

RMK teabehalduse poliitika

1. Üldsätted

- 1.1. RMK teabehalduse poliitika (edaspidi poliitika) sätestab teabehalduse üldnõuded RMK-s ja tagab teabe haldamise tõhusa korraldamise kogu teabe elutsükli ulatuses – teabe tekkimisest ning kasutamisest kuni arhiveerimiseni, üleandmiseni ja/või hävitamiseni.
- 1.2. Detailsemad dokumendihaldust puudutavad nõuded on sätestatud „RMK dokumendihalduse juhendis“ ja isikuandmete kaitse alased nõuded „RMK isikuandmete töötlemise juhendis“.
- 1.3. Töötaja on kohustatud järgima poliitikas kehtestatud põhimõtteid. Töötaja ülesanded, kohustused ja õigused teabe haldamisel on täiendavalt määratud struktuuriüksuse põhimääruses, töötaja ametijuhendis ja „RMK töökorralduse reeglite juhendis“.
- 1.4. Käesolevas dokumendis kasutatavad mõisted ja lühendid on defineeritud "[Mõistete ja lühendite leksikonis](#)". Ühtse leksikoni kasutamine võimaldab hoida terminoloogia läbivalt järjepidevana kogu RMK dokumentatsioonis ning vältida mõistete dubleerimist või erinevat tõlgendamist.

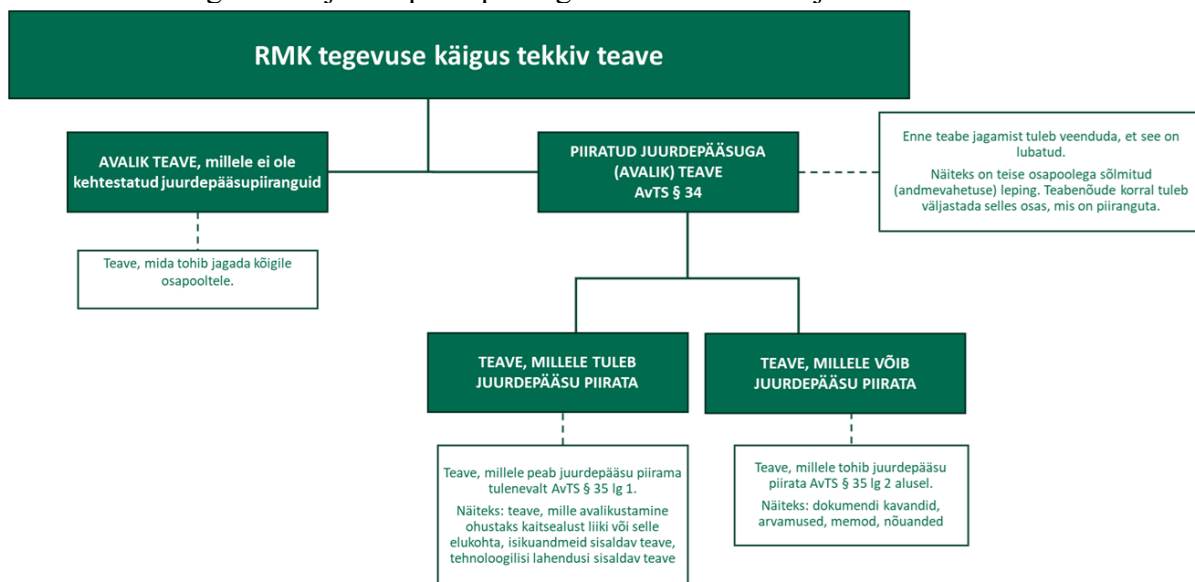
2. Teabehalduse üldpõhimõtted

- 2.1. Teave on igasugune informatsioon, millel on isiku või organisatsiooni jaoks väärtus ning mis on vajalik organisatsiooni toimimiseks (andmed, dokumendid, veebisisu, suuline teave jne).
- 2.2. RMK teave tekib õigusaktides sätestatud ülesannete täitmise käigus.
- 2.3. RMK teave asub paberkandjal, digitaalselt võrguketastel ja välistel andmekandjatel, Microsoft 365 keskkondades, (nt OneDrive, Outlook), infosüsteemides ja rakendustes, nt dokumendihaldussüsteemis (edaspidi DHS).
- 2.4. Teabe töötlemiseks kasutatakse RMK poolt hallatavaid ja kasutatavaid infosüsteeme ja rakendusi, mille loetelu asub „Infosüsteemide ja rakenduste kataloogis“ Jiras.
- 2.5. Teabehaldus on tegevus, mis toetab RMK eesmärkide saavutamist teabe haldamise, jagamise ja vahetamise kaudu. Teabehalduse alamtegevused on andmehaldus, dokumendihaldus, arhiivihaldus, sisuhaldus sise- ja välisveebis ning teabele juurdepääsu ja teabe kaitse ning hävitamise korraldamine.
- 2.6. RMK asjaajamisperioodiks on kalendriaasta (1. jaanuar–31. detsember).

3. RMK teabe liigitamine

- 3.1. Teabe liigitamise eesmärk on omada ülevaadet RMK põhiülesannete täitmisel tekkiva teabe, selle allikate, hoiukohtade, juurdepääsupiirangute ja säilitustähtaegade kohta. RMK tegevuse käigus tekkiv teave on kirjeldatud „RMK teabe liigitusskeemis“.
- 3.2. Teabe liigitusskeemis on teave liigitatud funktsioonipõhiselt sarjadesse ja allsarjadesse, millele on määratud tähised, säilitustähtajad ning teabe loomise ja säilitamise eest vastutavad teabe omanikud. Teabe kirjelduse lahtris on täpsustav ülevaade sarja/allsarja sisust. Lisaks on liigitusskeemis välja toodud teabe kaitsevajadus ja võimalikud juurdepääsu piiramise alused.
- 3.3. Juurdepääsupiirangu alusel liigitatakse RMK-s teave:

- 3.3.1. avalik teave – mis tahes viisil ja mis tahes teabekandjale jäädvustatud ja dokumenteeritud teave, mis on saadud või loodud RMK tegevuse käigus avalikke ülesandeid täites ja millele ei ole kehtestatud juurdepääsupiirangut.
- 3.3.2. piiratud juurdepääsuga teave ehk asutusesiseseks kasutamiseks mõeldud teave – RMK tegevuse käigus tekkinud teave, millele on juurdepääs piiratud lähtuvalt [Avaliku teabe seadusest](#) (edaspidi AvTS) või mõnest teisest õigusaktist.
- 3.3.3. Teabe liigitamine juurdepääsupiirangu alusel on toodud joonisel 1.



Joonis 1. Teabe liigitamine juurdepääsupiirangu alusel

- 3.4. Juurdepääsupiirangu seadmist kirjeldab täpsemalt „[Juurdepääsupiiranguga teabe haldamise juhised](#)“, mille alusel lisatakse juurdepääsupiiranguga dokumendile vastav märge.
- 3.5. RMK-l on kohustus avalikustada üldiseks kasutamiseks mõeldud teavet RMK veebilehel ja avalikus dokumendiregistris (edaspidi ADR). Lisaks tuleb avaldada päringu alusel (nt e-kirja teel saabunud päring) muu teave, millele ei ole juurdepääs piiratud.
- 3.6. Avaliku teabe puhul, millele on juurdepääs AvTS-i alusel piiratud, on ADR-is avalikustatud ainult dokumendi registreerimisandmed, sisule juurdepääs puudub. Füüsiliste isikutega seotud dokumentidel on isiku nimi asendatud märkega „Füüsiline isik“.
- 3.7. Kui RMK-lt küsitakse dokumenti, millele on juurdepääs piiratud, siis:
 - 3.7.1. kui ainult osa dokumendist sisaldab juurdepääsupiiranguga infot (nt isikuandmeid), siis avalikustatakse vaid need osad, millele juurdepääs ei ole piiratud. Piiratud juurdepääsuga teave kaetakse kinni või tehakse väljavõte ainult avalikustatavast osast.
 - 3.7.2. kui kogu dokument sisaldab juurdepääsupiiranguga teavet, siis teavet ega dokumenti ei väljastata. Vastuses märgitakse, millise õigusakti ja sätte alusel juurdepääs on piiratud.
- 3.8. Töödokumentidele, mis registreeritakse DHS-is, on lubatud juurdepääsu piirata AvTS § 35 lõike 2 alusel. Töödokumentideks loetakse näiteks eelnõusid, projekte, lõpuni vormistamata dokumente ning paberkandjal õigusaktide väljatrukke enne nende vastu võtmist.

- 3.9. DHS-is ei registreerita üldjuhul võrguketastel, välistel andmekandjatel, infosüsteemides ja rakendustes ning Microsoft 365 keskkonna OneDrives asuvaid dokumente ja andmeid, mis ei kuulu vaikimisi avalikustamisele ja mida kasutatakse asutuse siseselt igapäevatöö käigus. Kogu RMK teave on välja toodud „RMK teabe liigitusskeemis“.
- 3.10. Töödokumentide hävitamise kord on sätestatud juhendis „RMK arhiividokumentide menetlemise juhis“.
- 3.11. Teabe korrektse liigitamise eest vastutab teabe omanik.

4. Teabe kaitse korraldamine ja juurdepääsude haldamine

- 4.1. Teabe liigitamise järgselt rakendab RMK asjakohaseid organisatsioonilisi, füüsilisi kui ka infotehnoloogilisi turvameetmeid, tagamaks vastavalt vajadusele:
 - 4.1.1. teavet töötlevate infosüsteemide ja rakenduste tervikluse, käideldavuse, privaatsuse ja konfidentsiaalsuse;
 - 4.1.2. andmete pseudonüümimise, anonüümimise ja krüpteerimise, sh ka arendus- ja testkeskkondades;
 - 4.1.3. õigeaegse teabe hävitamise, kui säilitamise kohustus on möödunud;
 - 4.1.4. intsidentide korral andmete kättesaadavuse õigeaegse taastamise;
 - 4.1.5. elektrooniliste ja füüsiliste juurdepääsude haldamise;
 - 4.1.6. IT-varade, nt arvuteid ja võrke kaitsvate süsteemide (viirusetõrje, tulemüürid, ründe tuvastamise süsteemid ja andmete liikumise monitooringusüsteemid, turvaparandused) olemasolu.
- 4.2. RMK infosüsteemides ja rakendustes toimub teabele ligipääsu piiramine juurdepääsuõiguste kaudu.
 - 4.2.1. Infosüsteemide ja rakenduste kasutajate haldamine toimub vastavalt „[RMK identiteedi- ja juurdepääsuhalduse juhendile](#)“.
 - 4.2.2. Peakasutajate määramine ja ülesannete kirjeldamine on toodud “RMK infosüsteemide peakasutajate määramise ja ülesannete kirjeldamise juhendis”
 - 4.2.3. Väliste registrite kasutusõiguste andmine tööülesannete täitmiseks toimub vastavalt „Väliste süsteemide haldamise juhendile“.
- 4.3. Füüsiline juurdepääsuhaldus on kirjeldatud “RMK kontoritesse juurdepääsude andmise juhendis”.
- 4.4. Logimisega seotud põhimõtted nii RMK poolt arendatud, kui RMK jaoks arendatud rakenduste puhul on sätestatud „Logimise spetsifikatsiooni“ dokumendis Confluences.
- 4.5. Piiratud juurdepääsuga teabe hoidmisel on töötaja kohustatud järgima järgmisi põhimõtteid:
 - 4.5.1. piiratud juurdepääsuga teavet on lubatud kopeerida, paljundada, RMK-st paberkandjal või elektroonilisel kujul välja viia, saata või kolmandatele isikutele jagada üksnes juhul, kui see on otseselt seotud tööülesannete täitmisega ja selleks on olemas õiguslik alus. Õiguslikuks aluseks loetakse muuhulgas lepingulist andmevahetust, seadusest tulenevat kohustust või tööprotsesside toimimiseks vajalikku andmete edastamist (näiteks infosüsteemides ja rakendustes koostatud üleandmise ja vastuvõtmise aktide edastamine lepingupartnerile ning auditite raames teabe edastamine audiitorile). Vajaduse korral aitab õigusliku aluse olemasolu piiratud juurdepääsuga teabe jagamiseks või mittejagamiseks välja selgitada õigus- ja hangete osakond;
 - 4.5.2. teistele töötajatele võib piiratud juurdepääsuga teavet avaldada ainult tööülesannete täitmise vajadusel;

5. Teabevahetuse korraldamine

- 5.1. Dokumentide jagamiseks on lubatud kasutada ainult DHS-i ja RMK Microsoft 365 keskkonda, nt OneDrive, Outlook, Teams. Muude võimalike failijagamisteenuste kasutamiseks tuleb need kooskõlastada IT-abiga.
- 5.2. Väliste andmekandjate kasutamine tuleb kooskõlastada IT-abiga, kes põhjendatud juhul tellib mäluseadme ning vajadusel krüpteerib selle enne kasutamist.
- 5.3. Piiratud juurdepääsuga teabe edastamisel tuleb kasutada tehnilisi või korralduslikke meetmeid teabe kaitseks. Piiratud juurdepääsuga dokumendid vastavalt märgistada.
 - 5.3.1. Eriliiki isikuandmeid ja süütegudega seotud andmeid sisaldav teave lisaks märgistamisele täiendavalt krüpteerida, näiteks DigiDoc rakendust kasutades.
 - 5.3.2. Piiratud juurdepääsuga teabe edastamisel postiga või kulleriga tuleb ümbrik saata tähitult adressaadile.
 - 5.3.3. Töötajad peavad hoiduma piiratud juurdepääsuga teabe jagamisest avalikes kohtades või ebatavalise side kaudu.

6. Konfidentsiaalsuskokkulepete sõlmimine ja intellektuaalse omandi määramine

- 6.1. RMK töötajad ja lepingupartnerid kinnitavad konfidentsiaalsustingimused lepingu sõlmimisel.
- 6.2. Lepingu sõlmimisel kolmanda osapoolega toote või teenuse tarbimisel või pakkumisel tuleb jälgida, et intellektuaalse omandi õigused oleksid tagatud nii intellektuaalse omandi kasutamise kui ka õiguste omamisel.
- 6.3. Avalikest allikatest saadava teabe korral tuleb jälgida, et täidetud on nii autoriõiguse kui andmekaitse tingimused.
- 6.4. Dubleerimine, teisendamine muusse vormingusse või ärilistest salvestistest (video, heli) eraldamine on lubatud vaid juhul, kui seda lubavad autoriõiguse seadused või kohaldatavad litsentsid.
- 6.5. Täielik või osaline standardite, raamatute, artiklite, aruannete või muude dokumentide kopeerimine on keelatud, v.a autoriõiguse seaduse või kohaldatavate litsentsidega lubatud.

7. Teabe säilitamine hävitamine ja arhiveerimine

- 7.1. Digitaalselt tekkinud teave tuleb säilitada ja arhiveerida vormingutes, mis võimaldavad tagada salvestuskandja ja vormingu loetavuse kogu säilitusperioodi jooksul, kaitstes neid tulevastest tehnoloogia muudatustest tuleneva kaotsimineku eest.
- 7.2. Kogu säilitamise perioodi kestel tuleb säilitada ka kõik krüpteeritud arhiivide või digitaalsignatuuride juurde kuuluvad krüptovõtmed ja programmid.
- 7.3. RMK teabe liigitusskeemis on teabele määratud säilitustähtajad ning teabe loomise ja säilitamise eest vastutavad teabe omanikud. Töödokumentide säilitustähtaeg on üldjuhul 5 aastat.
- 7.4. Teabe hävitamine tagab, et säilitustähtaja ületanud teave ei koorma asjatult infosüsteeme ja rakendusi ning tööruume ja dokumendihoidlaid.
- 7.5. Infosüsteemides ja rakendustes asuva teabe hävitamine toimub koostöös kvaliteedi- ja teabehaldusosakonnaga, infotehnoloogia arenduste osakonnaga, infotehnoloogia halduse osakonnaga ning infosüsteemide või rakenduste peakasutajatega.

- 7.6. Kui isikuandmeid sisaldava teabe hävitamine infosüsteemidest ei ole säilitustähtaja möödumisel võimalik, tuleb kasutada isikuandmete varjamiseks täiendavaid meetmeid näiteks anonüümimist.
- 7.7. Teabe hävitamise või anonüümimise kohta peab säilima jälg, nt paberkandjal teabe hävitamise akt, infosüsteemis või rakenduses hävitamise metaandmejälgi või Jiras vastav tööpilet.
- 7.8. Paberkandjal teabe hävitamist korraldab kvaliteedi- ja teabehaldusosakond.
- 7.9. Paberkandjal, infosüsteemides, rakendustes, võrguketastel, välistel andmekandjatel ja Microsoft 365 keskkondades olevad töödokumendid hävitatakse säilitustähtaja möödumisel omaniku poolt.
- 7.10. Töödokumentide hävitamisele kehtivad samasugused nõuded kui ametlikele dokumentidele, välja arvatud dokumenteerimise kohustus.
- 7.11. Arhiividokumentide säilitamine, arvelevõtt, kasutamine, üleandmine ja hävitamine toimub „RMK arhiividokumentide menetlemise juhise“ alusel.

8. Andmete seiramine

- 8.1. Andmekaitsealaste nõuete täitmist seiravad andmekaitse spetsialist ja infoturbejuht regulaarselt igapäevatöö käigus ning teabe- ja dokumendihaldusspetsialist perioodiliselt.
- 8.2. Andmete töötlemisega seotud rikkumiseks loetakse turvanõuete rikkumist, mis põhjustab piiratud juurdepääsuga teabe juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise, loata avalikustamise või juurdepääsu võimaldamise. Nt kui isikuandmeid sisaldavatele andmetele saavad juurdepääsu kõrvalised isikud, avalikus dokumendiregistris on näha füüsilise isiku andmed, RMK kasutajakonto (nimi ja salasõna) saab avalikuks, isikuandmeid sisaldavad dokumendid lähevad kontorist kaotsi jne.
- 8.3. Teabe kaitsega seotud võimalike rikkumiste avastamiseks seiratakse:
 - 8.3.1. ADR-i juurdepääsupiirangute õigsust;
 - 8.3.2. infosüsteemides ja rakendustes isikuandmete töötlemise aluste kehtivust koostöös IT tootejuhtidega ja infosüsteemide või rakenduste peakasutajatega;
 - 8.3.3. isikuandmeid sisaldava teabe säilitustähtaegu koostöös IT tootejuhtidega ja infosüsteemide või rakenduste peakasutajatega.
 - 8.3.4. Microsoft Purview riskihinnanguid ja -indikaatoreid, et tuvastada teabe kaitsega seotud võimalikke rikkumisi ning ennetada ja uurida turvaintsidente ning andmelekked.
- 8.4. Avastatud rikkumised dokumenteeritakse Jiras. Tulevaste rikkumiste ennetamiseks võetakse kasutusele vajalikud parandusmeetmed, nt juhendite täiendamine, töötajate koolitamine, toimingute analüüsimine.
- 8.5. Teabe kaitsega seotud rikkumisel hinnatakse ohu taset andmesubjekti õigustele ja otsustatakse Andmekaitse Inspeksiooni, Riigi Infosüsteemi Ameti, Politsei- ja Piirivalveameti ja andmesubjekti teavitamise vajadus.

9. Vastutus teabehalduse korraldamisel

- 9.1. Juhatus vastutab andmekaitse nõuete täitmise eest RMK-s ja tagab andmete kaitsmiseks vajalikud ressursid, määrab ametisse andmekaitse spetsialisti ning defineerib andmekaitsealased rollid.
- 9.2. Andmekaitse spetsialist koostöös teabe- ja dokumendihaldusspetsialistiga:
 - 9.2.1. korraldab teabe kaitse nõuete kirjeldamist, täitmist ja järgmist, nõustab töötajaid igapäevaselt piiratud juurdepääsuga seotud teabe kaitse küsimustes;

- 9.2.2. vastutab teabehaldusega ja piiratud juurdepääsuga teabe kaitsega seotud juhendite ja juhiste koostamise eest;
- 9.2.3. koolitab töötajaid teabehalduse ja andmekaitse teemadel.
- 9.2.4. kontrollib, et organisatsioon töötleks ja kaitseks andmeid vastavalt seadusele ja käesolevale korrale ning teistele õigusaktidele.
- 9.3. Teabele juurdepääsu tagamise, teabe kasutamise ja hävitamise eest vastutab dokumendi omanik.
- 9.4. Kvaliteedi- ja teabehaldusosakond vastutab teabe kaardistamise, dokumendi- ja arhiivihalduse korraldamise, teabehalduse poliitika, „RMK teabe liigitusskeemi“ ning dokumendi- ja arhiivihalduse juhiste koostamise, DHS-i ja ADR-i arendamise, kasutajate nõustamise ja juhendamise, RMK pitsati hoidmise ja kasutamise eest.
- 9.5. Infotehnoloogia halduse osakond vastutab infosüsteemide ja rakenduste, võrguketaste toimimise, Microsoft 365 keskkondade, juurdepääsuõiguste haldamise ning teabe varundamise, säilitamise ja hävitamise korraldamise eest.
- 9.6. Kommunikatsiooni- ja turundusosakond vastutab teabe nõuetekohase avalikustamise eest RMK välisveebis, teistes avalikkusele suunatud infokanalites (nt Facebook, Instagram, Youtube) ja RMK siseveebis.
- 9.7. Uus töötaja tutvub teabehalduspoliitikaga tööle asumisel töötaja iseteenindusportaalil.