, ametinimetust ning tööle võtmist / puhkuse andmist / lähetusse saatmist jne ning kus vaid mingi üksik fakt vajab eraelu kaitseks piirangut).

5. Dokumentidele, mis on loodud või saadud enne avaliku teabe seaduse kehtima hakkamist (2001. a), enam piirangut kehtestada ei saa. [Avaliku teabe seadus](#) lubab piirangu kehtestada maksimaalset 10-ks aastaks. Erand sellest on juurdepääsupiiranguga isikuandmed, millele on võimalik kehtestada piirang 75-ks aastaks. Sellisel juhul on piirangu alguseks dokumentide loomise või saamise aeg, mitte piirangu kehtestamise aeg (AvTS § 40 lg 1).

§ 41. Mida teha, kui piirang aegub?

Kui juurdepääsupiirangu aegumisel ei ole võimalik sellekohaseid märkeid üle kontrollida (et piirangut maha võtta või pikendada), peab dokumendiregistri avalikus vaates olema selgitus, et dokumendil võib olla peal aegunud piirang ja seda võib ikkagi teabenõude korras küsida.

§ 42. Kuidas piirangut kohaldada, kui dokument liigub ühest asutusest teise?

1. Teabevaldaja seatud juurdepääsupiirang on siduv ka kõigile teistele teabevaldajatele. Kui otse eriseadusest ei tulene teisiti, ei saa teine asutus piirangut omatahtsi kehtetuks tunnistada ega eirata. Vastasel juhul kohaldub vääртеovastutus (AvTS-i § 54¹ lg 1). Ainult piirangu seadnu saab selle kehtetuks tunnistada, teised saavad vaid tema tähelepanu juhtida.

29 Või isiku surmast alates 30 aastaks või kui surma ei ole võimalik tuvastada, siis sünnist alates 110 aastaks.

³⁰ Delikaatsete isikuandmete ammendava loetelu annab IKS § 4 lg 2.

2. Tihti sisaldavad elektroonilised kirjad lõpus taolist märget „...Selles e-kirjas sisalduv teave (kaasa arvatud manused) on mõeldud ametialaseks kasutamiseks ning seda võivad kasutada vaid e-kirja adreassaadid. E-kirjas sisalduvat teavet ei tohi ilma saatja selgelt väljendatud loata edasi saata ega mistahes viisil kõrvalistele isikutele avaldada. Juhul, kui Te olete saanud käesoleva e-kirja eksituse tõttu, teavitage sellest koheselt saatjat ning kustutage e-kiri oma arvutist.“ Sedalaadi märke puhul ei ole tegemist juurdepääsupiirangu mäkega AvTS-i mõistes, kuna mäрге ei sisalda piirangu alust ega aega.

§ 43. Mida teha, kui teine asutus on unustanud juurdepääsupiirangu seada ?

Mida teha, kui teisest asutusest tuleb dokument, millele on unustatud märkida juurdepääsupiirang, kuigi see peaks kindlasti olema? Sellisel juhul võib piirangu seada ka asutus, kes dokumendi sai. Kuid kindlasti tuleb teavitada dokumendi saatnud asutust.

§ 44. Kas eraisikule saadetak kiri vajab piirangut?

1. Eraisikule endale ei ole AvTS-i juurdepääsupiirang siduv, ta ei ole teabevaldaja AvTS-i mõttes. Isiku enda otsustada on, kas ta omaenda eraelu või ärisaladuse kaitseks piirangu saanud teavet avalikustab või mitte.³¹ Piirang kaotab mõtte, kui eraisik ise on teabe avalikustanud, sel juhul võib selle seadnud asutus piirangu kehtetuks tunnistada.
2. Juurdepääsupiirang pannakse asutusse jäävale koopia, kuna see on siduv asutusele endale (sh dokumendiregistris dokumendi andmete näitamisel ja otseligi pääsu võimaldamisel).
3. Kuna eraisikule juurdepääsupiirang siduv ei ole, siis ei ole eraisikule väljasaadetavale kirjale, juurdepääsupiirangu märkimine kohustuslik. Asjaajamiskorra ühtsete aluste § 10 lg 7 kohaselt peab erinevalt vormistatud dokumentidel olema tagatud sisu samasus, mitte dokumentide identsus.
4. Kui sama sisuga elektrooniline kiri saadetakse mitmele füüsilisele isikule korraga, siis ei tohi kirja saajale olla näha kõigi kirja saajate nimed ja aadressid. Selle vältimiseks tuleb kasutada pimekoopiat.

³¹ Kui ta avalikustab teise isiku eraelu kahjustavat teavet või delikaatseid isikuandmeid, võib järgneda väärteovastutus [isikuandmete kaitse seaduse](#) §-de 42 alusel või [karistusseadustiku](#) § 157¹ lg 1 ja 3 alusel. Tsiviilvastutus kohaldub, kui ettevõtte töötaja avalikustab ärisaladust.

4. peatükk. Kontaktteave asutuse võrgulehel

§ 45. Mis kontaktteavet tuleb võrgulehel avaldada?

1. Kontaktteave on andmed, mille põhjal avalikkus saab aru, millega asutus/üksus/ametnik tegeleb ja kuidas kontakteeruda. Võrgulehel tuleb avaldada:

- a) asutuse ja selle üksuse põhimäärused (AvTS-i § 28 lg 1 p 3);
- b) ametnike ametijuhendid (AvTS-i § 28 lg 1 p 5);
- c) asutuste koosseisud koos ametnike nimede, haridus- ja erialaandmete, telefoninumbrite ja e-posti aadressidega (AvTS-i § 28 lg 1 p 6);
- d) täitmata ametikohad asutustes (AvTS-i § 28 lg 1 p 19);
- e) asutuse vastuvõtukorraldus (AvTS-i § 28 lg 1 p 24 ja 27).

1¹. Võrgulehel ei kuulu avalikustamisele sisejulgeoleku tagamise, riigikaitsepoliitika kujundamise, riigikaitse korraldamise sh riigi sõjalise kaitse planeerimise, ettevalmistamise ja juhtimise või riigisaladuse ja salastatud välisteabe kaitse korraldamisega tegeleva ametniku ega töötaja kontaktandmed, kui sellise teabe avalikuks tulek ohustaks riigi julgeolekut või riigisaladuse ja salastatud välisteabe kaitset. Sellised andmed on piiranguga avaliku teabe seaduse § 35 lg 1 punkti 3¹ alusel.

2. Kui asutus on andnud mõned enda funktsioonid üle teisele asutusele/ettevõttele (näiteks riigiasutustele osutab raamatupidamisteenust ja personaliarvestust Riigi Tugiteenuste Keskus), siis tuleb kontaktide juures näidata ära, milliseid funktsioone täidavad teised asutused/ettevõtted ning lisada link nende võrgulehele (kui see on olemas).

Näiteks võib tuua [Andmekaitse Inspektsiooni](#) võrgulehe.

3. Kuna [avaliku teenistuse seaduse](#) kohaselt võib ametiasutustes olla nii ametnikke kui töölepinguga töötavaid teenistujaid, siis tuleks võrgulehel avalda teave, millised ametikohad on täidetud ametnikega ja millistel töökohtadel töötavad töölepinguga teenistujad. Sellise teabe avalikustamine on oluline seetõttu, et võrgulehe külastajal oleks arusaadav, milliste ametikohtadel töötajate puhul peavad ametijuhendid ja palgaandmed jms andmed olema avalikud, kuna seadus kohustab avalikustama ainult ametnike andmeid (AvTS § 28 lg 1 punktid 5 ja 6 ning ATS § 65 lg-d 1 ja 2 ja § 119 lg-d 1 ja 2).

§ 46. Kuhu kontaktteave paigutada?

1. Kontaktteave on võrgulehe vaadatavamaid osi, seetõttu peaks ta tiitellehe avanemisel jääma kasutajast ühe klõpsu kaugusele (nn. ühe klõpsu reegel).

2. AvTS §-s 28 sätestatud teave on võrgulehe põhiteave. On lubamatu avaldada põhiteavet üksnes asutuse dokumendiregistri või asutuse õigusaktide andmekogu kaudu.

§ 47. Kuidas kontaktteavet kokku lõimida?

Asutus peaks kasutama digitaalse avaldamise eeliseid ning kontaktteabe lõimima:

1) vastuvõtukorraldus (AvTS-i § 28 lg 1 p 24 koosmõjus punktiga 27 ja p 23) – vastuvõtuajad jm vastuvõtuga seotud asjaolud koos asutuse üldiste kontaktandmetega soovitavalt kontaktteabe alguses, samuti eelseisvad muudatused vastuvõtukorralduses;

2) asutuse ja selle üksuste põhimäärused (§ 28 lg 1 p 3) – soovitavalt hüperlingituna kontaktteabe lehel, asutuse ja struktuuriüksuse nime peal klõpsatavana. Kasutajasõbralik on lisada kontaktteabes üksuse nimetuse juurde kokkuvõtlikult üksuse vastutusala kirjeldus, kui põhimäärus on liiga üldsõnaline, ning eriti, kui üksuse nimetus ei ole üldarusaadav,

3) koosseis, täidetud ametikohad (ametnike nimede ja kontaktandmetega) ning täitamata ametikohad (sama sätte p 6 ja 19) – koondnimekirjana. Personaalse lisateabe (foto, elu- ja töökäik, publikatsioonide loetelu jms) avaldamiseks on vaja ametniku nõusolekut,

4) kehtetu 12.09.2016,

5) ametniku ametijuhend või seda asendav dokument (p 5), tema haridus ja eriala (p 6) – ametniku kontaktireal selleks sobilikul andmeväljal klõpsatavana. Ametniku hariduse all näidatakse

[haridusseaduses](#) nimetatud haridustase või riiklikult tunnustatav kraad ning diplomil märgitud eriala. Fraas „kõrgharidus omandamisel“ ei vasta seadusele (tegu on keskharidusega).

Väikese ja keskmise suurusega asutuse lõimitud kontaktteabe eeskujuks sobib [Andmekaitse Inspektsiooni kontaktteave](#).

§ 48. Millised on suure asutuse kontaktteabe erisused?

1. Võrgumaterjal, sh kontaktteave, ei peaks olema pikalt keritav (st ekraanivaadet ei tuleks pikalt allapoole kerida).
2. Suure asutuse puhul, kus kontaktteave ületab oluliselt 2 ekraanivaate mahu, tuleb see esitada hüperlingitud sisukorrana, kus üksuse nime peal klõpsamine viib täpsema kontaktteabeni.
3. Kasutajasõbralik lisavahend on ülevaatlik organogramm, kus üksusel klõpsamine avab detailsema kontaktteabe. Organogramm peab olema kergesti käsitletav. Vaevaliselt avanev ja kirbukirjas skeem tuleks pigem jätta avaldamata.
4. Suures asutuses, kus ametnike loetelu on väga mahukas, on otstarbekas luua võimalus otsida võrgulehelt ametnikku tema nime ning ametikoha järgi.

Head näited suure organisatsiooni klõpsatavate pealkirjadega kontaktandmestikust on [kontaktteave Haridus- ja Teadusministeeriumi võrgulehel](#) (kõrvalmenüü sisaldab haldusala kontaktteabe linke) ning . Nimepõhise otsingu heaks näiteks on ka [telefoniraamat Maksu- ja Tolliameti võrgulehel](#)³²

§ 49. Kuidas avaldada asutuse koosseis?

Kohustus avalikustada asutuse koosseis ei ole täidetud, kui avalikustatakse vaid ametnike nimekiri. Koosseis hõlmab nii täidetud kui täitmata ametikohti ning nii ametnikke kui töötajaid.

§ 50. Kas töötajate ja koosseisuväliste teenistujate nimesid võib avaldada?

1. Töötajate ametikohad tuleb koosseisus isikustamata kujul ära näidata.
2. Ülevaatlikkuse huvides on mõistlik näidata ka koosseisuväliste teenistujate ametikohad.
3. Töötajate ja koosseisuväliste teenistujate nimede näitamiseks peab olema töökorralduslik vajadus. Näiteks pole enamasti vaja avalikustada autojuhtide ja valvurite nimesid, koosseisuvälise pressiesindaja nimi aga tuleb tavaliselt näidata. Samuti võib näidata nende töötajate nimed ja kontaktid, kes töökorralduslikult suhtlevad kodanikega (näiteks sekretär).

§ 51. Kuidas avalikustada täitmata ametikohad?

Täitmata ametikohad avalikustatakse üldises koosseisunimistus ametikohana, kus teenistuja nime asemel on märges „ametikoht täitmata“. Täitmata ametikohtade avalikustamise nõue ei ole kaetud rubriigiga „Tööpakkumised“, sest kõigile täitmata ametikohtadele ei ole tavaliselt konkursi kuulutatud.

Teave käimasolevate konkursside kohta avalikustatakse, kas asutuse võrgulehel või kui teave käimasolevate konkursside kohta avalikustatakse ainult avaliku teenistuse kesksel võrgulehel, siis tuleb veebilehel selgitada, kuidas leida teavet käimaolevate konkursside kohta ja lisada vastav link.

§ 52. Kuidas avaldada kontaktteavet peatatud teenistussuhte korral?

1. [Avaliku teabe seaduse](#) § 28 lg 1 p 6 näeb ette, et võrgulehel avaldatakse asutuse koosseisus ette nähtud ametikohti täitvate ametnike andmed.
2. Kui teenistussuhe on peatatud püsivalt (mitte nt üksnes ametipuhkuse ajaks), siis isik ei täida asutuse koosseisus ette nähtud ametikohta ning tema andmeid ei tule avaldada.
3. Rasedus, sünnitamine ja väikelapse kasvatamine on eraelu ning osalt kui tervises seisund kuulub ka delikaatsete isikuandmete alla ([isikuandmete kaitse seadus](#), § 4 lg 2).

³² Lingid seisuga 25.08.2016.

4. Rasedus- ja sünnitus- ning lapsehoolduspuhkusel oleva ametniku nime ei ole vaja avaldada ning puhkuse põhjuse kuvamine on seadusevastane.
5. Kui ametnik on rasedus- ja sünnitus- või lapsehoolduspuhkusel, näidatakse kontaktteabes tema asemel asendava ametniku nimi, või kui asendajat ei ole, siis tehakse ametikoha juurde nime näitamata märge „teenistussuhe peatatud“.
6. Teenistussuhte peatanud ametnike nimede jätkuvaks näitamiseks peab olema mõjuv põhjus.

§ 53. Kuidas avaldada ametijuhendeid?

1. Avalikustama peab nii täidetud kui täitmata ametikohtade ametijuhendid.
2. Kui ametijuhend puudub, siis asendab seda asutuse või struktuuriüksuse põhimäärus. Sellisel juhul asendab ametinimetusel klõpsatavat ametijuhendi hüperlinki põhimääruse hüperlink.
3. Kui ametijuhend või seda asendav põhimäärus on liiga üldsõnaline ning võrgulehe külastaja vajab teavet ametniku konkreetse vastutusvaldkonna kohta, siis on kasutajasõbralik lisada ametinimetuse juurde (nt sulgudesse) kokkuvõtlikult ametniku vastutusvaldkonna nimetus.

§ 54. Kas ametniku kontaktandmetena peab avaldama otsekontaktid?

1. [Avaliku teabe seaduse](#) § 28 lg 1 p 6 näeb ette, et võrgulehel avaldatakse ametnike telefoninumbrid ja e-posti aadressid. Sätte eesmärk on tagada, et isikud saaksid avaliku võimu teostajaga kas telefonitsi või e-posti kaudu kontakteeruda.
2. Ametniku lauatelefoni ja otsese e-posti aadressi asemel võib olla otstarbekam avaldada üksuse sekretäri omad, kui ametnikul on liikuv töö, ta pääseb harva arvuti juurde või kui töö iseärasuste tõttu on vaja suhtlemiskoormust hajutada.
3. Sekretäri andmete avaldamine ametniku otsekontaktide asemel ei tohi olla formaalne, vaid see peab tagama isikule reaalse kontaktivõimaluse, mitte soovitusel mõne aja pärast uuesti pöörduda.
4. Pikema eemalviibimise korral suunatakse telefon töölolevale asendajale või sekretärile ning e-postkast varustatakse äraolekust ja asendajast teatava automaatvastusega.

§ 55. Kuidas võimaldada kontaktteabe masinloetavat allalaetavust?

1. Asutuse ja selle üksuse põhimäärused, täitmata ametikohad asutustes ja asutuse vastuvõtukorraldus on avaandmed, mis tuleb avalikustada võimalusel masinloetaval kujul ja avatud vormingus.
2. Ametnike ametijuhendid ja asutuste koosseisud koos ametnike nimede, haridus- ja erialaandmete, telefoninumbrite ja e-posti aadressidega tuleb samuti avalikustada masinloetaval kujul ja avatud vormingus, kuid selle taaskasutamist võib piirata AvTS § 3¹ lõigetes 7-9 sätestatud korras (AvTS § 29 lg 4).
3. Avaandmete ning taaskasutamise piiramise kohta loe täpsemalt käesoleva juhise §-st 84¹.

§ 56. Miks ei tohi kasutada menüüpunkti „Avalik teave“?

Kogu võrgulehel avalikustatav info ongi avalik teave. Eksitav ja vääri on kasutada mõne rubriigi või alamrubriigi pealkirjana „Avalik teave“.

§ 57. Kuidas avaldada asutuse vastuvõtukorraldus?

1994. aastal jõustunud [avaldustele vastamise seadus](#) nägi ette, et asutuste juhtidel peab olema vastuvõtuaeg. Seetõttu lisati [avaliku teabe seaduse](#) § 28 lg 1 p 24 nõue vastuvõtuajad avaldada. Avaldustele vastamise seadus asendati aga 2004. aastal [märgukirjale ja selgitustaotlusele vastamise seadusega](#), mis ei sisalda enam asutuse juhtide vastuvõtukohustust. Küll aga on igal asutusel kellaajad ja muud tingimused, kuidas kohapeal pöördunud isikuid vastu võtta. Seetõttu tuleb asutuse juhtide vastuvõtuaegade avaldamise nõuet koosmõjus sama sätte punktiga 27 vaadelda kui kohustust avaldada võrgulehel vastuvõtuaegade ja muu vastuvõtukorralduse teave. Punkti 24 järgi tuleb teave vastuvõtukorralduse muutumisest avaldada vähemalt 10 päeva ette.

§ 58. Kuidas viidata seotud asutustele?

1. AvTS-i § 32 lg 3 kohaselt peab riigi keskasutuse (ministeerium, maavalitsus, Riigikantselei) võrgulehelt pääsema otse nende halduses olevate asutuste võrgulehele. Nende lingid tasub anda keskasutuse kontaktteabe juures kõrvalmenüüna. Otstarbekas on hallatavate asutustena käsitleda ka ühinguid ja sihtasutusi, kus keskasutus on riigi esindaja.
2. Analoogia kohaldub valla- ja linnavalitsuste ning nende asutuste, allasutuste ja ühingute ning sihtasutuste suhtes.
3. Otstarbekas on lisada ka selliste institutsioonide lingid, kellega asutus on oma tegevuses seotud, olemata alluvusvahekorras (nt Riigikohtu ja advokatuuri lingid Justiitsministeeriumi võrgulehel).

5. peatükk. Asutuse personaliteabe avalikkus ja piirangud

§ 59. Kas asutuse personaliteave on avalik?

1. Avaliku sektori asutus tegutseb maksumaksja raha eest, teostades avalikku võimu, pakkudes avalikke teenuseid või täites muid avalikke ülesandeid. Personaliküsimused lahendatakse asutuses enamasti haldusakti vormis. Sestap on ka avaliku sektori personaliteave avalik: kes, kus ja kellena töötab, kui palju palka saab, mis asjus lähetuses käib, millal puhkab jne (AvTS-i § 3).
2. Avalikkust saab piirata, kui on konkreetne alus kas AvTS-is (§ 35 lg 1 p 31) või eriseaduses. Vt ka juhendi § 75.
3. Kindlasti ei saa juurdepääsupiirangu alus olla üldsäte, näiteks AvTS-i § 4 lg 3 või § 40 lg 3.

§ 60. Kas piirangu alus saab sisalduda üksnes personalikäskkirjas?

Juurdepääsupiirangu vajalikkuse hindamiseks tuleb vaadata mitte üksnes vastavat haldusakti vm põhidokumenti, vaid ka alus- ja lisadokumente. Piirangu põhjus võib tulla näiteks teenistuja avalduses näidatud asjaoludest või avaldusele lisatud dokumendist (näiteks arstitõendist).

§ 61. Kas juurdepääsupiirang piirab juurdepääsu tervele dokumendile?

Eraelu puutumatus oluliselt kahjustav tõik ega muu piiranguga teave ei tee veel kogu dokumenti automaatselt piirangualuseks. Vt ka selle juhendi § 38.

§ 62. Kas teenistuja nimi on juurdepääsupiirangu aluseks?

Teenistuja nime, ametikoha jms tööalase (mitte eraelulise) teabe avaldamine teabenõude korras või dokumendiregistri otseligiipääsu kaudu ei saa veel põhjustada eraelu puutumatus olulist kahjustamist (AvTS-i § 35 lg 1 p 12). Vt ka selle juhendi § 30 lg 1 ja 3.

§ 63. Kas teenistuja tööväliline kontaktteave on avalik?

Teenistuja töövälise kontaktteabe (nt kodune posti- ja e-posti aadress, isikliku telefoni number) sattumine teabenõude korras või dokumendiregistri kaudu piiramatu hulga võõraste isikute kätte võib oluliselt kahjustada tema eraelu puutumatus (AvTS-i § 35 lg 1 p 12). Sellele saab vajadusel seada piirangu. Vt ka selle juhendi § 31 lg 1.

§ 64. Kas puhkuse põhjus võib olla juurdepääsupiiranguga?

1. Teenistuja puhkuse fakt iseenesest ei ole piiranguga teave. Kuid eraelu puutumatus võib oluliselt kahjustada (AvTS-i § 35 lg 1 p 12) puhkuse andmise põhjus kas puhkusekäskkirjas või selle alusdokumendis, nt lisapuhkus lapsinvaliidi kasvatamise eest, rasedus- ja sünnituspuhkus jne.
2. Eraelulise põhjuseta tavalise puhkuse määramise alus (nt põhipuhkus, lisapuhkus teenistusstaaži eest) ei ole piiranguga teave.
3. Ka õppepuhkuse andmine (selle andmise põhjus) ei ole piiranguga teave. Küll aga võib piirata ligipääsu teabele, mis õppeasutuses ja erialal teenistuja õppepuhkuse ajal õpib, sest see on tema eraelu. Loomulikult ei saa seda piirangut rakendada alati, nt tööandja tasutud õppe korral

§ 65. Mille alusel piirata juurdepääsu terviseandmetele?

Töövõimetus-, puhkuse- jm personalidokumentidele võib olla lisatud andmeid teenistuja tervises seisundi kohta. Need on [isikuandmete kaitse seaduse](#) § 4 lg 2 p 3 kohaselt delikaatsed isikuandmed. Neile ja kõigile teistele delikaatsetele isikuandmetele (vt vastavat loetelu [isikuandmete kaitse seaduse](#) § 4 lg 2) on eraldi juurdepääsupiirangu alus: AvTS-i § 35 lg 1 p 11.

§ 66. Mida pidada silmas lähetusdokumentide puhul?

1. Teave avaliku teenistuja lähetuse kohta (kes millal kuhu milleks lähetati) on tavaliselt piiranguta teave. Seega ei ole põhjendatud kõigile lähetuse käskkirjadele piirangu kehtestamine lähetuse lõpuni. Tihti toodud põhjus, et siis võivad tulla vargad, ei ole aktsepteeritav, sest lähetuse käskkirjad ei sisalda ametnike elukoha andmeid. Samuti ei käi ametnik lähetuses kogu perega.
2. Juurdepääsu saab seada lähetusteabele, mille avalikuks tulek kahjustab riiklikku või teenistuslikku järelevalvet (menetlusega seotud ametniku lähetuse eesmärk, aeg ja koht). Kui ei ole erinormi,

seatakse piirang AvTS-i § 40 lg 2 alusel. Kuid see piirang on lühiajaline: kuni vajaduse möödumiseni (st lähetuse või menetluse lõpuni).

3. Euroopa Liidu jm rahvusvahelise organisatsiooni töökohtumise päevakava ja materjalid on korraldajad mõnikord tunnistanud ürituse toimumiseni või otsuse vastuvõtmiseni juurdepääsupiiranguga teabeks. Kui seda ei reguleeri [riigisaladuse ja salastatud välisteabe seadus](#) ega muu otse kohaldatav õigusakt (nt välisleping või EL-i määrus), võib AvTS-i mõttes olla tegu teabega, mille avalikustamine kahjustaks riigi välissuhtlust (§ 35 lg 1 p 3). Ka see piirang on lühiajaline: kuni ürituse toimumiseni või otsuse vastuvõtmiseni.

4. Lähetusaktide lisamaterjaliks olevate transpordi- ja majutusdokumentide puhul tuleb arvestada, et nende sisu avalikustamine enne lähetust võib võimaldada inimese liigset jälitamist.

Kui ei ole tegu riigisaladuse vms erijuhtumiga, on avalikkusel õigus teada, et ametiisik N. N. sõitis maksimumsja raha eest X linna täitma teenistusülesannet. Sellisele teabele ei saa enamasti piirangut seada. Samuti on avalikkusel õigus teada, millised kulutused sellega kaasnesid. Kuid detailne eelteave selle kohta, millal isik millises sadamas või lennujaamas viibib ja kus ööbib, võib olla liiast. Jälitamist võimaldav teave võib oluliselt kahjustada eraelu puutumatus (AvTS-i § 35 lg 1 p 12), hõlmates ka sisuliste tööülesannete täitmise välist aega (sõidud, ööbimised jne). Loomulikult saab sellele piirangut seada üksnes eelteabe korral – kuni lähetuse toimumiseni. Tagantjärele, pärast lähetust, see teave enam jälitamist ei võimalda ega saa olla piirangu aluseks.

5. Toodud loetelu hõlmab olulisemaid piirangu põhjusi, kuid ei ole ammendav.

§ 67. Mis tähtajad kehtivad personalidokumentide juurdepääsupiirangutele?

1. AvTS-i § 40 lg 3 alusel saab 75-aastast piirangutähtaega kehtestada üksnes teabele või selle osale, millele on kehtestatud piirang AvTS-i § 35 lg 1 p 11–15 alusel. Vt juhendi § 40. Muus osas on piirangu maksimaalne kehtivus 5 aastat, mida võib veel 5 aastaks pikendada (AvTS § 40).

2. Rõhutame, et 75 ja 5 aastat on lihtsalt ajaline ülempiir. Kui on ilmne, et piirangu põhjus võib varem ära langeda, siis peaks seda ka piirangu tekstis näitama (vrd juhendi § 27 lõikes 1 toodud näidistekstiga).

3. Kui personalidokumendid (puhkuse-, lähetuse- ja lisatasukäskkirjad) on vormistatud digitaalselt ega sisalda piiranguga teavet, võimaldatakse neile otsejuurdepääs dokumendiregistri kaudu. Seadusega kooskõlas ei ole sel juhul kasutada personalikäskkirjade puhul märget „Avalik, väljastatakse teabenõude korral“.

6. peatükk. Asutuse palgateabe avalikkus ja piirangud

§ 68. Mis on avaliku sektori palgaandmete avalikkuse eesmärk?

Avaliku sektori tegevuse (sh eelarvevahendite kasutamise) selgus ja läbipaistvus on üks demokraatliku riigikorra aluseid. See võimaldab avalikkuse kontrolli avaliku võimu teostamise üle, eriti raha kulutamise otstarbekuse üle. Selgusest lähtub ka [põhiseadus](#), andes kodanikele teabeõiguse asutuste tegevuse suhtes (§ 44 lg 2).

§ 69. Millised on avaliku sektori töötasude läbipaistvuse meetmed?

Avaliku sektori töötasude selgus on tagatud neljal viisil:

- korruptsioonivastase seaduse alusel ametiisikute palgaandmete avalikustamisega majandushuvide deklaratsioonides (seaduse 3. peatükk);
- avaliku teabe seaduse alusel teabe avalikustamisega asutuse võrgulehel;³³
- avaliku teabe seaduse alusel teabenõude esitamisega teabe saamiseks või otseligipääsuga dokumendiregistri kaudu;
- avaliku teenistuse seaduse alusel avaliku teenistuse kesksel võrgulehel (§ 65 ja 119).

§ 70. Keda puudutab korruptsioonivastase seaduse ja avaliku teenistuse seaduse alusel palgaandmete avaldamine?

- [Korruptsioonivastase seaduse](#) alusel avalikustatakse palgaandmed majandushuvide deklaratsioonides tagasisivaatena üks kord aastas. Avaldamiskohaks on deklaratsioonide register.
- Avalikustamine puudutab neid, keda see seadus käsitleb ametiisikutena. See isikute ring ei lange kokku ametnike ega eelarvest palka saavate isikute ringiga.³⁴
- [Kehtetu alates 19.05.2014].
- Avaliku teenistuse seaduse alusel avalikustatakse palgaandmed üks kord aastas:
 - ametniku põhipalk jooksva kalendriaasta seisuga;
 - kogu eelmisel aastal teenitud põhipalk, muutuvpalk ning muu teenistusülesannetest tulenev tulu.
- Palgaandmed avalikustatakse hiljemalt 1. mail avaliku teenistuse kesksel võrgulehel (avaliku teenistuse seaduse § 65, 119).

§ 71. Kuidas avaldada avaliku teabe seaduse alusel palgaandmeid võrgulehel?

- AvTS-i § 28 lg 1 p 25 käsitleb asutuste võrgulehel riigi- ja omavalitsusasutuse palgamäärade ja -juhendite, lisatasu maksmise ja erisoodustuse andmise kordade avaldamist. Selle sätte asjus leidis Riigikohus 19.05.2009. a määruses 3-4-1-1-09 (RT III, 27, 199), et:
 - säte hõlmab nii ametiasutusi kui hallatavaid asutusi,
 - säte hõlmab nii avalikke teenistujaid kui töölepingulisi teenistujaid,
 - säte nõuab umbisikulist töötasu- jm määrade ja -kordade avalikustamist,
 - säte ei nõua isikustatud kujul (st konkreetse töötaja kohta) andmete avaldamist,
 - sätet ei saa kohaldada töötajate suhtes, kelle suhtes ei ole määrasid ja kordasid õigusaktiga kehtestatud ja kellel need on määratud individuaalse töölepinguga.
- Palgamäärad ja palgajuhendid, lisatasu maksmise ja erisoodustuse andmise kord tuleb võimalusel avalikustada masinloetaval kujul ja avatud vormingus, kuid selle taaskasutamist võib piirata AvTS § 3¹ lõigetes 7-9 sätestatud korras (AvTS § 29 lg 4).

³³ AvTS §-de 28 ja 29 kohaselt avaldab asutus oma võrgulehel mh kehtivad palgamäärad ja palgajuhendid, lisatasu maksmise ja erisoodustuse andmise korra (§ 28 lg 1 p 25). Samuti avaldatakse asutuse koosseis, ametijuhendid ja haridusandmed (§ 28 lg 1 p 6) ning eelarve ja selle täitmisaruanne (§ 28 lg 1 p 11).

³⁴ Ametiisikutena käsitletakse isikuid, kel on õiguspädevus vastu võtta teistele isikutele kohustuslikke otsuseid, teha toiminguid, osaleda riigi- või munitsipaalvara erastamise, võõrandamise või kasutusse andmise otsuste tegemisel ning kohustus täita oma ametialaseid kohustusi ausalt ja õiguspäraselt. Muu hulgas peetakse ametiisikuks vabakutselisi ametipidajaid (notarid, kohtutäiturid, pankrotihaldurid) ning riigi, omavalitsuse ja avalik-õigusliku juriidilise isiku asutatud äri- ja mittetulundusühingute ning sihtasutuste juhtorganite liikmeid (§ 4 ning § 3 lg 2).

§ 72. Kas muul viisil saab palgaandmeid töötaja nõusolekuta avaldada?

1. Avaliku teenistuse seaduse alusel isikustatud palgaandmete avaldamine ning AvTS-i § 28 lg 1 p 25 alusel umbisikuline palgaandmete avaldamine üldjuhul küsimusi ei tekita.
2. Kui aga palgaandmeid küsitakse teabenõude korras ja nimeliselt, leitakse tihti, et see on vastuolus üldise tööõigusliku põhimõttega, mille kohaselt tööandja avaldab palgaandmeid kolmandatele osapooltele üksnes töötaja nõusolekul ([töölepinguseaduse](#) § 28 lg 2 p 13).
3. Kuid sama norm lubab avaldada palgaandmeid ka töötaja nõusolekuta, kui avaldamise aluseks on seadus. Keegi ei kahtle, et isikustatud palgaandmeid võib töötaja nõusolekuta avaldada nt kriminaaluurimist, kohtumenetlusi või maksustamist käsitlevate seaduste alusel. Kuid ka avaliku teabe seadus on seadus, mis annab aluse palgaandmete nõusolekuta avaldamiseks.

§ 73. Kas seadusandja on soovinud avaliku sektori palgaandmete avalikkust?³⁵

1. Seadusandja on tõepoolest soovinud, et avaliku sektori palgaandmed oleksid avalikud.
2. Riigikogule esitatud avaliku teabe seaduse algeelnõus kavandati muudatused palgaseaduse paragrahvi 8. Neis öeldi selgelt, et keeld töötaja nõusolekuta palgaandmeid avaldada ei kehti avalikele teenistujatele ega riigi- ja omavalitsusasutuste töötajatele.
3. Eelnõu [seletuskirjas](#) kommenteeriti palgaseaduse muudatusi nii:

Palgaseaduse muutmisel (§ 61) on lähtutud avaliku sektori palkade avalikkuse põhimõttest, vältimaks maksumaksja raha ebaotstarbekat kasutamist ja et ära hoida või välja selgitada korruptiivse tulu saamist. Avalike teenistujate palkade avalikkuse põhimõtete rakendatakse enamikus Euroopa Liidu riikides.
4. Palgaseadust ei muudetud avaliku teabe seadusega, sest avaliku teabe seaduse eelnõu menetlemise ajal juba täiendati [palgaseaduse § 8 muutmise seadusega](#) teatud palkade avalikustamist käsitlevat sätet. Paragrahv § 8 lg 3¹ viitas lahtise loeteluna muudele seadustele, seega ka avaliku teabe seadusele.
5. Seega lähtus seadusandja avaliku sektori töötasude avalikkusest. Seadusandja ei ole seda põhimõtet muutnud [palgaseaduse](#) asendamisel [töölepingu seadusega](#) (vrd palgaseaduse § 8 ja töölepinguseaduse §-d 28 lg 2 p 13).

§ 74. Milliseid palgaandmeid saab teabenõude korras küsida?

1. Teabenõude korras on võimalik välja nõuda dokumente töötasu ja hüvitiste kohta, kui isik saab tasu ja hüvitisi riigi, omavalitsuse ja avalik-õigusliku juriidilise isiku eelarvest.
2. AvTS-i § 36 lg 1 p 9 keelab niisugustele dokumentidele juurdepääsupiirangut seada. Nimetatud sätet tuleb vaadelda koosmõjus:
 - a) § 3 lg-ga 2: avalikule teabele juurdepääsu võib piirata seaduse alusel,
 - b) § 35 lg 1 punktiga 12: juurdepääsu piiratakse teabele, mille avaldamine kahjustab oluliselt eraelu puutumatust. Teave eelarveraha saamisest tasuna/hüvitisena ei saa isiku eraelu puutumatust oluliselt kahjustada. See ei ole ju teave selle kohta, kuidas ta seda raha kulutab.
3. Kui tekib vastuolu keelu vahel eelarveraha saamist salastada ja teatud isikuteavet avalikustada, siis eraldatakse teave ja tagatakse juurdepääs nendele andmetele (teabe või dokumendi osadele), millele piirangud ei kehti. Näiteks jäetakse haigus- ja hooldushüvitiste andmete väljastamisel neist välja teave hüvitise määramise aluste kohta või siis väljastatakse teave umbisikustatud kujul.

§ 75. Kas palgaandmete teabenõude korras küsimist saab piirata?

Palgaandmeid ei anta välja, kui andmed on AvTS-i alusel piiranguga või kui eriseadus sätestab erinõuded (§ 2 lg 2), näiteks:

³⁵ Palgaandmete avalikkuse nõue ei kehti riigi- ja kohaliku omavalitsuse sihtasutuste, mittetulundusühingute ja äriühingute töötajate kohta, kes saavad töötasu äriühingu, sihtasutuse või mittetulundusühingu eelarvest

- a) riigisaladuse ja salastatud välisteabe kaitse seaduse kohaselt on julgeolekuasutuste ja mõnede kaitseväeliste struktuuride koosseisus riigisaladus (§ 7 p 8 ja § 9 p 6);
- b) [Kehtetu alates 19.05.2014];
- c) politsei ja piirivalve seaduse § 4 lg 5 kohaselt on Politsei- ja Piirivalveameti kriminaalosakonna ja teabeturbe korralduse struktuur ja teenistujate koosseis asutusesiseseks kasutamiseks mõeldud teave.
- d) avaliku teabe seaduse § 35 lg 1 p 3¹ kohaselt on asutusesiseks kasutamiseks mõeldud teabeks teave sisejulgeoleku tagamise, riigikaitsepoliitika kujundamise, riigikaitse korraldamise sh riigi sõjalise kaitse planeerimise, ettevalmistamise ja juhtimise või riigisaladuse ja salastatud välisteabe kaitse korraldamisega tegeleva ametniku, töötaja ning tema ülesannete kohta, kui sellise teabe avalikuks tulek ohustaks riigi julgeolekut või riigisaladuse ja salastatud välisteabe kaitset.

7. peatükk. Planeeringute avalikkus ja piirangud

§ 76. Miks on planeerimine avalik menetlus?

1. Ruumiline planeerimine on [planeerimisseaduse](#) alusel toimuv avatud haldusmenetlus.³⁶ Planeeringute koostamine on avalik, kaasamaks huvitatud isikuid, tagamaks õigeaegset teavitamist ja võimaldamaks kaitsta igäihe huvisid (planeerimisseaduse § 9 lg 1). Seda õigust aitavad tagada ka normid, mis kohustavad avalikustama kõiki planeeringuid koos lisadega menetluse vältel menetluse läbiviija veebilehel.

2. Planeerimine on maakasutuse ja ehitustegevuse aluseks, kujundades inimeste elukeskkonda. Planeerimise avalikkuse juures tuleb arvestada üldise taustaga. Eestis on avalikud maamõõduandmed (sh kinnistute aerofotod), kinnisomandi andmed ja hoonete andmed, mille puhul riive eraelule võib olla oluliselt suurem.³⁷ Seega mahub planeerimise avalikkus Eesti ühiskonnas aktsepteeritud raamidesse.

§ 77. Mis seadused reguleerivad planeerimise avalikkust?

Planeeringuandmestiku avalikustamisele kohaldub nii planeerimisseadus kui ka AvTS. Need seadused ei ole avalikustamise suhtes vastuolus, vaid täiendavad teineteist.

§ 78. Millist avalikustamist näeb ette avaliku teabe seadus?

AvTS-i alusel ette nähtud avalikustamise teed kohalduvad ka planeeringuandmestikule:

- a) teabenõue,
- b) digitaaldokumendile otseligipääs asutuse dokumendiregistri kaudu,
- c) võrgulehel (avaandmetena) avaldamine (AvTS-i § 28 lg 1 p 17 ja 32).

§ 79. Milliseid piiranguid näeb ette avaliku teabe seadus?

1. Planeeringu andmestiku puhul vajab reeglina piirangut isiklik kontaktteave. Näiteks kui naaberkinnistu omanik on avaldanud kinnistu aadressist erineva postiaadressi või lisanud asutusega peetud kirjavahetuses oma e-posti aadressi, telefoninumbri vms, siis on võimalik sellele osale seada piirang AvTS-i § 35 lg 1 p 12 alusel. See tähendab, et teabele ei ole dokumendiregistri kaudu otseligipääsu ja teabenõude korral väljastatakse dokument ilma isikliku kontaktteabeta.

2. Kinnistu aadressiga seonduvat on selgitatud selle juhendi §-s 32.

3. Nagu juba öeldud selle juhendi § 31 lõikes 2: asutusel ja juriidilisel isikul ei ole eraelu, ta esindaja täidab tööülesandeid, ja ka see ei ole eraelu, seega nende suhtes piirangut rakendada ei saa.

4. Nagu juba öeldud selle juhendi §-s 30: pelgalt inimese nime vms üldandmete (sünniaeg, isikukood) sisaldumine või ka sellele nt isikukoodi lisamine ei saa olla piirangu aluseks.

§ 80. Millise avalikustamise näeb ette planeerimisseadus?³⁸

[Planeerimisseadus](#) näeb ette kohustuse avalikustada järgmine teave:

- a) üleriigilise-, maakonna, üld-, ja detailplaneeringutest, samuti riigi- ja kohaliku omavalitsuse eriplaneeringute kohta teabe avalikustamise planeeringu läbi viimise vältel planeeringu korraldaja veebilehel (näiteks § 15 lg 5, § 27 lg 11, § 57 lg 5 jt);
- b) keskkonnamõtjude strateegilise hindamise algatamisest või planeeringu algatamisest teavitamise ajalehes ja võrgulehel (§ 16 lg 3, § 28 lg 6, § 58 lg 5 ja 6 jt) ning puudutatud isikute teavitamise keskkonnamõtjude hindamise või planeeringu algatamisest (§ 16 lg 4, § 28 lg 7, § 58 lg 7 jt);

36 Avatud haldusmenetluse üldpõhimõtteid normib [haldusmenetluse seaduse](#) 3. peatükk.

37 Vt [maakatastriseadust](#) (§ 6) ja maakatastri [võrgupõhist infosüsteemi](#), samuti [kinnistusraamatuseadust](#) (10 ptk ja §-d 77¹⁴–77¹⁶) ja kinnistusraamatu [võrgupõhist infosüsteemi](#) ning [ehitusseadustik](#) (§ 58) ja ehitisregistri [võrgupõhist infosüsteemi](#).

38 Kuna 01.07.2015 kehtima hakanud planeerimisseadus ei sätesta enam planeerimise avalikustamise osas üldisi nõudeid, vaid vastavad nõuded on ära toodud iga planeeringu liigi all eraldi, siis ei kajasta eeltoodud loetelu kõiki avalikustamise nõuetele viitavaid paragrahve.

- c) planeeringu koostamise ajaks kehtestatud ajutisest ehituskeelust teatamise (§ 42 lg 5; § 79 lg 5, § 132 lg 6);
- d) väljapanekute ja avalike arutelude korraldamise ja sellest teavitamise (§-d 19 lg 4 ja 5, § 32 lg 4 ja 5, § 38 lg 4 ja 5 jt)
- e) planeeringu kehtestamisest teatamise ja nendega kohapeal tutvumise võimaldamise (§ 24 lg 3, § 50 lg 6 jt).
- f) avaliku väljapaneku ja avaliku arutelu tulemustest teavitamise (§ 24 lg 2, § 52 lg 1 jt);
- g) kinnistu omanike sundvõõrandamisest või sundvalduse seadmisest teatamise tähtkirjaga (§ 43 lg 2, § 77 lg 8, § 111 lg 2, § 128 lg 9).

Ruumilise arengu põhimõtete ja suundumuste kujundamiseks võib Rahandusministeerium anda juhendeid, mis avalikustatakse ministeeriumi veebilehel ([planeerimisseaduse § 7](#)).

§ 81. Milliseid piiranguid näeb ette planeerimisseadus?

1. Väljapanek, avalik arutelu ning suuliste ja kirjalike ettepanekute ja vastuväidete esitamine on avalik ehk avatud menetlus. Planeerimisseadus tagab kohapealse juurdepääsu materjalidele nii planeeringu koostamise ajal kui järel.
2. Seega saab kohapeal tutvuda ka kirjavahetuses sisalduva isikliku kontaktteabega ehk AvTS-i § 35 lg 1 p 12 alusel kehtestatud piiranguga teabega. Samas tuleb selline tutvumine fikseerida (AvTS-i § 39).
3. Puudutatud isikuid, kellele haldusorgan planeerimise alast kirjavahetust peab, on viisakas hoiatada, et nad arvestaksid avalikkusega. Avalikkusega peab arvestama ka planeeringu algataja.

§ 82. Kas ehitusprojekte saab küsida teabenõudega?

1. Ehitusprojekt on projekteerimise käigus koostatud ehitise või selle osa ehitamiseks ja kasutamiseks vajalike dokumentide kogum, mis sisaldab ehitamiseks ja asjakohasel juhul ka ehitise kasutamiseks ja korrashoiuks vajalikku teavet (§ 5).
2. [Autoriõiguse seaduse](#) § 4 lg 3 punkt 14 loeb autoriõigusega kaitstavaks teoseks:
 - a) arhitektuurne graafika (joonistused, eskiisid, skeemid, joonised, plaanid, projektid jm);
 - b) arhitektuuri- ja maastikuarhitektuuriteosed (hooned, rajatised, pargid, haljasalad jm).
3. Nõusolekuta ja autoritasu maksmiseta ei ole lubatud reprodutseerida arhitektuuri- ja maastikuarhitektuuriteoseid ehk ehitisi (sama seaduse § 18 lg 2 p 1).
4. Seadus ehitusprojektidega tutvumist ei keela, kuid sellise teabe taaskasutamisele saab seada piiranguid autoriõiguste kaitseks AvTS § 3¹ kohaselt. Tuleb arvestada, et autori nõusolekuta on arhitektuurset graafikat lubatud kasutada üksnes füüsilise isiku poolt isiklikul eesmärgil (autoriõiguse seaduse § 18) ning autoriõiguse seaduse §-s 19 sätestatud tingimustel teaduslikel, hariduslikel, informatsioonilistel ja õigusemõistmise eesmärkidel.

8. peatükk. Avaliku teabe taaskasutamine

§ 83. Mõisted

1. Taaskasutamise mõisted ja nõuded on Eesti avaliku teabe seadusse võetud üle avaliku sektori teabe direktiivist – täpsemalt [avaliku sektori valduses oleva teabe taaskasutamise direktiivist 2003/98/EÜ \(koos täiendustega 2013/37/EL\)](#).
2. „Taaskasutamine“ tähendab, et algselt ühel eesmärgil (avaliku ülesannete täitmisega) asutusse kogutud teave tehakse kättesaadavaks isikutele, kes kasutavad seda sama teavet hoopis teistel eesmärkidel, oma erahuvides (näiteks äriatel või heategevuslikel eesmärkidel). Teabevaldajate vaheline teabevahetus oma avalike ülesannete täitmiseks ei ole avaliku teabe taaskasutamine.
- 2¹. „Avaandmed“ kõigile avalikult vabalt kasutamiseks antud, veebist kättesaadavaid, masinloetavas formaadis toorandmeid ilma kasutamise-, patente- ja levitamiskiiranguteta.
3. „Masinloetavus“ tähendab, et digitaalne teave on piisavalt struktureeritud, nii et tarkvara suudab kergesti tuvastada, ära tunda ja välja lugeda, üksikuid faktiväiteid ja nende sisemist struktuuri. Selgitused masinloetavuse kohta leiata „[Eestiavaliku teabe masinloetava avalikustamise rohelistest raamatust](#)“. Selles selgitatakse (p 4.5.) masinloetavuse 5-tärni-skaalat, kus 1 tärn on kõige vähem ning 5 tärni kõige enam kasutajasõbralik. Näiteks ka tavalised, PDF ja DOC failid on masinloetavad, kuid ühe tärni tasemega.
4. „Avatud vorming“ on platvormist sõltumatu vorming. „[Veebide koosvõime raamistiku](#)“ kohaselt peab avaliku sektori asutuse võrgulehelt allalaetav dokument (nt ametijuhend, põhimäärus vms) olema vormingus, mida saab avada nii vabavaraga kui firmapõhise tarkvaraga (nt odf, pdf, png, svg, rtf, digiallkirjastatult BDOC või DDOC). Nende pakitud versioonid esitatakse ZIP-vormingus, Firmapõhiste vormingute (nt doc, xls, ppt) kasutamist välditakse.

§ 83¹. Millised on taaskasutamise piirangud?

1. Osa avalikust teabest tuleb aktiivselt avalikustada, võimalusel masinloetaval kujul ja avatud vormingus, teabevaldaja võrgulehel ([AvTS § 28 lg 1 ja § 29](#)). Seda teavet võib kas piiranguteta taaskasutada (juhise § 84) või võib taaskasutamine olla piiratud (juhise § 84¹).
- Aga ka teabenõude korras võidakse küsida teavet taaskasutamise eesmärgil (teabenõudja peab sellest teabevaldajat teavitama, AvTS § 14 lg 2¹). Sel juhul peab teabevaldaja samuti lähtuma AvTS §-st 3¹.
- Nimelt peab AvTS § 3¹ lg 3 kohaselt teabe taaskasutusse andmisel olema tagatud isiku eraelu puutumatus, autoriõiguste kaitse, riigi julgeoleku kaitse, ärisaladuse ja muu juurdepääsupiiranguga teabe kaitse. Seetõttu peabki teabevaldaja enne teabe taaskasutusse andmist (ükskõik kas siis võrgulehel avalikustamisel või taaskasutamise eesmärgil esitatud teabenõudele vastamisel) hindama teabe üldisele kasutamisele piirangute kehtestamise vajadust.
2. See kohustus kehtib seega kõigi teabevaldajate suhtes, mh hallatavad asutused nagu raamatukogud, muuseumid ja arhiivid ning avalikke ülesandeid täitvad äri- ja mittetulundusühingud, sihtasutused ja füüsilised isikud.

§ 84. Milline teave kuulub piiranguteta avalikustamisele taaskasutuseks?

1. Kehtetu 16.01.2016
- 1¹. AvTS § 28 lg 1 punktides 1-4, 7, 8, 10-13, 15-24, 26, 27, 31¹ ja 32² nimetatud teave loetakse avaandmeteks ja tuleb avalikustada masinloetaval kujul ja avatud vormingus ning tehakse üldsusele kättesaadavaks **taaskasutamise piiranguteta**.
2. Masinloetavusest või avatud vormingust võib kõrvale kalduda, kui masinloetavale kujule või avalikku vormingusse viimine ei ole võimalik või nõuaks ebaproportsionaalseid kulutusi ([AvTS § 3¹ lg 4](#)). Ilmselt ei ole masinloetavus ja avatud vorming võimalikud ega ka asjakohased näiteks paberkandjal teabe puhul, mille ka tavalisele digitaalkujule viimine nõuab ebaproportsionaalselt suuri pingutusi või ei ole üldse võimalik. Sellisel juhul võimaldab teabevaldaja juurdepääsu nende algkujul või mistahes muus vormis.

§ 84¹ Millisele teabe taaskasutamisele tuleb vajadusel seada piirangud?

1. AvTS § 28 lg 1 punktides 5, 6, 9, 14, 25, 28, 29, 31 (st ka dokumendiregistrid) ja 32 nimetatud teave tuleb teabevaldajal küll avalikustada masinloetaval kujul ja avatud vormingus veebilehel, kuid kogu see teave ei ole mõeldud piiramatuks taaskasutamiseks. Dokumendiregistrite osas vaata lisaks ka käesoleva juhise § 19¹.

2. Teabevaldaja peab AvTS § 3¹ lõigetest 5-8 tulenevalt välja selgitama, kas ja millisele osale sellest teabest:

- a) on seadusega kehtestatud juurdepääsupiirang (nt avaliku teabe seaduse § 35 alusel, maksukorralduse seaduse § 26 – maksusaladus jms);
- b) on juurdepääs piiratud muul seaduses sätestatud viisil – nt juurdepääs üksnes õigustatud huvi korral (rahvastikuregister) või on juurdepääsuks ette nähtud muud eritingimused (nt kohtumenetluses toimikuga tutvumise kord menetlusseadustikus);
- c) või kas teave sisaldab isikuandmeid.

3. Kui vastus on jaatav, siis reeglid:

- a) juurdepääsupiiranguga teavet ei avalikustata ega anta ka muul viisil üldiseks kasutamiseks;
- b) ülejäänud osa teabest võib anda taaskasutamiseks, kui seeläbi ei kaasne juurdepääsupiiranguga teabe avalikuks tuleku ohtu ega kahjustata oluliselt isiku eraelu puutumatus (mõjude hindamise kohta loe käesoleva juhendi §-st 91);
- c) taaskasutamiseks antav teave tuleb avalikustada avaandmetele ette nähtud reeglite kohaselt (st võimaluse korral masinloetaval kujul ja avatud vormingus (AvTS § 31 lg 4), kuid taaskasutamisele võib seada piiranguid (AvTS § 3¹ lõiked 7-9), loe täpsemalt käesoleva juhendi §-st 92.

4. Andmekogude juurdepääsupiiranguta andmed kuuluvad samuti avalikustamisele (AvTS § 28 lg 1 p 30 ja § 29 lg 5), kuid ka nende puhul tuleb läbi viia eelpoolkirjeldatud hindamine. Teave, mis selle hindamise kohaselt otsustatakse anda üldiseks kasutamiseks, tuleb võimalusel teha kättesaadavaks ajakohasena ning viisil ja vormis, mis võimaldab avaandmed alla laadida tervikliku andmekogumina koos metaandmetega masinloetaval kujul ning avatud vormingus. Andmekogu kohta loe täiendavaid selgitusi juhise järgmisest §-st.

§ 84² Kas dokumendiregistrid peavad olema masinloetaval kujul tervikuna allalaetavad?

(Kehtetu 16.01.2016 vt § 19¹ ja 84¹)

§ 85. Kust leida tehnilisi selgitusi?

(kehtetu märts 2016)

§ 86 Kellele ja kus kehtib masinloetava avalikustamise kohustus?

(kehtetu märts 2016)

§ 87. Mis on andmekogu?

1. Nagu öeldud, kuuluvad andmekogude juurdepääsupiiranguta andmed avalikustamisele tervikliku andmekogumina koos metaandmetega masinloetaval kujul ning avatud vormingus.

2. Kuid mitte igasugune avalikku teavet sisaldav infosüsteem ei ole seaduse mõttes andmekogu. Infosüsteem on tehniline mõiste. Sellega tähistatakse korrastatud andmehulki. Ka perfokaartide kataloog, exceli tabel ja võrguleht on iseenesest infosüsteemid.

3. Andmekogu on õigusliku tähendusega mõiste. Andmekogu on selline infosüsteem, mille asutamiseks:

- a) seadusandja on väljendanud oma tahet – kas otse seadusega või seaduses sisalduva volitusnormiga;
- b) kohalik omavalitsus on seadusega reguleerimata kohaliku elu küsimuses kasutanud oma enesekorraldusõigust ja asutanud enda andmekogu (kohaliku omavalitsuse korralduse seaduse § 6 lg 3 p 2).³⁹

³⁹ Omavalitsuse võimalus asutada sel alusel isikuandmeid sisaldavaid andmekogusid on piiratud. Igasugune isikuandmete töötlemine on iseenesest eraelu riive. Põhiõiguste tuntav riive (näiteks isiklike kontaktandmete

4. Lähemalt on andmekogude mõistet selgitatud Andmekaitse Inspeksiooni [andmekogude juhendis](#).
5. Seega ilma andmekogu staatusega infosüsteemi andmete avalikustamine on teabevaldajale kohustuslik niivõrd, kui võrd infosüsteem sisaldab võrgulehel avaldamisele kuuluvad andmeid.
6. Uute andmekogude avaandmed peavad olema masinloetavad ja tervikuna allalaetavad algusest peale. Masinloetavuse nõue jõustus 29.12.2012. Varem asutatud andmekogude täiendavalt töötlemata avaandmetele tagatakse masinloetav juurdepääs hiljemalt 01.02.2016 (vt [AvTS § 58²](#)).
7. Andmekogu avaandmed peavad olema juurdepääsetavad [Eesti teabevärava](#) kaudu. Piisav on sinna linkimine (võrguaadress ei pea tingimata sisaldama osist „eesti.ee“, kuid § 29 lg 6 peab silmas Eesti teabeväravat, mitte muid portaale).

§ 88. Kas võib masinloetavana avalikustada lisa-andmeid, mida seadus ei nimeta?

(Kehtetu alates 16.01.2016)

§ 89. Mis on isikuandmete taaskasutamisel õiguslik alus?

(Kehtetu alates 16.01.2016)

§ 90. Kas juurdepääs isikuandmetele tuleb tagada kiirel ja hõlpsal viisil?

(Kehtetu 16.01.2016)

§ 91. Mida peaks arvestama eraelu riive mõjude hindamisel?

1. Enne isikuandmeid sisaldada võiva teabe taaskasutusse andmist tuleb teabevaldajatel viia läbi eraelu riive mõjude hindamine. Seda nii seniste andmete kättesaadavaks tegemisel kui uute infosüsteemide loomisel ja e-teenuste kavandamisel (AvTS § 29 lg 4 ja 5).
2. Mõjude hindamisel tuleb üle vaadata avalikustamise õiguslik alus. Teabevaldaja peab teadma, milliseid isikuandmeid millise õigusnormi alusel ta masinloetavasse taaskasutusse lülitab. Lisaks AvTS-le võivad eriseadused kehtestada täiendavaid lubavaid või keelavaid erisusi, sh välistada massipäringud. Näiteks [karistusregistrisse on lubatud vaid üksikpäringud](#), seega jääb masinloetav avalikustamine koos tervikuna allalaetavusega ära.
3. Mõjude hindamisel tuleb üle vaadata, kas avalikustamine vastab isikuandmete töötlemisel kehtivale minimaalsuse põhimõttele. Seda nii sisulise ulatuse kui ka ajalise ulatuse osas. Teavet, mis on vananenud või mille avalikustamise tähtaeg on ületanud, ei tohi enam kättesaadavana hoida – eriti isikuandmeid. Vajadusel tuleb säilitus- ja avalikustamistähtjad üle vaadata.
4. Lisaks minimaalsuspõhimõttele tuleb hinnata, ega kiiresti vananeva ja muutliku teabe juures teki madala andmekvaliteedi tõttu inimeste õiguste kahjustamise ohtu. Näiteks kohtuistungite teave, kohtu- ja kohtutäiturikutsed ning muud Ametlikes Teadannetes avaldatavad teated võivad näidata inimesi süüdi- või võlguolevatena, mis aga hilisemas menetluses ei pruugi tõeks osutada.
5. Inimeste jälgimis- ja jälitamisvõimaluste loomine masinloetava taaskasutuse kaudu on pigem hüpoteetiline. See võimalus võib siiski tekkida, kui avalikustada avaliku sektori töötajate või teenuseosutajate tulevast täpset paiknemisinfot.
6. Kõige laiem risk on võimalus, et suur arv inimesi muutub kerge vaevaga profileeritavaks – taaskasutusse saadud teavet töödeldakse tarbimis-, valimis- vms eelistuste kaardistamiseks.
7. Samuti tuleb arvestada mosaiigiefektiga. Masinloetav andmetöötlus võimaldab kokku segada erinevaid infokilde niihästi avalikust sektorist, ühis- ehk sotsiaalmeediast kui mujalt – näiteks inimeste harjumisi koos nende kontaktandmetega. On taunitav, kui inimesi häiritakse soovimatute pakkumistega, kasutades teavet, mida avalik sektor on nende kohta kogunud. Inimese enda teadmata võivad tekkida kaardi- või reitingurakendused, kus ta on nimeliselt või vähemalt äratuntavalt tuvastatav.

avaldamine, tundlike või häbistavate andmete kogumine jne) peab olema kindlasti sätestatud seaduses. See ei saa olla tuletatud omavalitsuse õigusest otsustada kohaliku elu küsimusi, mis ei ole seadusega antud kellegi teise otsustada.

8. Lisaks suunatud ja isikustatud reklaamile võimaldab profileerimine ilma inimeste endi teadmata hinnapõhist diskrimineerimist (lahterdamine, kes oleks nõus või võimeline kõrgemat hinda maksma). Inimkäitumise profileerimine võimaldab koguda andmeid kindlustusmaksete tõusuks või kindlustusest keeldumiseks.

9. Halvimal juhul võib inimese teadmata toimuv profileerimine viia identiteedivarguseni ja vara omastamiseni.

10. Riskide hindamisel ei saa arvestada tavapärase taaskasutajatega. Juurdepääsupiiranguta avalikule teabele peab juurde pääsema igaüks ilma kasutuse eesmärki põhjendamata või täpsemalt: ilma kasutuse eesmärki avaldamata. Näiteks võivad mingi andmekogu tavakasutajad olla jäätmekäitlusettevõtted, kellel on eraelu mitte riivav kindel kasutuseesmärk. Andmekogule juurdepääsu võimaldamisel ei tohi aga teisi kasutajaid diskrimineerida – masinloetavat avalikustamist peavad siis saama samamoodi kasutada ka otseturustusettevõtted, kellel on hoopis teistsugune eesmärk.

11. Samuti saab mõjude hindamisel vaadata, mis on sisulise tähenduseta abiandmed, mida ei ole vaja taaskasutusse anda, kuna see vaid koormab andmestikku ülearusega. Tihti on ülearuseks teabeks andmekogudesse sissekanded teinud töötajate nimed (nt kohturegistris kohtunikuabi ja sekretäri nimed).

§ 92. Mida eraelu riive mõjude hindamise põhjal otsustada?

1. Mõjude hindamise tulemusena saab teabevaldaja otsustada:

- a) anda isikuandmed taaskasutusse koos muude andmetega, kuna eraelu riive on ebaoluline;
- b) anda isikuandmed taaskasutusse, kuna avalikustamine on seaduslik kohustus, kuid kohaldada muu teabega võrreldes vähem kasutajasõbralikumat lahendust;
- c) mitte võimaldada andmekogus ja/või asutuse võrgulehel isikuandmete kättesaadavust nn veebirobotitel – isegi kui samade andmete saamiseks teabenõude korras (üksikpäringuna) piirangut ei ole. Näiteks kasutades selleks captcha tehnoloogiat.
- d) anda teave masinloetavas taaskasutusse, kuid enne umbisikustada (anonümiseerida) selles olevad isikuandmed. Seda saab loomulikult kasutada siis, kui selliselt töödeldud teave säilitab taaskasutamiseks oma väärtuse. Kui inimene ei ole tuvastatav, siis seadus ei loe vastavat teavet isikuandmeteks ning ka juurdepääsupiiranguid seada ei ole vaja. Arvestada tuleb aga eri allikate kokkusegamisvõimalusi (mosaiigiefekti) – seetõttu peaks teabevaldaja pärast umbisikustamist tegema aimatavuskatseid. Kui teave on otsustatud umbisikustada, siis seda peab tegema teabevaldaja ise, seda ei saa teha taaskasutaja ülesandeks.

2. Samuti peaks teabevaldaja hindama, kas masinloetava avalikustamise osas on otstarbekas anda taaskasutajaile tehnilisi juhtnööre. Mõistlik on lisada ka hoiatus, et taaskasutamisel ei rikutaks [elektroonilise side seaduse § 103¹](#) ja [IKS § 12 lõike 5](#), samuti [IKS §-de 17-21](#) nõudeid.

3. Koos mõjude hindamisega peaks teabevaldaja üle vaatama ka oma võrgulehel avaldatavad isikuandmete töötlemise selgitused (privaatsuspoliitika, [AvTS § 28 lg 1 p 31¹](#)) – kas see arvestab masinloetava avalikustamisega. Nimetatud selgitused võiksid sisaldada ka viidet sellele, et õigus enda andmetega tutvuda ja muud [IKS §-des 17-21](#) tagatud õigused kehtivad edasi ka taaskasutusse läinud isikuandmetele.

4. Andmekogude avalikkust käsitlevad sätted pärinevad tihti üksikpäringute ajast, mil tervikuna masinloetaval kujul allalaadimist ette ei kujutatud. Seetõttu peaks teabevaldaja vaatama oma andmekogude kohta käivaid õigusakte ka selle pilguga, et kas nad ei vaja uutes oludes varasest tugevamat eraelu riivet pehmemdavaid muudatusi.

9. peatükk. Riigihangete avalikkus ja piirangud

§ 93. Miks peavad olema riigihanked läbipaistvad?

Riigihangete korras teenuste ja kaupade tellimise eesmärgiks on tagada hankija rahaliste vahendite läbipaistev ja säästlik kasutamine.

Riigihanked peavad olema läbipaistavad kahel põhjusel:

- a) et tellijaks olev hankija ei eelistaks üht pakkujat teisele või tegutseks omavoliliselt, millega võib kaasneda eelarveliste vahendite ebaratsionaalne kasutus.
- b) et tagada pakkujate võrdne kohtlemine - see tähendab, et välistatud peaksid olema olukorrad, kus hankija põhjendamatult üht pakkujat teistele eelistab. Et seda vältida, selleks peavad olema hankedokumentid kõigile pakkujatele varakult ja võrdsetel tingimustel kättesaadavad.⁴⁰

§ 94. Millised dokumendid on hankemenetluses piiranguga?

1. Riigihangete seaduse kohaselt on konfidentsiaalne ainult pakkumus (RHS § 43 lg 4). See tähendab eelkõige seda, et pakkumused edastatakse reeglina suletult ning neile ei ole kellelgi, sh ka hankijatel, juurdepääsu enne pakkumiste avamist.

Pakkumuste avamisel peab hankija võimaldama pakkujatel või nende volitatud esindajatel viibida pakkumuste avamise juures (RHS § 46 lg 4). Hankija koostab pakkumuste avamise protokoll, kuhu kantakse pakkujate nimed, registrikoodid ja esitatud pakkumuste maksumused, sealhulgas pakkumuste osamaksumused, kui neid arvestatakse pakkumuste hindamisel, ning muude pakkumuste hindamise kriteeriumitele vastavate pakkumust iseloomustavate numbriliste näitajate väärtused. Hankija ei avalikusta pakkumuste avamisel pakkumuste sisu osas, mis rikuks pakkujate ärisaladust või kahjustaks nendevahelist konkurentsi. Pärast pakkumuste avamist on pakkumused täies mahus kättesaadavad ainult hankijatele.

2. Seega ei saa pakkuja nimi ja pakkumuse maksumus olla peale pakkumuste avamist konfidentsiaalsed ehk piiranguga teave. Pakkuja saab vastava teabe küsida välja ka avaliku teabe seaduse alusel teabenõude kaudu. Hankija võib jätta pakkujale protokoll osaliselt väljastamata, kui see sisaldab ärisaladust või muud avalikustamisele mittekuuluvat teavet.

3. Pakkumusi tuleb pakkumustena käsitleda riigihangete seaduse § 43 lg 4 mõistes kuni lepingu sõlmimiseni või hankedokumentides määratud pakkumuse jõusoleku minimaalse tähtaja lõppemiseni, mis tähendab, et hankemenetluse käigus ei saa pakkumuste sisu osas esitada teabenõudeid. Kuna riigihangete seadus sätestab nõuded ainult hankemenetluse raames (hankemenetluse lõppemise alused on ära toodud RHS § 29 lg 3), siis peale hankemenetluse lõppemist RHS § 43 lg 4 olevat piirangut enam rakendada ei saa, sest peale hankemenetluse lõppu riigihangete seadus ei kohaldu.

Eeltoodu ei tähenda aga seda, et kõik pakkumused muutuksid peale hankemenetluse lõppu automaatselt avalikus, vaid edaspidi tuleks piirangute kehtestamisel lähtuda pakkumuste sisust. Seega peab ka peale hankemenetluse lõppu hankija kaitsma pakkuja edastatud konfidentsiaalset teavet, mis puudutab eelkõige tehnika- või ärisaladusi või ka muud piiranguga teavet. Et hankijal oleks arusaadav, millist teavet peavad pakkujad oma pakkumusteks konfidentsiaalseks, peaks hankijad hankedokumentidesse kirjutama nõude, et pakkumustes tuleb ära näidata, milline teave ja mis põhjusel on konfidentsiaalne.

4. Eeltoodu ei laine täies ulatuses lihthangetele. Kuna lihthangete korral ei koostata pakkumuste avamise protokoll, siis saab hankemenetluse jooksul küsida teavet ainult RHS § 54 sätestatud juhul ja korras. RHS § 54 lg 2 p 3 näeb pakkujatele, kelle pakkumus on tunnistatud hankija poolt vastavaks, hankemenetluse käigus ette võimaluse esitada hankijale taotluse saamiseks hankijalt teada eduka pakkumuse eeliseid võrreldes pakkuja pakkumusega. Taotluse saamisega on hankija kohustatud

40 Võrdse kohtlemise põhimõtte tähendab ka kohustust tagada läbipaistvus, et võimaldada kontrollida selle põhimõtte järgimist, on öelnud ka Euroopa Kohus (18. juuni 2002. aasta otsus kohtuasjas [C- 92/00](#); HI, EKL 2002, lk I-5553, punkt 45, ja 12. detsembri 2002. aasta otsus kohtuasjas [C-470/99](#) : Universale-Bau jt, EKL 2002, lk I-11617, punkt 91).

väljastama edukat pakkumust iseloomustavad andmed ja selle eelised tema pakkumusega võrreldes ning edukaks tunnistatud pakkumuse esitanud pakkuja või pakkujate nimed.

Lihthangetes tehtud otsustest teavitamisel lähtub hankija RHS §-des 54 ja 55 sätestatust. Otsustest teavitamisel peab hankija tavapäraselt järgima, et ta ei avaldaks konfidentsiaalset teavet, nt ärisaladust.

§ 95. Kas kvalifitseerimisdokumendid on pakkumuse osa?⁴¹

Pakkumus ja kvalifitseerimisdokumendid on oma olemuselt erinevad. Seega ei laiene kvalifitseerimisdokumentidele konfidentsiaalsuse nõue. Nende avalikustamisel teistele pakkujatele või väljastamisel teabenõude korras tuleb aga jälgida, et ei avalikustataks neis sisalduda võivat piiranguga teavet (näiteks ärisaladust, vt § 33).

Samuti on Euroopa Kohus leidnud kohtuasjas nr [C-450/06](#), et tulenevalt ausast konkurentsist on oluline, et hankijad ei avaldaks hankemenetluses saadud teavet, mille sisu võidakse kasutada konkurentsi kahjustamiseks, ei käimasolevas menetluses ega ka hilisemates hankemenetlustes.⁴² Juhul, kui dokumentide esitaja on määratlenud need osad dokumentidest, mis sisaldavad ärisaladust või muud piiranguga teavet, tuleb hankijal need osad katta või muuta loetamatuks enne dokumentide soovijale edastamist.⁴³

§ 96. Kas riigihanke tulemusena sõlmitud lepingutele saab kehtestada juurdepääsupiirangut?

1. Lepingutes, sh ka hankelepingutes, konfidentsiaalsuskokkulepete sõlmimist piirab seadus (AvTS). Nimelt saavad teabevaldajad kehtestada dokumentidele, sh ka hankelepingutele, juurdepääsupiirangu üksnes juhul, kui selleks on seadust tulenev alus. Seega saab hankija lepingu teise poolega (hankemenetluse võitjaga) konfidentsiaalsuskokkuleppeid sõlmida üksnes niivõrd, kuivõrd selleks annab õiguse AvTS-st või eriseadusest tulenev konkreetne juurdepääsupiirangu alus. Sellisele seisukohale on asunud ka Tallinna Ringkonnakohus kohtuasjas nr [3-08-1980](#).

2. Samas tuleb pöörata tähelepanu ka asjaolule, et riigihangete läbiviimiseks kasutatakse reeglina ka avalikku raha. Nimelt sätestab AvTS § 36 lg 1 p 9, et teabevaldajad ei tohi tunnistada asutusesiseseks kasutamiseks dokumente eelarvevahendite kasutamise kohta ja punktist 10 tulenevalt ka andmeid teabevaldaja varaliste kohutuste kohta. See kinnitab veelkord, et hankeleping ei saa olla täies ulatuses piiranguga.

3. Kui lepingus siiski sisaldub kaitsmist vajav teave, näiteks ärisaladus või tehnoloogiliste lahenduste kirjeldus, ei muuda see lepingut täies ulatuses konfidentsiaalseks. Juurdepääsupiirang (näiteks AvTS § 35 lg 1 punktid 17 ja 10) tulebki sel juhul kehtestada üksnes sellele osale lepingust, mis vastavat teavet sisaldab. Ärisaladuse puhul tuleb vajadusel seda ka põhjendada (täiendavalt vaata ka § 33). Lepingus peavad olema kindlasti avalikud lepingu pooled, lepingu ese ja lepingu maksumus.

4. Praktikas võib lepingule olla lisatud ka hankemenetluses esitatud pakkumus, millest osa andmeid võib kajastada omakorda ka lepingus. Sellisel juhul saab lepingule lisatud pakkumuses olla konfidentsiaalne teave, mis sisaldab pakkuja ärisaladust või muud teavet, mis kahjustaks ettevõtete vahelist konkurentsi. Seega ei saa lepingu lisaks oleva pakkumuse piirangu alus olla enam RHS § 43 lg 4. Eeltoodu ei tähenda seda, et lepingu lisatud pakkumus ei või sisaldada piiranguga teavet, kuid sellisel juhul saab piirangu kehtestada kas AvTS-st või mõnest eriseadusest tuleneval alusel, juhul kui pakkumus sellist teavet sisaldab.

41 <https://riigihanked.riik.ee/lr1/web/guest/pakkumus>

42 Euroopa Kohtu 14. veebruar 2008. a otsus kohtuasjas C-450/06: Varec SA, punktid 33,34.

43 https://riigihanked.riik.ee/lr1/c/document_library/get_file?p_l_id=15617&folderId=431009&name=DLFE-32501.pdf

10. peatükk. Juurdepääsupiiranguga teabe kaitse

§ 97. Kas avalikku teavet, millel ei ole juurdepääsupiiranguid, peab ka kaitsma?

1. Asutus peab kaitsma enda valduses olevat avalikku teavet igal juhul. Seda sõltumata sellest, kas teave on piiranguga või piiranguta, paberil või elektrooniline, isikuandmetega või isikuandmeteta, andmekogusse kuuluv või andmekogu-väline.
2. Mistahes avaliku teabe puhul peab asutus tagama selle:
 - a) käideldavuse – et teave on õigeaegselt ja hõlpsalt kättesaadav selleks volitatud isikule või tehnilisele vahendile;
 - b) tervikluse – et teave on õige ja täielik ja seda ei ole volitamata muudetud;
 - c) konfidentsiaalsuse – et teavet saavad kasutada ainult selleks volitatud isikud või tehnilised vahendid.
3. Kõige selle tagamiseks peab teabevaldaja rakendama organisatsioonilisi, füüsilisi ja infotehnilisi kaitsemeetmeid. Sellise kohustuse paneb asutustele AvTS § 43 lg 1-2.⁴⁴

§ 98. Miks jagada piiranguga teavet erinevatesse järkudesse?

1. Piiranguga teave asutuses võib olla üpris erineva tundlikkusega. Näiteks kirjavahetus kodanikega on alati piiranguga. Isegi kui kirja sisu ei vaja juurdepääsupiirangut, siis kodaniku isiklikud kontaktandmed ei ole avalikud (piirang AvTS § 35 lg 1 p 12 alusel). Kuid kas kodanikega peetavale kirjavahetusele peaks kohaldama ka asutuse-siseselt piiranguid – nii et ligipääs dokumendisarijale või koguni dokumendile võimaldatakse üksnes neile, kel on konkreetne tööalane vajadus? Kas selliseid kirju peaks enne väljasaatmist krüptima? Niisuguste turvameetmete lai kasutamine aeglustab asutuse töökiirust, suurendab töökoormust, põhjustab lisakulusid. Tavalise kirjavahetuse suhtes oleks see ebamõistlik.
2. Suurem osa piiranguga teabest on reeglina selline, mille puhul piisab, kui:
 - a) asutuse sees pääsevad sellele ligi need, kes tavaliselt pääsevad dokumendiregistrisse,
 - b) e-postiga saadetakse krüptimata e-kirju ning paberposti puhul lihtkirju (mitte tähitud kirju).
3. Kuid osa piiranguga teabest võib olla eriti tundlik, näiteks:
 - a) lastekaitse alased materjalid või vähemalt osa neist,
 - b) lapsendamissaladust sisaldavad materjalid,
 - c) soovahetuse materjalid,
 - d) diplomaatiliste kohtumiste ja Euroopa Liidu töörühmade memod või vähemalt osa neist,
 - e) ettevõtete ja asutuste turvameetmete kirjeldused, mille leke toob kaasa suuri kulutusi.
4. Kõige lihtsam ja hõlpsam viis on eristada turvameetmete kohaldamisel:
 - a) tavalist piiranguga teavet ning
 - b) eriti tundlikku teavet.

Piiranguga teabe järkudeks jagamine võimaldab rakendada keerukamaid ja kulukamaid meetmeid üksnes selle suhtes, mis tõesti tõhusamat kaitset vajab.

5. Järkudeks jagamise vajaduse kindlakstegemine on lihtne. Te peaksite eristama eriti tundlikku piiranguga teavet, kui leiate, et:

- a) osale teabele tuleks ka asutuse sees juurdepääsu piirata nii, et igaüks, kes näeb dokumendiregistri asutuse-sisest vaadet, seda teavet siiski ei näeks;
- b) osa teabe puhul peab kindlalt välistama lekkeriski kirja saatmisel ning võimaluse, et aadressaadi kodakondsed saavad aadressaadile saadetud lihtkirja või krüptimata e-kirja lugeda.
- c) teave esineb suure hulganäht, nt dokument sisaldab väga paljude inimeste andmeid.

Näiteks inimeste nimed ja isiklikud kontaktandmed ühes konkreetnes dokumendis võivad olla tavaline piiranguga teave (AvTS § 35 lg 1 p 12 piirang). Kui aga asutuses on digitaalandmestik, mis sisaldab kümme tuhat nime koos kontaktandmetega? Ning kui asutuse tegevusvaldkond või dokumendisari võimaldab anda andmetele lisatähendusi isikute profileerimiseks (näiteks teatud liiki haiguste põdejad või teatud ravimit vajavad isikud Haigekassas)? Selline andmestik võib kogumis olla eriti tundlik teave, mis vajab tugevamat

⁴⁴ Isikuandmeid sisaldava teabe puhul annab IKS § 25 põhjalikumad, kuid üldjoontes samad nõuded.

kaitset.

6. Mõnda liiki avaliku teabe – andmekogude, elutähtsate elektrooniliste teenuste ning valitsusasutuste andmestiku – turvameetmete kohta on täiendavaid õigusakte ning meetmete katalooge. Sellest lähemalt järgmistes paragrahvides.

§ 99. Milliseid turvameetmeid peab rakendama andmekogude kaitseks?

1. Avalik teave hõlmab ka andmekogusid. Inspektsioon on selle kohta, kuidas eristada infosüsteeme (tehniline mõiste) ja andmekogusid (juriidiline mõiste), andnud [eraldi juhendi](#).
2. Riigi ja omavalitsuste andmekogudes peab rakendama [Vabariigi Valitsuse määrusega](#) kehtestatud infosüsteemide kolmeastmelist etalonturbe süsteemi (ISKE).⁴⁵ Seda haldab [Riigi Infosüsteemi Amet](#).
3. [ISKE-t tuleb rakendada ka andmekogu staatusega infosüsteemide suhtes, kui nad on ühendatud x-teeaga](#) (riigi infosüsteemi andmevahetuskihiga).⁴⁶
4. Kuigi ISKE on iseenesest mahukas kataloog, ei ole seda keeruline kasutada. Andmekogu pidaja korraldab turvaanalüüsi, hinnates ära riskid ning määratledes turvaklassi. Turvaanalüüsi põhjal valib ta kataloogist kohased turbemeetmed.⁴⁷ ISKE sisaldab meetmeid nii suure digitaalse registri kui ka perfokaartidel peetava lihtsa andmestiku jaoks. ISKE rakendamisel keerulisemates andmekogudes tuleks siiski kasutada professionaalse asjatundja abi.
5. Andmekogu turvasemest sõltub ka kohustusliku andmeturbeauditi sagedus: vastavalt 2 aasta (kõrge tase), 3 aasta (keskmine tase) või 4 aasta (madal tase) järel (vt [Vabariigi Valitsuse määrus](#)).
6. ISKE mõjutab ka sellise teabe kaitset, mis andmekogusse ei kuulu. Ilmselt suur osa füüsilistest ja osa organisatsioonilistest turvameetmetest, mida asutuses andmekogu pidamiseks rakendatakse, mõjutab ka asutuses oleva ülejäänud teabe kaitset. Lisaks juhenduvad ISKE-st valitsusasutused oma infoturbe korraldamisel – sõltumata sellest, kas nad peavad andmekogusid või mitte (valitsuse [15.03.2012 määrus nr 26 „Infoturbe juhtimise süsteem“](#)).

§ 100. Millal rakendada ISO standardeid ja kas nad asendavad ISKE-t?

1. Andmeturbe korraldamisel võib kohaldada ka Rahvusvahelise Standardiorganisatsiooni (ISO) standardeid. Andmeturbe standardid algavad seerianumbriga 2700. Selle kohta vt [Eesti Standardikeskuse](#) teavet.
2. Nii ISKE kui ISO standardid tagavad andmeturbe alal sarnase lõpptulemuse. Kuid ISO standardite rakendamine on keerulisem, sest nad põhinevad tööprotsesside kirjeldusel (ISKE lähtub infovara kirjeldusest, mis on lihtsam). Ka väline auditeerimine on ISO standardite puhul reeglina kallim kui ISKE puhul.
3. Seega ISO standardid on rakendamisel keerulisemad ja kallimad kui ISKE. Neid on mõistlik kasutada siis, kui vahetate tundlikku teavet välismaiste koostööpartneritega ning partnerite vahel peab olema suur vastastikune usaldus. ISO standardeid ja nende auditeid tuntakse kogu maailmas.

<i>ISO standardi rakendamine ei vabasta andmekogu pidajat ISKE-kohustusest. ISKE on seaduslik kohustus, ISO standardid on vabatahtlik valik.</i>
--

§ 101. Millised erinõuded kehtivad valitsusasutustele?

1. Vabariigi Valitsus kehtestas [15.03.2012 määrusega nr 26 „Infoturbe juhtimise süsteem“](#) valitsusasutustele infoturbe alal ühtsed alusnõuded.

⁴⁵ Turvameetmete süsteemi rakendamist riigi ja omavalitsuste andmekogudes nõuab AvTS § 43.9.

⁴⁶ Seda nõuab [Vabariigi Valitsuse 24.04.2008 määruse nr 78 „Infosüsteemide andmevahetuskiht“](#) § 19.

⁴⁷ Turvaanalüüsi koostamist nõuab [Vabariigi Valitsuse 20.12.2007 määruse nr 252 „Infosüsteemide turvameetmete süsteem“](#) 2. ptk.

2. Määrus paneb valitsusasutuse juhile (ministeeriumis kantslerile) infoturbe alase vastutuse ja ülesanded. Määrus nõuab samuti, et asutuses määrataks infoturbejuht (kes võib olla korraga mitmes asutuses), ning sätestab tema ülesanded. Muuhulgas peab asutuse juht:

- a) vähemalt kord aastas kinnitama infoturbejuhi koostatud infoturbe raporti riskide kohta ja järgmise aasta riskide maandamise tegevuskava;
- b) kehtestama oma asutuses ning asutuse hallatavates riigiasutustes infoturbe alased juhised (infoturbepoliitika).

3. Infoturbepoliitikaga tuleks muuhulgas kindlaks määrata:

- a) asutuse infoturbe alane tööjaotus;
- b) asutuse infovarade eest vastutajad;
- c) infole juurdepääsuõiguste haldamine;
- d) reeglid kasutajate isiklike e-seadmete tööalaseks kasutamiseks, tööandja seadmete kasutamiseks väljaspool töökohta ning kaugtöö korraldamiseks;
- f) infoturbeintsidentide käsitlemise reeglid, sh asutuse arvutivõrgu ja infosüsteemide väärkasutuse järelmid;
- g) konfidentsiaalkohustuse reeglid.

4. Oluline on, et infoturvet (sealhulgas piiranguga teabe kaitset) võetakse kogu asutuse asjana, mitte IT- või infoturbeüksuse eralõbuna. Infoturbepoliitika tuleb siduda asutuse kogu töökorraldusega. Selle koostamisel ja rakendamisel peavad kindlasti osalema asutuse juhtkond, asjaajamisüksus ja juristid.

5. Infoturbe eesmärgid tuleb lõimida ka asutuse teistesse sisedokumentidesse (sisekorraeskiri, asjaajamiskord jne). Näiteks dokumendihaldusele juurdepääsu reeglid asjaajamiskorras on osaks infoturbepoliitikas ettenähtud pääsuõiguste haldamise reeglistikust.

6. Sõltumata sellest, kas asutus peab andmekogusid või mitte, viitab määrus vajadusele üldiselt juhinduda ISKE-st (§ 1 lg 2).

7. Asjakohased dokumendinäidised on Riigi Infosüsteemi Ameti võrgulehel.

§ 102. Mis on kõige elementaarsemad organisatsioonilised turvameetmed?

1. Kõige elementaarsem ja üldisem organisatsiooniline ehk töökorralduslik abinõu teabe kaitseks on võimalikult täpne vastutuse paikapanek tööprotsesside eest.

2. Pääsuõiguste haldamine (nii ruumidesse kui infosüsteemidesse) peab katma ametnikke, töötajaid ja koostööpartnereid kogu (koos)töötsükli jooksul – (koos)töösuhte tekkimisest kuni lõppemiseni. Külalisi ei tohi seal, kus on füüsiline juurdepääs piiranguga teabele, üksi jätta.

3. Kui piiranguga teabe saladuses hoidmise kohustus ei tulene seadusest (näiteks ametnikel avaliku teenistuse seaduse §-st 55), tuleb see katta lepingutega.

4. Isikuandmete kaitse seadus paneb isikuandmete töötlejale kohustuse pidada infovarade arvestust, dokumenteerides andmetöötlusprotsessis osalevad seadmed ja tarkvara (vt ka AKI varasemat [juhust](#))

5. Asutuse infoturbepoliitika, asjaajamiskord ja muud sisedokumendid võivad olla täiuseni lihvitud, aga neist ei ole kasu, kui personal ei ole saanud koolitust ega ole nõuetest teadlik.

§ 103. Mis on kõige elementaarsemad füüsilised turvameetmed?

1. Kõige raskemate tagajärgedega riskid nii paber- kui digitaalteabele on tulekahju ja uputus. Esimesena tuleb mõelda nende vastaste meetmete peale. Ruumid ja seadmed peavad olema kaitstud tule, vee, ülekuumenemise ja voolukõikumiste eest.

2. Füüsilise juurdepääsu piiramine ruumidesse ning teabe töötlemise ja hoidmise kohtadesse on teine meetmete rühm. See algab uste lukustamisega ning võtmete/pääsukaartide haldamisega. Igaüks asutuses ei peaks saama igäühe ruume avada – vastutus hajub. Eriti tundliku teabe puhul kasutage lukustatud kappe ja sahtleid.

3. Töökoha asend, seadmete ja paberite füüsiline paigutus peab tagama, et kõrvaliste isikute pilk liigselt uidata ei saaks, rääkimata millegi märkamatus kaasavõtmisest. Seda saab täiendada infotehnilise meetmega – arvuti ekraanilukuga.

4. Piiranguga teavet sisaldavad paberid tuleb hävitada nõuetekohase, sobiliku peenestusastmega paberipurustajas või põletada.
5. Iga kontoritöötaja teab, et enamik saladusi lekib tavaliselt printeri juures. Kui asutuses on eriti tundlikku infot, siis tuleks selle puhul kasutada kas füüsilist meetet (füüsiline ligipääs printerile vaid volitatud isikuile) või infotehnilist meetet (printer trükitab välja selle ametniku/töötaja paberid, kes ennast konkreetse töövoo juures tellijana tuvastab).

§ 104. Mis on kõige elementaarsemad infotehnilised turvameetmed?

1. Digitaalteabe hävimise eest kaitstakse varukoopiate tegemisega.
2. Digitaalteabe kasutajad peavad olema nimeliselt tuvastatavad. Välistatud peab olema võimalus, et kasutajaõigusi antakse nii, et konkreetne kasutaja pole teada või veel hullem – et üks kasutaja saab tegutseda teise nime all.
3. Igast andmetöötlustoimingust peab maha jääma nimeline jälg (logi). Mitte üksnes põhiteabe säilitustähtajad, vaid ka põhiteabe kasutamise logide säilitustähtajad tuleb kindlaks määrata.
4. Vältida tuleb piiranguga digitaalteabe hoidmist väljaspool andmekogusid ja dokumendihaldussüsteemi (näiteks asutuse struktuuriüksuste võrguketastel – nii ei ole teabe terviklus piisavalt tagatud).
5. Kui turvameetmete rakendamist saab automatiseerida, siis tuleks seda kindlasti teha:
 - a) infosüsteemi (näiteks asutuse arvutivõrgu, andmekogu, dokumendihalduse) kasutajaõiguste andmisel peab kasutaja olema sunnitud süsteemihaldurilt saadud salasõna kohe enda valitu vastu vahetama. Ebaturvalise salasõna valimist tuleb automaatselt tõkestada. Kasutaja peab olema sunnitud kindla perioodi järel salasõna vahetama;
 - d) ekraaniluku pealemineku saab automaatseadistada;
 - e) säilitamistähtaja ületanud teabe hävitamist tuleks samuti automatiseerida niihästi töökoormuse kergendamiseks kui ka riski maandamiseks, et seda ei viitsitagi hävitada;
 - f) väga suurte ja tundlike andmekogude puhul tuleks rakendada kasutusanomaaliate automaatseiret. Niisugune seire on nõutav näiteks Schengeni infosüsteemis. Selline tarkvaralahendus abistab asutuse sisekontrolliüksust andmete väärkasutuse avastamisel.

§ 105. Kuidas kasutada eemaldatavaid andmekandjaid?

1. Eriti tähelepanelik tuleb olla piiranguga teabe salvestamisel eemaldatavatele andmekandjatele ehk irdseadmetele (mälupulk, mälukaart, väline kõvaketas, CD/DVD-plaat). Selliste vidinate kaotamine või varastamine on printeri järel teine suur lekete allikas. Kui piiranguga teave on neil krüptimata, siis tuleb neid hoida lukustatud kapis või sahtlis. Eriti tundlikku teavet ei tohi üldse eemaldavaile andmekandjatele salvestada.
2. Töölase teabe, sh piiranguga teabe käitlemisel tohib kasutada vaid asutuses arvelevõetud andmekandjaid.
3. Andmekandjatel oleva teabe kustutamiseks tuleb kasutada kas failide mitmekordset ülekirjutamist vastava tarkvaraga või andmekandja füüsilist hävitamist.

§ 106. Kuidas edastada piiranguga teavet asutusest välja?

1. Vältida tuleb piiranguga teabe edastamist telefoni teel. Telefonikõne puhul pole võimalik tuvastada kõne vastuvõtja isikut, kõne sisu võib kostuda kõrvaliste isikuteni. Turvalisem on videokõne – eeldusel, et kõnelejad tunnevad teineteist.
2. Piiranguga teabe edastamiseks ühest asutusest teise sobib dokumendivahetuskeskuse infosüsteem ehk [DVK](#). DVK kasutab turvalist infosüsteemide andmevahetuskihti ehk X-teed.
3. Piiranguga teabe edastamiseks Eesti isikutele on esimese valikuna soovitatav kasutada ametlikku e-posti (isikukood@eesti.ee, registrikood@eesti.ee). Need, kes on selle endale seadistanud või sisestanud [eesti.ee teabevärvasse](#) oma mobiiltelefoni numbri, on ühtlasi aktseptinud [ametliku e-posti kasutustingimusi](#). Nende kohaselt annab isik nõusoleku menetlusdokumentide elektrooniliseks kättetoimetamiseks, kui nõusolek on seaduse kohaselt vajalik. Nõusolek on vajalik haldusmenetluse seaduse kohaselt (§ 27 lg 2). Kohtu-, väärteo- ja täitemenetluses ei ole nõusolek vajalik.

Menetlusdokumendi (mis sageli sisaldab piiranguga teavet) kättetoimetamiseks saadetakse ametlikule e-posti aadressile e-kiri või [eesti.ee teabevaravasse](http://eesti.ee/teabevaravasse) sisestatud mobiilinumbrile SMS-sõnum. E-kiri või SMS sisaldab teadet koos lingiga. Link viib kas [eesti.ee teabevaravasse](http://eesti.ee/teabevaravasse) või mõnesse muusse sisselogimist nõudvasse portaali. Lingi avamiseks tuleb end sisse logida, sellest jääb maha jälg, mis on tõendiks dokumendi kättesaamise kohta. Loomulikult saab ametlikul e-posti aadressil saata ka tavalisi teateid ja kirju (ilma lingita), mille puhul seadus kättetoimetamist ei nõua.

4. Kui e-kiri on jõudnud kirja saaja seadmesse, läheb vastutus riskide eest talle üle. Enne seda liigub e-kiri sidevõrgu kaudu saatjalt saajale. Sidevõrke haldavad sideettevõtjad, kellele [elektroonilise side seadus](#) paneb saladuse hoidmise kohustuse. Siiski peab arvestama, et krüptimata e-kirja liikumine üle interneti sisaldab riske. Kui e-kiri sisaldab eriti tundlikku piiranguga teavet, siis on mõistlik kirja sisu krüptida.

Lihtsaim võimalus digitaalse teabe lühiajaliseks krüptimiseks on [DigiDoc3 krüpto](#) tarkvara. Tegemist on ID-tarkvara osaga, mis paigaldatakse kasutaja arvutisse koos ID-tarkvara paigalduspaketiga. Lisaks konkreetse isikukoodiga krüptimisele on võimalik kasutada ka [ettevõtte ja asutuse sertifikaati](#). Oluline on meeles pidada, et krüptitud teave läheb kaotsi, kui aadressaadi ID-kaarti (või ettevõtte/asutuse krüptosert) on aegunud või ei saa seda muul põhjusel kasutada.

5. Kui saadate e-kirja korraga mitmele erinevale isikule, siis kirjutage aadressid pimekoopia-reale, kus aadressaadid ei näe üksteise aadresse. Ärge kasutage tavalist aadressivälja või koopiarida, kus saajad üksteise e-posti aadresse näevad. Teatavasti on eraisiku kontaktandmed, sh e-posti aadress, juurdepääsupiiranguga teave (AvTS § 35 lg 1 p 12). Erandiks on omavahel seotud aadressaadid, näiteks ühiste huvidega kaastaotlejad samas menetluses, kes menetluse käigus niigi teavad üksteise kontaktandmeteid.

6. Paberposti edastavad postiteenuse osutajad. [Postiseadus](#) paneb neile saladuse hoidmise kohustuse. Posti toimetamisest postkasti läheb vastutus üle postkasti omanikule. Piiranguga teavet sisaldav kiri ei tohi olla lahtisel postkaardil, vaid kinnises ümbrikus. Eriti tundliku piiranguga paberteabe edastamisel tuleks kasutada lihtkirjast kindlaimaid edastusviise (tähtkiri, kuller- ja otsepost).

§ 107. Kas teisele asutusele võib anda otseligipääsu piiranguga teabe juurde?

1. AvTS koostati paberajastul. Ta lähtub sellest, et (paber)teave on füüsiliselt ühe asutuse valduses ja teise asutuse esindajaid lastakse selle juurde igakordsete taotlustega. AvTS ei näinud ette olukordi, kus asutustel on ühine dokumendihaldussüsteem või kui üks asutus saab otseligipääsu teise asutuse digitaalteabesse.

2. Kui asutustel on ühine dokumendihaldussüsteem, siis olgu see jagatud tehniline platvorm, mitte jagatud ligipääsuga andmestik. Üks asutus ei tohi pääseda teise asutuse dokumendihalduse sisemisse vaatesse. AvTS eeldab, et dokumendiregistri asutuse-sisene vaade on tööpoolest asutuse sisene vaade.

3. Otseligi pääse ehk „torusid“ teise asutuse dokumendihaldusse tuleks võimalusel vältida. Otseligi pääsu võimaldamisel peab olema selge vajadus avaliku ülesande täitmiseks. Inspektsioon kontrollib, et otseligipääs hõlmaks üksnes seda dokumendisarja, mis on sellise ülesande täitmisel tegelikult hädavajalik.

Näiteks Riigi Tugiteenuste Keskusele antakse ligipääs teenindatava asutuse personalidokumentide sarjale. Teenindatava asutuse menetlusteabele ligipääsu vajadus puudub.

4. Korraga mitut asutust puudutava infohalduse riskiks on vastutuse hajumine. Sellepärast tuleb ühise dokumendihalduse ning otsejuurdepääsude puhul rangelt tagada, et kõigist toiminguid (sh teabe vaatamisest tavakasutaja poolt, samuti süsteemihaldurite tegevusest) jääks maha nimeline jälg (logi).

11. peatükk. Kriminaal- ja väärteomenetluses kogutud teabe avalikustamine

§ 108. Kust tulevad piirangu alused?

Avaliku teabe seaduse (AvTS) § 35 lg 1 p 1 alusel on teabevaldaja kohustatud tunnistama asutusesiseseks kasutamiseks mõeldud teabeks kriminaal- või väärteomenetluses kogutud teabe, välja arvatud vastavalt väärteomenetluse seadustikus (VTMS) ja kriminaalmenetluse seadustikus (KrMS) sätestatud tingimustel avaldatav teave.

§ 109. Kuidas toimub menetlusteabe avalikustamine menetluse ajal?

1. Kriminaalmenetluses on toimikumaterjalide avaldamise üldtingimused sätestatud KrMS § 214. Kohtueelse menetluse andmete avaldamine on lubatud prokuröri loal kriminaalmenetluse, avalikkuse või andmesubjekti huvides, kui see ülemäära:

- 1) ei soodusta kuritegevust ega raskenda kuriteo avastamist;
- 2) ei kahjusta Eesti Vabariigi või kriminaalmenetluse huve;
- 3) ei sea ohtu ärisaladust ega kahjusta juriidilise isiku tegevust;
- 4) ei kahjusta andmesubjekti ega kolmandate isikute õigusi, eriti delikaatsete isikuandmete avaldamise puhul. Väärteomenetluse puhul on analoogsed tingimused sätestatud VTMS § 62 lõikes 1 ning kohtuvälises menetluses otsustab andmete avalikustamise lubatavuse kohtuvälise menetleja.

2. Nimetatud sätted reguleerivad teabele juurdepääsu võimalusi ajal, mil menetlus on käimas. Sisuliselt kehtib see regulatsioon ka ajal, kui menetlus on formaalselt lõpetatud, samas kestab veel kaebemenetlus või on seaduses sätestatud tähtaeg menetluse uuendamise otsustamiseks (nt KrMS § 202 lg 2, § 203¹ lg 3, § 205 lg 2 jms).

§ 110. Mis ajani reguleerivad menetlusteabele juurdepääsu menetlusseadustikud?

1. Vastavalt KrMS § 209 lõikele 1 antakse kriminaaltoimik arhiivi, kui kriminaalmenetlus lõpetatakse KrMS §-des 200–205² sätestatud alustel. Sellisel juhul on tegemist arhiveerimisega arhiiviseaduse (ArhS) tähenduses. Vabariigi Valitsuse 30.07.2004 määrus nr 261 „Kriminaaltoimiku arhiivimise kord ja toimiku säilitamise tähtajad pärast kriminaalmenetluse lõpetamist“ § 4 näeb ette tähtajad kriminaaltoimikute üleandmiseks uurimisasutuste arhiivi. Nimetatud tähtaegade sätestamisel on aluseks võetud põhimõtte, et kriminaaltoimik arhiveeritakse siis, kui kriminaalmenetluse uuendamise võimalused on ennast sisuliselt ammendanud.

Seega alates toimiku arhiveerimisest ei reguleeri toimikumaterjalide avaldamist enam menetlusseadustik ja aluseks tuleb esmajoones võtta arhiiviseadus koosmõjus avaliku teabe seadusega.

2. Kohtuvälises menetluses loetakse väärteomenetlus lõppenuks ja otsus jõustunuks, kui otsuse peale ei ole kaebust esitatud ja kaebetähtaeg on möödunud (VTMS § 199 lg 1). Ka väärteomenetluses ei kohaldu peale otsuse jõustumist toimikule juurdepääsu võimaldamisel enam väärteomenetluse seadustiku sätted ega AvTS § 35 lg 1 p 1, kuid kehtima jäävad kõik muud piirangu alused.

§ 111. Kuidas toimub menetlusdokumentidele juurdepääsu võimaldamine peale menetluse lõppu?

1. Arhiveeritud toimikumaterjalide juurdepääsupiirangute ja andmete väljastamise üle otsustab ja selle õiguspärasuse eest vastutab teabevaldaja, see tähendab asutus, kus arhiveeritud toimik asub.

2. Juurdepääsupiirangud arhiivitoimikus sisalduvale teabele tulenevad üldalusena AvTS §-st 35 ning eriseadustest. Nii näiteks ei kuulu teabenõude korral avalikustamisele kolmandate isikute andmed, kui see võib oluliselt kahjustada nende eraelu puutumatust. Samuti tuleb juhul, kui jälitustoimingute materjale säilitatakse kriminaaltoimikus, enne toimikule juurdepääsu võimaldamist, eemaldada või katta kinni andmed kolmandate isikute kohta, kes ei olnud süüdistatavad (KrMS § 126¹² lg 7). Kuna jälitustoimingud riivavad oluliselt isikute eraelu puutumatust, siis ei kuulu avalikustamisele ka kriminaaltoimikuks säilitatavad jälitustoimingute materjalid nende süüdistatavate/kahtlustatavate osas, keda süüdi ei ole mõistetud. Sellised andmed on piiranguga AvTS § 35 lg 1 p 12 alusel.

3. Kohtuvälise menetluse väärteotoimikutele võimaldatakse juurdepääs peale menetluse lõppu ja otsuse jõustumist ulatuses, mis ei sisalda piiranguga teavet.

§ 112. Kuidas avalikustada kohtuvälises menetluses tehtud väärteootsuseid?

Kui KrMS § 408¹ lg 1 kohaselt kuulvad kohtulahendid avalikustamisele arvutivõrgus selleks ette nähtud kohas, siis kohtuvälises menetluses tehtud otsuse avaldamine ei tähenda otsuse

avalikustamist internetis, nagu on see kohustuslik kohtuotsuste puhul. Avaldamine VTMS § 62 lg 2 puhul tähendab eelkõige võimalust ja luba avalikustada teabenõude korral andmeid menetlusvälistele isikutele. Oluline on aga see, et sealjuures ei avalikustataks andmeid suuremas ulatuses, kui on ette nähtud KrMS § 408¹ lg-s 2 ja 3 kohtuotsuste avalikustamise puhul.

§ 113. Kuidas avalikustada alaealise süüdlase andmeid?

KrMS § 408¹ lg 2 sätestab, et avalikustatud kohtulahendis ei avalikustata alaealise süüdistatava nime, isikukoodi või sünniaega või asendatakse need initsiaalide või tähemärkidega, välja arvatud juhul, kui avaldatav jõustunud kohtulahend on vähemalt kolmas, milles alaealine on kuriteos süüdi mõistetud. Ka kohtutoimikutele juurdepääsu võimaldamisel tuleb lähtuda alaealise süüdlase andmete avalikustamisel KrMS § 408¹ lg-st 2. Kui avaliku teabe seaduse alusel teabenõude korras on alaealise süüdlase andmed välja küsitavad, siis kaotab avalikustatud kohtuotsustes andmete kinni katmine oma mõtte, seda enam, et tihti on sellised istungid ka kinnised.

Nii põhiseadus, lastekaitse seadus kui ka muud seadused kehtestavad alaealiste õiguste ja huvide erilise ning kõrgendatud kaitse. Tähelepanu tuleb pöörata ka asjaolule, et alaealise süüdistatava andmed ei muutu avalikuks ka peale tema täiealiseks saamist, sest toimik kajastab alaealise tegevust kuriteo toime panemisel.

§ 114. Kui pikaks ajaks saab piirangu kehtestada?

Sõltuvalt piirangu alustest on tähtajad erinevad (AvTS § 40). Üldjuhul on piirangu tähtajaks viis aastat, mida võib asutuse juht pikendada veel viis aastat. Isikuandmeid sisaldavale teabele on juurdepääsupiirang selle saamisest või dokumenteerimisest alates 75 aastat või isiku surmast alates 30 aastat, või kui surma ei ole võimalik tuvastada, siis 110 aastat isiku sünnist (vaata ka juhendi § 40).

§ 115. Kellel on õigus tunnistada dokumente asutusesiseseks kasutamiseks?

AvTS § 41 reguleerib ka korra, kuidas toimub teabe asutusesiseseks tunnistamine:

- a) teabe tunnistab asutusesiseseks kasutamiseks mõeldud teabeks asutuse juht;
- b) alternatiivina võib asutuse juht kehtestada dokumentide loetelus sarjad, milles sisalduvatele dokumentidele võib juurdepääsupiirangud kehtestada. Sarja kuuluvale konkreetsele dokumendile juurdepääsupiirangu rakendamise otsustab sel juhul asutuse juht või tema määratud pädev töötaja, lähtudes dokumendi sisust ja juurdepääsupiirangu eesmärgist;
- c) kui teabekandja seda võimaldab, tehakse asutusesiseseks kasutamiseks mõeldud teabeks tunnistatud dokumendile või dokumendikogumile vastav märge. Toimiku iga lehte eraldi ei pea märgistama, seadus annab võimaluse dokumentide kogumile seada ka üldmärke (nt esilehel või kaantel).

§ 116. Kas kolmandatel isikutel on õigus saada juurdepääsu piiranguga teabele?

AvTS § 38 lg 4 alusel võib asutuse juht otsustada asutuseväliste isikute juurdepääsu võimaldamise asutusesiseseks tunnistatud (isikuandmeid mittesisaldavale) teabele, kui see ei kahjusta riigi või omavalitsusüksuse huve. Tegemist on diskretsiooniotsusega, kus tuleb hinnata erinevaid huvisid. Samuti tuleb kaaluda, kas juurdepääs on võimalik anda osaliselt, arvestades seejuures andmete selekteerimisega kaasnevat töömahtu (AvTS § 23 lg 2 p 3).

§ 117. Kuidas käituda isikuandmetega?

1. Isikuandmeid sisaldava teabele juurdepääsu osas tuleb lähtuda AvTS-s sätestatud juurdepääsupiirangutest.

IKS § 14 lõike 2 alusel on kolmandale isikule isikuandmete (sh arhiivitoimikus olevate isikuandmete) edastamine või nendele juurdepääsu võimaldamine lubatud andmesubjekti nõusolekuta:

- a) kui kolmas isik, kellele andmed edastatakse, töötleb isikuandmeid seaduse, välislepingu või Euroopa Liidu Nõukogu või Euroopa Komisjoni otsekohaldava õigusaktiga ettenähtud ülesande täitmiseks;
- b) üksikjuhtumil andmesubjekti või muu isiku elu, tervise või vabaduse kaitseks, kui andmesubjektilt ei ole võimalik nõusolekut saada;
- c) kui kolmas isik taotleb teavet, mis on saadud või loodud seaduses või selle alusel antud õigusaktides sätestatud avalikke ülesandeid täites (seega ka süüteomenetluse käigus kogutud teave) ja taotletav teave ei sisalda delikaatseid isikuandmeid ning sellele ei ole muul põhjusel kehtestatud juurdepääsupiirangut.

2. IKS § 16 reguleerib isikuandmete töötlemist teadusuuringu või riikliku statistika vajadusteks.

§ 118. Millal puudub isikul juurdepääsuõigus tema andmeid sisaldavatele dokumentidele?

1. IKS § 20 lg 1 võimaldab lisaks kolmandatele isikutele keelduda väljastamast isikuandmeid sisaldavat teavet ka andmesubjektile endale, kui see võib:

- a) kahjustada teise isiku õigusi ja vabadusi;
- b) ohustada lapse põlvnemise saladuse kaitset;
- c) takistada kuriteo tõkestamist või kurjategija tabamist;
- d) raskendada kriminaalmenetluses tõe väljaselgitamist.

2. IKS § 20 lg 1 punktides 1, 3 ja 4 nimetatud võimalus võib arhiveeritud kriminaaltoimiku puhul kõne alla tulla eelkõige juhul, kui kriminaalmenetlus on lõpetatud kuriteo toimepannud isiku tuvastamatuse tõttu (KrMS § 200¹). Sellisel juhul on soovitatav, et uurimisasutus konsulteeriks enne andmesubjektile andmete väljastamise kohta otsuse tegemist prokuratuuriga.

3. Arhiveeritud toimikumaterjalide mittetutvustamise otsuse või teabenõude täitmisest keeldumise peale kaebamist reguleerib esmajoones AvTS § 46, mille järgi on isikul õigus pöörduda sellisel juhul vaidega Andmekaitse Inspeksiooni poole või kaebusega halduskohtusse. Lisaks on andmesubjektile sarnane võimalus ette nähtud ka IKS §-s 22.

Viljar Peep
peadirektor