**Riigisaladuse ja salastatud välisteabe seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu**

**seletuskiri**

**1. Sissejuhatus**

**1.1. Sisukokkuvõte**

Eelnõuga luuakse riigisaladuse ja salastatud välisteabe seaduses (edaspidi *RSVS*) ühetaoline struktuur riigisaladuse ja salastatud välisteabe (edaspidi koos *salastatud teave*)kaitset korraldavate ametkondade pädevust reguleerivates sätetes. Muudatus puudutab Kaitsepolitseiametit (edaspidi *KAPO*), Kaitseväe põhimääruses määratud struktuuriüksust, Välisluureametit (edaspidi *VLA*) ja riigi julgeoleku volitatud esindajat (edaspidi *RJVE*). Muudatusega luuakse ühetaoliselt sõnastatud õigusnormid, mille kohaselt esmalt sõnastatakse pädevused, seejärel pädevustest tulenevad ülesanded ning lõpuks ülesannete täitmisel tehtavad tegevused.

Tulenevalt vajadusest reguleerida rahvusvahelist koostööd salastatud teabe kaitsel, loob eelnõu õigusliku aluse pädeva asutuse ja ühtse kontaktpunkti rollide määramiseks Vabariigi Valitsuse 20. detsembri 2007. aasta määruses nr 262 „Riigisaladuse ja salastatud välisteabe kaitse kord“ (edaspidi *RSVKK*).

Eelnõuga täiendatakse ja täpsustatakse RJVE pädevusega seotud norme. RJVE-l on lisaks salastatud välisteabe kaitse korraldamisele ja kontrollimisele roll ka riigisaladuse kaitse korraldamisel ja kontrollimisel, kui riigisaladust avaldatakse välisriigile, rahvusvahelisele organisatsioonile või rahvusvahelise kokkuleppega loodud institutsioonile. Eelnõuga sätestatakse vastav pädevus RSVS-is.

Eelnõuga luuakse õiguslik alus salastatud välisteabe juurdepääsu andmisest keeldumiseks isikutele, kes ei nõustu endale salastatud välisteabe kaitse nõuete tutvustamise või kinnituse allkirjastamisega. Eesti Panga presidendil, Eesti Panga Nõukogu esimehel ja liikmel, kohtunikul, Riigikogu liikmel, riigikontrolöril, Vabariigi Valitsuse liikmel ning õiguskantsleril on ametikohajärgne juurdepääsuõigus salastatud välisteabele. Juurdepääsuõigus tekib ametikohale asumisega ja seda eraldi ei vormistata. Kui aga välislepingu kohaselt on salastatud välisteabe kaitse nõuete tutvustamine kohustuslik, kuid isik keeldub nõuete tutvustamisest või kinnituse allkirjastamisest, ei ole võimalik talle konkreetsele salastatud välisteabele juurdepääsu anda vaatamata ametikohajärgse juurdepääsuõiguse olemasolule.

Eelnõuga muudetakse salastatud välisteabe kaitset reguleerivate normide sõnastus selgemaks ja rakenduspraktikaga kooskõlas olevaks.

Eelnõu vähendab vähesel määral isikute halduskoormust. Eelnõuga tunnistatakse kehtetuks RSVS § 35 lõige 6, milles nähakse ette kohustus registreerida riigisaladuse välisriigile, rahvusvahelisele organisatsioonile või rahvusvahelise kokkuleppega loodud institutsioonile edastamine iga kord RJVE juures. Lisaks riigiasutustele võib olla vaja edastada riigisaladust välismaale näiteks ettevõtjatel, kes edaspidi seda enam RJVE juures registreerima ei pea.

**1.2. Eelnõu ettevalmistajad**

Eelnõu ja seletuskirja on koostanud Kaitseministeeriumi ja VLA ametnikud koostöös Justiitsministeeriumi, Siseministeeriumi ning KAPO esindajatega.

Eelnõu õiguslikku kvaliteeti on kontrollinud Kaitseministeeriumi õigusosakonna nõunik Liina Martinson ([liina.martinson@kaitseministeerium.ee](mailto:liina.martinson@kaitseministeerium.ee)<mailto:>). Eelnõu ja seletuskirja on keeleliselt toimetanud Luisa Keelelahenduste eesti keele vanemtoimetaja Tiina Alekõrs ([tiina@luisa.ee](mailto:tiina@luisa.ee)).

**1.3. Märkused**

Eelnõu ei ole seotud teiste menetluses olevate eelnõudega, Euroopa Liidu õiguse rakendamisega ega Vabariigi Valitsuse tegevusprogrammiga. Eelnõuga muudetakse järgmisi seadusi:

1) RSVS avaldamismärkega RT I, 08.07.2025, 47;

2) Eesti Panga seadus (edaspidi *EPS*) avaldamismärkega RT I, 01.03.2023, 45;

3) julgeolekuasutuste seadus (edaspidi JAS) avaldamismärkega RT I, 14.03.2023, 25;

4) kohtute seadus (edaspidi *KS*) avaldamismärkega RT I, 14.03.2025, 24;

5) Riigikogu liikme staatuse seadus (edaspidi *RKLS*) avaldamismärkega RT I, 30.12.2024, 19;

6) Riigikontrolli seadus (edaspidi *RKS*) avaldamismärkega RT I, 02.06.2021, 13;

7) Vabariigi Valitsuse seadus (edaspidi *VVS*) avaldamismärkega RT I, 07.05.2025, 9;

8) õiguskantsleri seadus (edaspidi *ÕKS*) avaldamismärkega RT I, 26.05.2020, 11.

Selleks et eelnõu seadusena vastu võtta, on vaja Riigikogu koosseisu häälteenamust, kuna VVS-i, EPS-i ja RKS-i muutmiseks on põhiseaduse § 104 punktide 8, 12 ja 13 järgi vaja Riigikogu koosseisu häälteenamust.

**2. Seaduse eesmärk**

Seaduse eesmärk on:

* muuta salastatud teabe kaitset korraldavate ametkondade pädevust reguleerivad sätted ühetaoliseks;
* sätestada õiguslik alus pädeva asutuse ja ühtse kontaktpunkti rollide määramiseks RSVKK-is rahvusvahelise koostöö tarbeks;
* reguleerida RJVE pädevus riigisaladuse kaitse korraldamisel ja kontrollimisel;
* muuta salastatud välisteabe kaitset reguleerivate normide sõnastus selgemaks ja rakenduspraktikaga kooskõlas olevaks.

Kehtivas seaduses on salastatud teabe kaitse korraldamisel eri ametkondades nende pädevused, ülesanded ja tegevused esitatud üksteisega läbisegi, mis on raskendanud rakendajatel mõistmast, millised pädevused mingil ametkonnal on, milliseid ülesandeid konkreetsete pädevuste raames tuleb täita ning milliseid tegevusi on võimalik teha ülesannete täitmiseks. Seaduse eesmärk on eristada üldpädevus, selle raames täidetavad ülesanded ja ülesannete täitmiseks tehtavad tegevused.

Salastatud välisteabe kaitse puhul ei ole kehtivas õiguses defineeritud rahvusvahelisest õigusest tulenevad rollid, mis on eriti olulised Euroopa Liidu ja Põhja-Atlandi Lepingu Organisatsiooni (edaspidi *NATO*) salastatud teabe kaitse puhul. Seaduse eesmärk on määrata nende rollide täitja.

Kehtivas õiguses ei ole sätestatud RJVE pädevust riigisaladuse kaitse korraldamisel ja kontrollimisel, kui riigisaladust avaldatakse välisriigile, rahvusvahelisele organisatsioonile või rahvusvahelise kokkuleppega loodud institutsioonile. Seaduse eesmärk on määrata kindlaks pädevus RSVS-i tasandil.

Kehtivas seaduses on salastatud välisteabe kaitsega seotud normid raskesti mõistetavad ega ole osal juhtudel enam rakenduspraktikaga kooskõlas. Seaduse eesmärk on muuta normid selgemaks ja rakenduspraktikaga kooskõlas olevaks.

Eelnõu väljatöötamise kavatsust ei ole koostatud. Vabariigi Valitsuse 22. detsembri 2011. aasta määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 1 lõike 2 punkti 5 kohaselt ei ole väljatöötamiskavatsus nõutav, kui seaduse rakendamisega ei kaasne olulist õiguslikku muudatust või muud olulist mõju. Eelnõu eesmärk on ajakohastada salastatud teabe kaitset reguleerivat regulatsiooni, kuid tegu ei ole põhimõtteliste muudatustega, millega kaasneks oluline õiguslik muudatus või muu oluline mõju.

**3. Eelnõu sisu ja võrdlev analüüs**

Eelnõu koosneb üheksast paragrahvist: §-dega 1–8 muudetakse RSVS-i, EPS-i, JAS-i, KS-i, RKLS-i, RKS-i, VVS-i ja ÕKS-i, §-ga 9 sätestatakse seaduse jõustumise aeg.

**Paragrahv 1. RSVS-i muutmine**

**Eelnõu § 1 punktidega 1, 5 ja 6** asendatakse RSVS-i tekstis:

* tekstiosa „elektrooniline teabeturve“ tekstiosaga „salastatud teabe küberturvalisus“;
* sõna „salajasus“ sõnaga „konfidentsiaalsus“;
* sõna „terviklikkus“ sõnaga „terviklus“.

Muudatuste eesmärk on ühtlustada RSVS-i terminikasutust küberturvalisuse seaduse (edaspidi *KüTS*) ja selle alusel antud õigusaktide terminikasutusega. KüTS § 1 lõike 2 kohaselt ei kohaldata KüTS-i riigisaladuse ja salastatud välisteabe töötlemisele ning sellise teabe töötlussüsteemide pidamisele. Erisuse põhjus on see, et salastatud teabe elektroonilise töötlemise korral tuleb rakendada rangemaid turvameetmeid, mis on reguleeritud RSVS-is ja selle alusel antud õigusaktides. See aga ei tähenda, et RSVS-is peaks kasutama KüTS-ist erinevaid termineid. Oma olemuselt on elektrooniline teabeturve küberturvalisuse tagamine salastatud teabe töötlussüsteemides. Samuti on konfidentsiaalsus, terviklus ja käideldavus olemuselt sama sisuga nii salastatud teabe töötlussüsteemide kui ka mittesalastatud teabe töötlemiseks kasutatavate võrgu- ja infosüsteemide puhul.

**Eelnõu § 1 punktiga 2** defineeritakse RSVS-is termin „salastatud teave“. Seni on definitsioon olnud RSVKK-is, kuid kuna RSVS-is on mitmes kohas väljendit „salastatud teave“ kasutatud, on otstarbekas tõsta termin RSVKK-ist RSVS-i. RSVKK vastav säte tunnistatakse kehtetuks.

**Eelnõu § 1 punktiga 3** defineeritakse RSVS-is termin „töötlemisõigus“. Juba praegu on sõna „töötlemisõigus“ RSVS-is mitmes kohas kasutatud, kuid seoses sellega, et käesoleva eelnõuga tehtavate muudatuste toimel hakkab RSVS sõnaselgelt reguleerima ka Euroopa Liidu ja NATO salastatud välisteabe töötlemisõiguse andmist, on otstarbekas defineerida ka vastav lühiväljend, et seda oleks võimalik vastavates sätetes kasutada.

**Eelnõu § 1 punktiga 4** muudetakseRSVS § 3 punktis 9töötlussüsteemi terminit.

Töötlussüsteemi mõistes tehakse kaks muudatust. Esiteks defineeritakse „töötlussüsteem“ küberturvalisuse seaduse § 2 punktis 1 nimetatud võrgu- ja infosüsteemi kaudu, sest olemuslikult on ka töötlussüsteem võrgu- ja infosüsteem. Teiseks tuuakse definitsioonis välja riigisaladuse või salastatud välisteabe töötlemine. See on tunnus, mis muudab võrgu- ja infosüsteemi töötlussüsteemiks.

**Eelnõu § 1 punktiga 7** muudetakse RSVS § 3 punktis 13 RJVE terminit.

RJVE mõiste muutmine on tingitud asjaolust, et RJVE ülesanded ei ole seotud ainult salastatud välisteabega. RJVE korraldab ja kontrollib ka riigisaladuse kaitset, kui seda avaldatakse välisriigile, rahvusvahelisele organisatsioonile või rahvusvahelise kokkuleppega loodud institutsioonile. Muudetud kujul mõistega arvestatakse mõlemat ülesannet. RJVE riigisaladuse kaitse korraldamise ja kontrollimisega seotud ülesanded on täpsemalt kirjeldatud eelnõukohases §-s 231.

**Eelnõu § 1 punktiga 8** viiakse RSVS § 9 punktis 10 variandmete ja konspiratsioonivõtete kasutamisega seotud teabe salastamise aluse sõnastus kooskõlla julgeolekuasutuste seaduse § 23 sõnastusega. RSVS § 9 punkti 10 kehtivas sõnastuses on kasutusel väljend „teeseldud isikud ja organid“. Väljend „isiku, asutuse või organi teesklemine“ oli kasutusel julgeolekuasutuste seaduse §-s 23 enne 01.07.2017. 01.07.2017 jõustus normi muudatus ning sellest alates on kasutusel väljend „variandmed ja konspiratsioonivõtted“.

**Eelnõu § 1 punktiga 9** täiendatakse RSVS § 10 uue punktiga 10, mis käsitleb salastatud teabe kaitseks kasutatavat krüptomaterjali ja selle kasutamise tingimusi käsitleva teabe salastamist. Seni on krüptomaterjalide kohta käiva teabe salastamine paigutatud töötlussüsteemi käsitleva teabe alla (RSVS § 10 punkt 2). See ei ole korrektne, sest kõik salastatud teabe kaitseks kasutatavad krüptomaterjalid ei ole seotud konkreetse töötlussüsteemiga.

**Eelnõu § 1 punktiga 10** täiendatakse RSVS § 11 lõikega 4 järgmises sõnastuses: „(4) Käesoleva paragrahvi lõike 3 alusel asutusesiseseks kasutamiseks mõeldud teabeks tunnistatud teabele kehtestatakse juurdepääsupiirang samaks tähtajaks, kui on käesoleva paragrahvi lõike 1 alusel kehtestatud määruses sätestatud samadele tunnustele vastava riigisaladuseks oleva teabe salastamistähtaeg, kui eraõigusliku isiku, välisriigi või rahvusvahelise organisatsiooniga sõlmitud lepingus ei ole sätestatud teisiti. Asutuse juht või tema volitatud isik võib juurdepääsupiirangu tähtaega pikendada kuni viie aasta võrra, kui juurdepääsupiirangu põhjus püsib, kuid kokku mitte rohkem kui 75 aastat.“.

RSVS § 11 lõike 3 järgi võib teatud riigisaladuse tunnustele vastava teabe tunnistada juurdepääsupiiranguga asutusesiseseks teabeks, kui selle teabe avalikuks tulek ei kahjusta küll riigi julgeolekut, kuid teabele juurdepääsu piiramine on ette nähtud lepingus või teabe avalikuks tulek kahjustaks riigi välissuhtlemist või teabevaldaja seadusest tulenevate ülesannete täitmist. Sellise juurdepääsupiirangu tähtajale kohaldub avaliku teabe seaduse (AvTS) § 40, sest RSVS erandit ette ei näe. AvTS § 40 lõikes 1 sätestatud üldreegli järgi on juurdepääsupiirangu tähtaeg kuni viis aastat ning asutuse juht võib pikendada seda kuni viie aasta võrra, kui juurdepääsupiirangu kehtestamise põhjus püsib. Loetelust, millist teavet võib RSVS § 11 lõike 3 järgi tunnistada juurdepääsupiiranguga asutusesiseseks teabeks, nähtub, et nimetatud teabest valdava osa avalikuks tulek võib kahjustada teabevaldaja ülesannete täitmist pikema aja jooksul. Reeglina ei peaks teabe juurdepääsupiirangu tähtaeg olema lühem, kui on samadele tunnustele vastava riigisaladuse salastatuse tähtaeg (15–75 aastat). Konkreetne näide on julgeolekuasutuse riigisaladus. Näiteks võib juurdepääsupiiranguga teabeks tunnistada julgeolekuasutuse struktuuriüksusi, koosseisu ja nende ülesandeid kajastavat teavet, mille avalikuks tulek ei kahjusta riigi julgeolekut. Samalaadse riigisaladuse salastatuse tähtaeg on 50 aastat. Pikk tähtaeg on põhjendatav sellega, et mõned julgeolekuasutuse funktsioonid ja struktuuriüksused on pikka aega püsivad. lühema tähtaja korral tuleks need aga avalikustada ning see kahjustaks julgeolekuasutuse edasist tegevust. Sama põhimõte ja samad tähtajad peavad kehtima ka juurdepääsupiiranguga asutusesiseseks kasutamiseks mõeldud teabe puhul.

AvTS kohustab teabevaldajat tunnistama asutusesiseseks kasutamiseks mõeldud teabeks teabe, mille avalikuks tulek kahjustab riigikaitse korraldamist, sõjalise kaitse planeerimist, ettevalmistamist ja juhtimist; sealhulgas tuleb kaitsta teavet, mille alusel on võimalik teha konkreetseid järeldusi ja anda hinnanguid näiteks Kaitseväe sõjaliste võimekuste kohta. Asutusesiseseks kasutamiseks tunnistatud teabe puhul on võimalik AvTS-i alusel juurdepääsupiirang kehtestada maksimaalselt kümneks aastaks, mis ilmselgelt ei ole teatud teabe puhul piisav, sest teabe avalikustamise korral peab olema tagatud riigi julgeoleku kaitse[[1]](#footnote-1). Teabe avalikustamine pärast AvTS-ist tuleneva tähtaja lõppu võib aga riigikaitset ja riigi julgeolekut kahjustada. Tekib olukord, kus teabele juurdepääsu piiramise vajadus jääb püsima ka pärast AvTS-is sätestatud maksimaalse tähtaja lõppu.

Seadusandja on selgelt väljendanud, et riigi julgeoleku kaitse on selline väärtus, mille kaitse vajadus on *expressis verbis* seaduses kirjeldatud, ning teabe üldiseks kasutamiseks andmisel peab olema riigi julgeolek tagatud[[2]](#footnote-2). RSVS-i sätete tunnustele vastava juurdepääsupiiranguga asutusesiseseks kasutamiseks mõeldud teabe puhul võib juurdepääsupiirangu tähtaja lõppedes tekkida oht, et teabele juurdepääsupiirangu kehtestamise põhjus on endiselt olemas ning teabe avalikustamise tulemusel saab kahjustada riigi julgeolek.

Pärast seadusega kehtestatud juurdepääsupiirangu tähtaja lõppemist on asutusel kohustus teave avalikustada asutuse dokumendiregistris[[3]](#footnote-3). Arvestatav uus julgeolekuoht on avaandmete masspäringud, andmete nn kraapimine[[4]](#footnote-4) ja allalaadimine eraisikute[[5]](#footnote-5) ning eri tsiviilasutuste[[6]](#footnote-6), sealhulgas välisriikides asuvate meediamajade poolt. Riigiasutuste avalikele dokumendiregistritele on juurdepääs igaühel, sealhulgas välisriigi kodanikul. Riigiasutuste avalikule teabele ei ole juurdepääs seaduse tasandil piiratud[[7]](#footnote-7). Lisaks saab Ukraina sõja näitel esile tuua küberrünnete järjest süsteemsema rakendamise sõjaliste eesmärkide toetuseks. Küberluureoperatsioonide fookus on liikumas riigikaitse ja poliitikaga seotud süsteemidele ning sihtmärgid on julgeoleku- ja kaitsesektor ning ettevõtted, mis neid toetavad[[8]](#footnote-8). Samuti on Eesti näitel leidnud tõendamist, et ka avalikult kättesaadavat infot edastatakse vaenuliku riigi luureteenistusele[[9]](#footnote-9). Avalikult kättesaadavaid andmeid koos teiste andmetega analüüsides võib jõuda riigi julgeolekut ohustavate tulemusteni. Sarnasel moel võib olla võimalik eri ministeeriumide valitsemisalade andmeid koos töödeldes teha järeldusi riigi julgeoleku tagamisega seotud võimete ja vahendite kohta. Kehtivas õiguses[[10]](#footnote-10) ei arvestata riigi julgeolekut tagavate asutuste eripära võrreldes muude riigiasutustega ning piisava efektiivsusega ei ole võimalik kaitsta riigi julgeoleku huvides olulist teavet. Arvestades eeltoodut, on tõusetunud vajadus riigi julgeoleku tagamise eesmärgil kaitsta teavet kauem kui AvTS-iga maksimaalselt lubatud kümme aastat.

**Eelnõu § 1 punktiga 11** täiendatakse RSVS § 20 lõikeid 11–13 viisil, mis võimaldab kohaldada paragrahvis viidatud korrakaitseseaduse erimeetmeid ka „administratiivalale sisenemisel ja alal viibimise ajal“.

RSVS § 20 lõigetes 11–13 sätestatakse töötleva üksuse õigusena riigisaladuse turvaalale sisenemisel või riigisaladuse turvaalal viibimise ajal kohaldada korrakaitseseaduse §-des 47–49 ja §-s 52 sätestatud riikliku järelevalve erimeetmeid. Samas toimub piiratud tasemel salastatud teabe töötlemine administratiivalal, kuid viidatud sätete sõnastus ei võimalda administratiivalale sisenemisel või sellel viibimisel korrakaitseseaduses sätestatud riikliku järelevalve erimeetmeid riigisaladuse kaitseks kasutada.

Muudatusega luuakse töötlevale üksusele võimalus paremini tagada salastatud teabe kaitse ka administratiivalal, isegi juhul, kui asutakse väljaspool nn tavapärast asukohta (nt sõidukis). Ei ole mõistlik, et erinevate (riigi)saladuse tasemete puhul saab töötlev üksus rakendada erinevaid teabe kaitseks mõeldud meetmeid.

Tavapäraselt on hoonesse sisenemisel esmane ala nn üldala, kus salastatud teabe töötlemist ei toimu, aga on hooneid, kuhu sisenemisel satutakse kohe administratiivalale, kus muu hulgas võib töödelda piiratud tasemel salastatud teavet. RSVKK § 461 lõike 1 kohaselt tuleb administratiivalale sisenevad isikud ja sõidukid tuvastada. Samas toimub isiku tuvastamise ja tema kontrolli teostamine korrakaitseseaduse § 47 alusel, mis on volitusnormina töötlevale üksusele antud RSVS § 20 lõike l1 puhul ainult turvaalale sisenemiseks, aga vajalikud meetmed (isiku tuvastamine ja tema kontroll) on vaja võtta enne administratiivalale sisenemist, mitte ainult turvaalade puhul.

Lisaks jäetakse RSVS § 20 lõigetest 11–13 välja sõna „riigisaladuse“.

RSVS-is ei eristata eraldi riigisaladuse töötlemiseks ette nähtud turvaala, seega tekitab sõna „riigisaladuse“ olemasolu antud lauses segadust ja on üleliigne. Sõna „turvaala“ on konkreetne ja üheselt arusaadav.

**Eelnõu § 1 punktiga 12** täiendatakse RSVS-i §-ga 201. Uude paragrahvi on üle toodud kehtiva § 35 lõiked 4–52. Muudatuse eesmärk on selgelt eristada rakendajate jaoks riigisaladuse avaldamist ja edastamist. Avaldamist tuleb mõista kui Eesti Vabariigi poolt teisele rahvusvahelise õiguse subjektile riigisaladuse teatavaks tegemist, mille aluseks on üldjuhul salastatud teabe vastastikuse kaitse kokkulepe või riigi õigusaktide kohaselt antud luba. Selline regulatsioon peab paiknema riigisaladuse kaitse üldsätete all.

Edastamine on konkreetse töötleva üksuse poolt riigisaladuse või seda sisaldava teabekandja edastamine teise poole töötlevale üksusele. Edastamist puudutav regulatsioon peab paiknema riigisaladuse töötlemise jaotises, kus paikneb ka § 35, milles seatakse edastamisele tingimusi.

Lõige 1 vastab kehtivale § 35 lõikele 4. Uues normis on kasutatud sõna „välisriigile“ erinevalt kehtivast § 35 lõikest 4, kus on kasutusel „välisriigi töötlevale üksusele“. Erinevuse põhjus on see, et riigisaladust avaldatakse teisele rahvusvahelise õiguse subjektile, milleks saab olla vaid välisriik või rahvusvaheline organisatsioon. Riigisaladust võib jätkuvalt avaldada ka välisriigi töötlevale üksusele, eeldusel et välisriigiga, kus töötlev üksus asub, on sõlmitud salastatud teabe vastastikuse kaitse kokkulepe või on riigisaladuse avaldamiseks loa andnud Vabariigi Valitsuse julgeolekukomisjon, kui teabe vastuvõtja tagab kaitse avaldatava teabe avalikuks tuleku eest. Avaldatava teabe kaitstuse hindamisel peaks Vabariigi Valitsuse julgeolekukomisjon konsulteerima julgeolekuasutuste ja RJVE-ga. RJVE saab uurida, kas rahvusvahelised organisatsioonid (eriti Euroopa Liit ja NATO), mille liige Eesti on, või selliste organisatsioonide liikmesriigid vahetavad teabe vastuvõtjaga salastatud teavet ja mis tingimustel see toimub (nt kas on sõlmitud leping). Julgeolekuasutused saavad anda ülevaate teabe vastuvõtja suhetest teiste riikide ja rahvusvaheliste organisatsioonidega.

Lõikesse 2 on koondatud kehtiva § 35 lõiked 5–52. Kolme lõike asemel on uues sõnastuses üks lõige, millel on kolm § 201 lõikes 1 sätestatust erinevalt riigisaladuse avaldamise juhtumit kirjeldavat punkti. Sõnastuse muutmise eesmärk on tagada parem arusaadavus. Normide mõte jääb samaks. Sõnastuslikult on tehtud kaks muudatust, mis normide sisu ei mõjuta. Punktis 1 ei ole erinevalt kehtivast § 35 lõikest 5 sõnu „käesolevas seaduses ja selle alusel antud õigusaktides sätestatud korras“, sest see on ilmne, et õigusakte tuleb järgida. Punktist 2 on võrreldes kehtiva § 35 lõikega 51 kustutatud sõnad „Euroopa Liidu õigusest“, sest § 50 lõike 11 järgi loetakse Euroopa Liidu täitmiseks kohustuslikust õigusaktist tulenevaid nõudeid RSVS-i tähenduses välislepingust tulenevateks nõueteks. Välislepingut on mainitud lõike 1 punktis 1.

**Eelnõu § 1 punktiga 13** muudetakse RSVS § 22 lõiget 1. Muudatus on vajalik seetõttu, et ka RJVE täidab riigisaladuse kaitse korraldamise ja kontrollimisega seotud ülesandeid. Eelnõuga sätestatakse need uues §-s 231. Muudatuse tulemusel viidatakse sättes ka sellele paragrahvile.

**Eelnõu § 1 punktiga 14** tunnistatakse kehtetuks RSVS § 22 lõike 2 punktid 3–5. Nendes punktides ei kirjeldata pädevusi ega ülesandeid, vaid tegevusi, mida tehakse pädevuse rakendamisel. Punktid viiakse üle uude lõikesse 21.

**Eelnõu § 1 punktiga 15** täiendatakse RSVS § 22 uue lõikega 21, milles esitatakse tegevused, mida KAPO ja Kaitseväe põhimääruses määratud struktuuriüksus sama paragrahvi lõikes 2 toodud pädevuste täitmisel teevad.

Siia lõikesse on üle toodud eelneva punktiga kehtetuks tunnistatud lõike 2 punktid 3–5 ning lisatud kaks uut punkti.

Punktiga 1 antakse KAPO-le ja Kaitseväe põhimääruses määratud struktuuriüksusele õigus anda töötlevale üksusele teavet ja täitmiseks kohustuslikke juhiseid riigisaladuse kaitse nõuete täitmiseks. Kohustuslike juhiste andmise õigus on vajalik selleks, et oleks võimalik suunata töötlevaid üksusi parimal võimalikul viisil riigisaladust kaitsma. Teavet antakse selleks, et töötlevatel üksustel oleks võimalik riigisaladust paremini kaitsta.

Punktis 2 on lisatud tekst, mille kohaselt tuleb vajaduse korral kaasata §-des 23, 231 ja 52 nimetatud asutus või selle struktuuriüksus. Tegemist on vastavates valdkondades eksperditeadmisi omavate ametkondadega, kelle teadmisi on vaja vastava valdkonnaga seotud rikkumise väljaselgitamiseks ja kahju hindamiseks.

Punktiga 5 lisatakse tegevusena koostöö tegemine riigisaladuse kaitse korraldamiseks ja kontrollimiseks riigiasutuste ning välisriikide, rahvusvaheliste organisatsioonide ja rahvusvahelise kokkuleppega loodud institutsioonidega, sest riigisaladuse kaitseks on vaja vahetada teavet välisriikide politsei- ja julgeolekuasutustega ning rahvusvaheliste organisatsioonide ja rahvusvahelise kokkuleppega loodud institutsioonidega.

**Eelnõu § 1 punktiga 16** muudetakse RSVS § 23 lõiget 2. Lõikes 2 sätestatakse VLA ülesanded salastatud teabe küberturvalisuse korraldamisel ja kontrollimisel. Selle tagajärjel tekib selge struktuur, kus kõigepealt on lõikes 1 määratud, et VLA-l on pädevus salastatud teabe küberturvalisust korraldada, ning seejärel on loetletud konkreetsed ülesanded.

VLA ülesanded salastatud teabe küberturvalisuse korraldamisel on töötlussüsteemide akrediteerimine, töötlussüsteemides kasutatavate turbelahenduste nõuetele vastavuse hindamine, töötlussüsteemides kasutatavate turbe- ja krüptomaterjalide kaitse ning töötlussüsteemide kiirgusturbe tagamine. Sellest lähtub ka uus lõike 2 tekst.

Kehtivad punktid 3 ja 4 on hõlmatud uues sõnastuses töötlussüsteemide akrediteerimise alla punktis 1. Tegemist on akrediteerimisega seotud tegevustega, mille eraldi väljatoomine ülesandena ei ole vajalik.

Uue punktiga 2 analoogset normi RSVS praegu ei sisalda. VLA ülesanne on muu hulgas hinnata töötlussüsteemides kasutatavate turbelahenduste salastatud teabe küberturvalisuse nõuetele vastavust. Turbelahendus on salastatud teabe kaitse tagamiseks kasutatav riist- või tarkvaraline (sealhulgas krüptograafiline) lahendus, mille eesmärk on tagada turbenõuete täitmine.

Kehtiv punkt 6 sisaldab kaht põhiülesannet, mida VLA salastatud teabe küberturvalisuse valdkonnas täidab – krüptomaterjalide töötlemise ja kiirgusturbe korraldamist. Uues sõnastuses on mõlema ülesande kohta eraldi punkt, vastavalt punkt 3 ja punkt 4.

Kehtivat punkti 7 ei ole uude sõnastusse üle kantud, sest see on konkreetne tegevus, milleks on vaja töötleva üksuse kaasabi. Töötlevat üksust saab kohustada turvameetmeid rakendama lõike 4 alusel tehtava ettekirjutusega.

Kehtivad punktid 1, 2, 5 ja 8 on üle viidud § 23 uude lõikesse 31.

**Eelnõu § 1 punktiga 17** tunnistatakse kehtetuks RSVS § 23 lõike 3 punktid 3–5. Need punktid viiakse üle lisanduvasse sama paragrahvi lõikesse 31. Selliselt tekib sätete selge struktuur ka VLA teise riigisaladuse kaitse pädevuse osas, milleks on riigisaladuse kaitse välisesindustes. Lõikesse 3 jäävad alles ülesanded, mida VLA täidab välisesindustes riigisaladuse kaitseks. Need on riigisaladuse kaitse korralduse nõuetele vastavuse kontroll, riigisaladuse ja salastatud teabekandjate töötlemise vastavuse nõuete kontroll ning tulenevalt ohuhinnangust turvaalal ebaseaduslikult teabe kogumise seadmete oleku kontroll.

**Eelnõu § 1 punktiga 18** täiendatakse RSVS § 23 lõikega 31. Sättes kirjutatakse lahti tegevused, mis on seotud lõigetes 2 ja 3 sätestatud ülesannete täitmisega. Nende lõigete punktid on enamjaolt sama sisuga nagu kehtiva § 23 lõigetes 2 ja 3 toodud vastavad punktid, kuid järgmiste erisustega.

Punktiga 1 antakse VLA-le õigus anda töötlevale üksusele teavet ja täitmiseks kohustuslikke juhiseid riigisaladuse kaitse nõuete täitmiseks. Kohustuslike juhiste andmise õigus on vajalik selleks, et oleks võimalik suunata töötlevaid üksusi parimal võimalikul viisil riigisaladust kaitsma. Teavet antakse selleks, et töötlevatel üksustel oleks võimalik riigisaladust paremini kaitsta.

Punktis 3 ei ole erinevalt kehtivast samasisulisest punktist (§ 23 lõike 2 punkt 2) soovituste andmist täiendavate turvameetmete rakendamiseks välja toodud, sest see on hõlmatud punktiga 1.

Kehtivas § 23 lõikes 2 ei ole antud VLA-le õigust teha Vabariigi Valitsuse julgeolekukomisjonile ettepanekuid salastatud teabe küberturvalisuse valdkonnas. Samas on selline õigus sätestatud lõikes 3 välisesindustes riigisaladuse kaitse korraldamise ja kontrollimise puhul. Ei ole mõistlikku põhjendust, miks salastatud teabe küberturvalisuse valdkonnas ei tohiks teha Vabariigi Valitsuse julgeolekukomisjonile ettepanekuid. Seetõttu on lõike 31 uues punktis 4 antud VLA-le see õigus mõlema valdkonnaga seonduvalt.

**Eelnõu § 1 punktiga 19** täiendatakse RSVS-i uue §-ga 231, mis reguleerib RJVE ülesandeid ja pädevust riigisaladuse kaitse korraldamisel ja kontrollimisel. Riigisaladuse kaitset korraldavaid asutusi reguleerib üldiselt RSVS § 22, mis määrab nendeks asutusteks KAPO ja Kaitseväe põhimääruses määratud struktuuriüksuse. Praktikas on piiratud ulatuses riigisaladuse kaitse korraldamise ja kontrollimise pädevus ka RJVE-l, kuid seda ei ole RSVS‑is selgelt reguleeritud. Näiteks korraldab RJVE välisriikidega salastatud teabe vastastikuse kaitse kokkulepete sõlmimist, kehtiva § 35 lõike 6 kohaselt tuleb riigisaladuse edastamine välismaale üldjuhul registreerida RJVE juures ja kehtiva RSVKK § 1221 kohaselt peab leping, mille raames edastatakse riigisaladust välismaale, sisaldama eraldi riigisaladuse kaitset käsitlevat osa, mis tuleb kooskõlastada RJVE-ga. Seega ei anta muudatusega RJVE-le uut pädevust ega piirata KAPO või Kaitseväe põhimääruses määratud struktuuriüksuse pädevust riigisaladuse kaitsel, vaid reguleeritakse selgemalt olemasolev RJVE pädevus.

Lõikes 1 kirjeldatakse RJVE üldist pädevust seoses riigisaladuse kaitse korraldamise ja kontrollimisega, milleks on riigisaladuse kaitse korraldamine ja kontrollimine selle avaldamisel välisriigile, rahvusvahelisele organisatsioonile või rahvusvahelise kokkuleppega loodud institutsioonile.

Lõikes 2 kirjeldatakse ülesandeid, mida RJVE seoses lõikes 1 toodud pädevusega täidab. Punktiga 1 reguleeritakse RJVE pädevus salastatud teabe vastastikuse kaitse kokkulepete sõlmimisel. Punktid 2 ja 3 on seotud vastavalt RSVS § 35 uue lõike 41 ja selle alusel antava RSVKK §-ga 233 ning RSVKK 5. peatüki 7. jao kavandatava uue 5. jaotisega. Viimane reguleerib salastatud teabekandja vedamist kaubana ehk juhtudel, kui teabekandjat ei ole selle suuruse, kuju, paigutuse, kaalu, sisu olemuse või suure koguse tõttu võimalik tavapäraselt vedada. Tegu on rahvusvaheliselt väga üksikasjalikult, ent paindlikult reguleeritud salastatud teabe kaitse valdkonnaga, mis tuleb rahvusvaheliste organisatsioonide julgeolekureeglitest ja välislepingutest Eesti õigusesse üle tuua, et seda saaks paremini rakendada. RSVKK-is reguleeritakse seejuures üksikasjalikumalt kaubana vedamiseks pakendamist, vedu saatvaid isikuid, transporti pakkuvaid teenusepakkujaid, rahvusvahelist vedamist ja transpordiplaani koostamist. RJVE poolt riigisaladust sisaldavate salastatud teabekandjate rahvusvaheliselt kaubana vedamise korraldamine ei tähenda seda, et RJVE organiseerib ise veo. Veo korraldamine, sealhulgas vedajaga lepingu sõlmimine, on töötleva üksuse ülesanne. Korraldamine hõlmab selles kontekstis näiteks töötleva üksuse juhendamist ja vajadusel asjakohaste välismaiste ametkondadega suhtlemist.

Välislepingus ettenähtud ülesannete kohta on eraldi punkt 4, sest RJVE peab lähtuma lisaks riigisisesele regulatsioonile salastatud teabe vastastikuse kaitse kokkulepetest ja rahvusvaheliste organisatsioonide liikmesriikidele täitmiseks kohustuslikest õigusaktidest.

Lõikes 3 kirjeldatakse tegevusi, mida RJVE teeb lõikes 1 nimetatud ülesannete täitmiseks. Lõige on sama sisuga nagu KAPO, VLA ja RJVE salastatud välisteabe kaitsega seotud ülesandeid reguleerivates paragrahvides toodud lõiked.

Lõikega 4 sätestatakse erandid, mil RJVE riigisaladuse kaitset ei korralda ega kontrolli. Sarnased erandid on sätestatud kehtivas § 35 lõikes 6. Sättes loetletud teabe osas on teadmisvajadus niivõrd piiratud, et RJVE teenistujatele ei ole võimalik sellele juurdepääsu anda.

Lõigetega 5 ja 6 sätestatakse RJVE õigused nõuete täitmise kontrollimisel ja rikkumise avastamise korral. Sätetega RJVE-le antavad õigused on sarnased KAPO-le, VLA-le ja RJVE‑le salastatud välisteabe valdkonnas antud õigustega.

**Eelnõu § 1 punktiga 20** asendatakse RSVS § 29 lõikes 2 sõnad „ja täiesti salajase taseme riigisaladusele“ tekstiosaga „käesoleva seaduse § 7 punktides 10 ja 11 sätestatud teabele ning täiesti salajase taseme riigisaladusele“.

RSVS § 29 lõikega 2 sätestatakse, et uurimisasutuse, prokuratuuri või kohtu määruse alusel ei lubata juurdepääsu piiratud, konfidentsiaalse või salajase taseme riigisaladusele, kui see seab ohtu kriminaalmenetluse seadustiku § 12614 punktides 2, 4, 5, 6 ja 7 sätestatud õiguste kaitse, ja täiesti salajase taseme riigisaladusele.

Praktilise tegevuse käigus on selgunud, et kaitset vajab ka Kaitseväe korralduse seaduse § 37 lõike 1 punktides 1 ja 2 ning lõikes 2 nimetatud viisil teavet koguva kaitseväeluuret teostava Kaitseväe struktuuriüksuse poolt teabe kogumist kajastav teave, kaasa arvatud kogumiseks kasutatavaid meetodeid, vahendeid ja jälgitavaid objekte käsitlev teave.

Vastavalt RSVS § 7 punktidele 10 ja 11 on riigikaitse riigisaladus kaitseväeluurega tegeleva Kaitseväe struktuuriüksuse poolt Kaitseväe korralduse seaduse § 37 lõike 1 punktides 1 ja 2 ning lõikes 2 nimetatud volituste rakendamisega teabe kogumist kajastav teave, kaasa arvatud kogumiseks kasutatavaid meetodeid, vahendeid ja jälgitavaid objekte käsitlev teave, ning kaitseväeluurealast rahvusvahelist koostööd käsitlev teave, välja arvatud teave, mille avalikuks tulek ei kahjusta Eesti Vabariigi julgeolekut. See teave salastatakse täiesti salajasel või madalamal tasemel kuni 50 aastaks.

Sarnaselt jälitustegevuse teabega on vajalik, et see teave ei saaks näiteks kriminaalmenetluse kaudu teatavaks kõrvalistele isikutele. Seega on vaja täiendada sätet viisil, mis tagab kaitseväeluure kogumist kajastava teabe, kasutatavate meetodite, vahendite ja jälgitavate objektide kaitse uurimisasutuse, prokuratuuri ja kohtu määruse alusel.

**Eelnõu § 1 punktiga 21** tunnistatakse kehtetuks RSVS § 35 lõiked 4–6.

Lõigete 4–52 sisu on viidud üle uude § 201.

Kehtiva § 35 lõike 6 kohaselt tuleb üldjuhul riigisaladuse edastamine välisriigile, rahvusvahelisele organisatsioonile või rahvusvahelise kokkuleppega loodud institutsioonile registreerida RJVE juures. Registreerimiskohustuse kehtestamise algne eesmärk oli võimaldada RJVE-l tagada, et riigisaladust avaldatakse vaid sellistele välisriikidele, kellega Eesti Vabariik on sõlminud salastatud teabe kaitse ja vahetamise kokkuleppe, või rahvusvahelistele organisatsioonidele või rahvusvahelise kokkuleppega loodud institutsioonidele, millega Eesti Vabariik on ühinenud. Aastatepikkuse praktika käigus on aga ilmnenud, et iga üksiku riigisaladust sisaldava teabekandja registreerimine RJVE peetavas põhiregistris tekitab töötlevatele üksustele viivitusi teabe edastamisel ning nõude rakendamine on töötlevatele üksustele liiga koormav ja ebaproportsionaalne.

RJVE-l on tekkinud õiguslike regulatsioonide täiendamise kaudu alternatiivsed võimalused riigisaladuse õiguspärase avaldamise kontrollimiseks muude ülesannete täitmise teel. Ülevaade riigisaladuse avaldamisest välisriigile, rahvusvahelisele organisatsioonile või rahvusvahelise kokkuleppega loodud institutsioonile saadakse RJVE regulaarsete salastatud teabe kaitse kontrollide käigus ning täiendavaks kontrolliinstrumendiks on nõue kooskõlastada RJVE-ga rahvusvahelise tsiviilõigusliku või halduslepingu juurde koostatav riigisaladuse kaitset käsitlev osa.

**Eelnõu § 1 punktiga 22** täiendatakse RSVS § 35 lõikega 7. Säte reguleerib tööstusjulgeoleku olukordi, kus koostöö põhineb tsiviilõiguslikul või halduslepingul ning kus üheks pooleks on juriidiline isik, näiteks ettevõte või avalik-õiguslik ülikool. Kuivõrd tegu ei ole riigiasutuste ega rahvusvahelise õiguse subjektidega, siis on salastatud teabe kaitse kokkulepete ning rahvusvahelise praktika järgi nende poolt salastatud teabe töötlemisele (sh edastamisele) kehtestatud täiendavad nõuded. Need nõuded kehtestatakse RSVKK-is, kus on sarnased nõuded ka salastatud välisteabe edastamise puhul.

**Eelnõu § 1 punktiga 23** muudetakse RSVS § 49 lõiget 3. Muudatuse tulemusel antakse komisjonile õigus teha ettepanek julgeolekukontrolli läbimise kohta isikule või organile, kelle pädevuses on julgeolekukontrolli läbimise otsustamine. Muudatus seondub eelnõuga kavandatava § 51 lõikega 8, mille kohaselt otsustab julgeolekukontrolli teostav asutus, kas isik on julgeolekukontrolli läbinud. Selleks et julgeolekukontrolli teostaval asutusel oleks võimalik julgeolekukontrolli läbimise kohta otsus teha, peab komisjonil olema õigus vastav ettepanek teha.

**Eelnõu § 1 punktiga 24** muudetakse RSVS § 50 lõikeid 1 ja 2. Lõike 1 muudatusega tuuakse RSVS-i tasandile praegu RSVKK §-s 114 nimetatud põhimõte kahe täiendusega.

Kehtivas § 50 lõikes 1 on kasutusel sõnastus „salastatud välisteabele kohaldatakse selle salastatuse tasemele vastavale riigisaladusele kohaldatavaid sätteid“. Kehtivas RSVKK §-s 114 on kasutatud sõna „töötlemine“. Sellise sõnastuse puhul ei ole üheselt selge, kas ka salastatud välisteabe kaitsega seotud tegevustele, mille raames otseselt salastatud välisteavet ei töödelda, tuleb kohaldada vastava tasemega riigisaladuse sätteid või mitte. Näiteks on ebaselge, kas turva- või administratiivala loomisele, kus töödeldakse salastatud välisteavet, kohaldub RSVS § 50 lõikes 1 sätestatud üldreegel. RSVS § 50 lõike 1 uue sõnastuse eesmärk on hõlmata kõik salastatud välisteabe kaitsega seotud aspektid selgelt ühe üldreegli alla. Sätte kohaselt kohaldatakse salastatud välisteabe *kaitsel* välislepingust tulenevaid nõudeid, arvestades käesolevas peatükis ja RSVS-i alusel antud õigusaktides sätestatud erisusi. Sättes kasutatud sõna „kaitse“ hõlmab ka salastatud välisteabe töötlemist. Sarnaselt on töötlemine hõlmatud riigisaladuse kaitse alla RSVS 2. peatüki 3. jaos „Riigisaladuse kaitse“. Nii on selgelt hõlmatud ka turva- ja administratiivalade loomisega seotud tegevused.

Teiseks on muudatuse eesmärk sätestada RSVS-is, et välislepingust tuleneva nõudena käsitatakse ka rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooni liikmesriikidele täitmiseks kohustuslikust õigusaktist tulenevaid nõudeid. Senises rakenduspraktikas on segadust tekitanud see, kas näiteks Euroopa Liidu või NATO õigusaktidest tulenevad nõuded on täitmiseks kohustuslikud.

Praktikas tuleb välislepingust tulenevaid nõudeid rakendada Euroopa Liidu ja NATO salastatud välisteabe kaitsel, sest nimetatud organisatsioonid on kehtestanud oma salastatud teabe kaitsmiseks eraldi regulatsioonid. Välisriikide salastatud välisteavet tuleb üldjuhul kaitsta sarnaselt riigisaladusega, sest välisriikidega sõlmitud salastatud teabe vastastikuse kaitse kokkulepped üldiselt sätestavad, et teise riigi salastatud teavet tuleb kaitsta sarnaselt enda riigi salastatud teabega. Mõnikord on välisriigiga sõlmitud kokkuleppes siiski välja toodud erisused, näiteks piiratud tasemel salastatud teabe kaitsmise puhul. Sel juhul tuleb rakendada lisaks riigisaladuse kaitse nõuetele ka vastavas salastatud teabe vastastikuse kaitse kokkuleppes toodud erisusi.

Turvaalade loomisel see suurt muudatust ei too, sest üldised turvaala nõuded ei erine regulatsioonides olulisel määral. Küll aga võib rahvusvahelistes regulatsioonides olla erisusi turvaala kasutamise puhul. Nii näiteks vastab NATO klass II turvaala Eesti turvaala üldisele regulatsioonile, kuid NATO klass I turvaala puhul tuleb arvestada teatud erisusi. Klass I turvaalale sisenedes saadakse kohe juurdepääs salastatud teabele. Seal töödeldava teabe salastatuse tase peab esiteks olema selgelt määratletud ning teiseks peab turvaala sissepääsukontrollisüsteem arvestama nii juurdepääsuõigust vastavale salastatuse tasemele kui ka konkreetse teabe teadmise vajadust. Analoogselt on turvaalade kasutamist reguleeritud Euroopa Liidu salastatud teabe kaitse regulatsioonides. Eestis on seni selliseid turvaalasid loodud Kaitseväes ning see on reguleeritud RSVKK §-dega 39–40, mis reguleerivad isikute viibimist turvaalal ja iseseisva sissepääsuõigusega isiku pääsu turvaalale.

RSVS § 50 lõikes 1 sätestatud üldpõhimõttest on võimalik teha erisusi RSVS 3. peatükis. Näiteks on seda tehtud § 51 lõikes 1, mille kohaselt tuleb salastatud välisteabele juurdepääsu õiguse ja salastatud välisteabe töötlemise õiguse andmise korral välislepingust lähtuda vaid juhul, kui seal on sätestatud rangemad või täiendavad nõuded võrreldes RSVS-i nõuetega. Näiteks kui välislepingus on sätestatud rangemad või täiendavad juurdepääsu- või töötlemisõiguse andmisest keeldumise alused võrreldes RSVS-iga, siis tuleb RSVS-ist erinevas osas lähtuda nimetatud nõuetest. Lisaks RSVS 3. peatükis sätestatud erisustele võib Vabariigi Valitsus § 50 lõike 7 või 8 alusel sätestada RSVKK-is või kaitseminister krüptomaterjalide töötlemist või kiirgusturvet reguleerivates määrustes RSVS § 50 lõikes 1 sätestatud üldpõhimõttest erisusi. Hulk erisusi ja täpsustusi on sätestatud näiteks RSVKK 5. peatüki 10. jaos „Salastatud välisteabe kaitse“.

Paragrahvi 50 lõike 2 kehtiva sõnastuse ajel pöörduvad rakendajad RJVE poole peaaegu alati, kui neile edastatud teave on märgistatud viisil, mis võib viidata selle salastatusele. Rakendajate ootus on, et RJVE teostab riigisaladuse ja salastatud välisteabe kaitsemeetmete võrdluse ning määrab selle pinnalt riigisaladuse ja rakendajale edastatud salastatud välisteabe salastatuse taseme vastavuse. Selline ootus on põhjendatud, kuid praktikas on RJVE jaoks ülesande täitmine kaitsemeetmete võrdluseks vajalike välismaiste regulatsioonide kättesaamatuse tõttu raskendatud ja seetõttu on otsuse tegemiseks kuluv aeg ebamõistlik. Eesti Vabariik lepib välisriigiga salastatud teabe vastastikuses kaitsmises kokku üldjuhul salastatud teabe vastastikuse kaitse kokkuleppe sõlmimise teel. Rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooni salastatud välisteabe kaitsmise kohustuse võtab Eesti Vabariik üldjuhul organisatsiooni või institutsiooniga ühinedes. Kui välisriigiga ei ole kokkulepet sõlmitud või Eesti Vabariik ei ole rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooniga ühinenud, ei ole üldjuhul vaja selle välisriigi, organisatsiooni või institutsiooni salastatud välisteavet riigisaladusega sarnaselt kaitsta. Sellise välisriigi, rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooni poolt edastatud juurdepääsupiirangu märkega teave tuleb lugeda avaliku teabe seaduse § 35 lõike 3 alusel asutusesiseseks kasutamiseks mõeldud teabeks ilma RJVE poole pöördumata. Edaspidi määrab RJVE riigisaladuse ja salastatud välisteabe salastatuse taseme vastavuse vaid kahel juhul.

Esiteks võib selline olukord tekkida siis, kui välislepingus ei ole salastatuse taseme vastavust kokku lepitud. Sellisel juhul on Eesti Vabariik ja välisriik sõlminud salastatud teabe vastastikuse kaitse kokkuleppe või on Eesti Vabariik välislepingu sõlmimise kaudu ühinenud rahvusvahelise organisatsiooni või rahvusvahelise institutsiooniga, kuid välislepingus ei ole salastatuse taseme vastavust kokku lepitud. Näiteks on Eesti ühinenud Rahvusvahelise Kriminaalkohtu (ICC) Rooma statuudiga (RT II 2002, 2, 5), mille artikli 87 lõige 3 kohustab osalisriike hoidma kohtu dokumente „konfidentsiaalsena“, kuid ei loetle ega täpsusta osalisriikide ja kohtu salastatud teabe võrdväärsust tasemeti.

Teiseks võib selline olukord tekkida siis, kui välislepingut ei ole sõlmitud, kuid välisriigi, rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooni salastatud välisteabe kaitsmine on Eesti Vabariigi huvides. Säte loob seega võimaluse kaitsta salastatud välisteavet juhul, kui salastatud teabe vastastikuse kaitse kokkulepet ei ole sõlmitud. Välisriik ei pruugi salastatud teabe vastastikuse kaitse kokkuleppeid sõlmida, salastatud välisteavet võib olla vaja töödelda enne kokkuleppe sõlmimist (näiteks ka läbirääkimiste ajal) või salastatud välisteabe töötlemise vajadus võib olla niivõrd lühiajaline, näiteks seotud konkreetse projektiga, et salastatud teabe vastastikuse kaitse kokkuleppe sõlmimisele ei ole mõistlik ressurssi kulutada. RSVS-i järgi pole ilma välislepinguta lubatud teisele poolele avaldada riigisaladust ilma Vabariigi Valitsuse julgeolekukomisjoni loata, kuid käesolev säte võimaldab teise poole salastatud välisteavet Eestis salastatud välisteabena kaitsta, kui Eesti Vabariigi huvides on teha välisriigi, rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooniga koostööd, mille raames edastab teine pool Eesti Vabariigile enda salastatud välisteavet. Sellisel juhul tuleb pöörduda RJVE poole, kes suhtleb vajaduse korral teise poole pädeva asutusega, teostab vajaduse korral riigisaladuse ja salastatud välisteabe kaitsemeetmete võrdluse ja määrab riigisaladuse ja salastatud välisteabe salastatuse tasemete vastavuse. Otsus taseme vastavuse määramise kohta tuleb avaldada RJVE veebilehel.[[11]](#footnote-11) Normis ei ole teadlikult täpsustatud, kes ja millisel viisil otsustab, et salastatud välisteabe kaitsmine on konkreetsel juhul Eesti Vabariigi huvides. Salastatud välisteabe töötlemine ei ole eesmärk omaette, vaid kaasneb mingi tegevusega, mis omakorda tuleneb poliitilisel tasandil langetatud otsusest. Seepärast sõltub see, millal tuleks pöörduda RJVE poole, konkreetsetest asjaoludest. Näiteks võib olla Eesti huvides kaitsta strateegiliselt oluliste partnerite või rahvusvahelisel sõjalisel missioonil osalevate partnerite salastatud välisteavet, sest selle volitamata avalikustamine põhjustaks kahju nii riikidevahelisele koostööle kui ka Eesti riigi mainele. Niisamuti tuleks Eesti Vabariigi huvi eeldada olukorras, kus salastatud teabe kaitse kokkuleppe läbirääkimisi on juba alustatud, kuid salastatud teavet on vaja vahetada juba enne kokkuleppe sõlmimist. Eesti Vabariigi huvi tuleks eeldada ka oluliste rahvusvaheliste organisatsioonide nagu Euroopa Liidu ja NATO liikmesriikide puhul.

Normis on eraldi välja toodud võimalus tunnistada salastatud välisteave asutusesiseseks kasutamiseks mõeldud teabeks, sest mõnel juhul ei vasta salastatud välisteabe kaitsemeetmed ühegi riigisaladuse taseme suhtes rakendatavatele kaitsemeetmetele. Sellisel juhul ei ole põhjendatud salastatud välisteavet sarnaselt riigisaladusega kaitsta.

Muudetud sõnastusest on välja jäetud kaitsemeetme vastavuse võrdluse teostamine, sest seda ei ole alati riigisaladuse ja salastatud välisteabe tasemete vastavuse määramiseks vaja teha. Tuleb arvestada, et niisuguse võrdluse tegemine on samuti ressursikulu, sest RJVE peab selle jaoks välja uurima teise riigi salastatud teabe kaitse reeglid ning võrdlema neid riigisaladuse kaitse reeglitega. Eelkõige saab võrdluse jätta tegemata välisriikide puhul, mis kuuluvad Euroopa Liitu ja/või NATO-sse, kuid millega Eesti Vabariik ei ole sõlminud salastatud teabe vastastikuse kaitse kokkulepet. Nende riikide salastatud teabe kaitsemeetmed on üldjuhul üksteisega sarnased ning Euroopa Liidu ja NATO julgeolekureeglite koostamisel on nende liikmesriikide salastatuse tasemeid Euroopa Liidu või NATO salastatuse tasemetega juba võrreldud. Seega saab taseme vastavuse riigisaladuse tasemele määrata ilma kaitsemeetmete võrdlust tegemata.

**Eelnõu § 1 punktiga 25** täiendatakse RSVS § 50 lõikega 21. Ilma täienduseta võib seaduse rakendajatele jääda arusaamatuks, kuidas tuleb käituda juurdepääsupiirangu märkega teabega, mille kohta RJVE § 50 lõike 2 alusel otsust ei tee. Segaduse vältimiseks viidatakse lõikes 21 avaliku teabe seadusele, mis sellist olukorda reguleerib. Keskne säte on avaliku teabe seaduse § 35 lõige 3, mille kohaselt välisriigi või rahvusvahelise organisatsiooni poolt edastatud juurdepääsupiirangu märkega teave, mida ei loeta vastavalt riigisaladuse ja salastatud välisteabe seadusele salastatud välisteabeks, loetakse asutusesiseseks kasutamiseks mõeldud teabeks. Lisaks on asjakohased veel avaliku teabe seaduse § 40 lõige 11, § 41 lõige 3 ja § 42 lõige 21.

**Eelnõu § 1 punktiga 26** muudetakse RSVS § 50 lõiget 4. Muudatuse tulemusel reguleerib säte vaid töötleva üksuse enda loodud salastatud välisteabe ebaõige salastatuse kustutamist või salastamisandmete parandamist, sest sel juhul on loogiline teha seda riigisaladusega sarnaselt §-s 15 sätestatud korras. Juhul kui teavet on edastatud teisele töötlevale üksusele, tuleb seda töötlevat üksust teavitada.

Kui salastatud välisteabe on loonud keegi teine, tuleb teavitada RJVE-d, sest salastatud välisteabe puhul, mida ei ole loonud töötlev üksus, tuleb üle kontrollida, kas salastatus tuleb kustutada või salastamisandmeid parandada. Kuna konkreetsete juhtumite asjaolud on erinevad, ei ole selles osas otstarbekas eraldi normi sõnastada. RJVE suhtleb vajaduse korral salastatud välisteabe avaldajaga, et saada edasised juhised, või annab ise töötlevale üksusele juhise, näiteks kui salastatud välisteabe avaldajat ei ole võimalik tuvastada või kui salastatud välisteabe avaldajat enam ei ole.

**Eelnõu § 1 punktiga 27** täiendatakse RSVS § 50 lõigetega 51 ja 52. Uue lõikega 51 sarnane norm on kehtivas õiguses RSVS § 52 lõige 5, mis tunnistatakse kehtetuks. Kehtiva RSVS § 52 lõike 5 kohaselt antakse salastatud välisteavet sisaldavad teabekandjad neid valdava töötleva üksuse tegevuse lõpetamisel viivitamata üle RJVE-le. Kehtival sõnastusel on mitu puudujääki.

Esiteks ei anta salastatud välisteavet sisaldavaid teabekandjaid alati üle RJVE-le. Kui salastatud teabekandja sisaldab nii riigisaladust kui ka salastatud välisteavet, on osal juhtudel mõistlik jätta see KAPO valdusesse. See, kelle valdusesse konkreetne salastatud teabekandja jääb, räägitakse läbi KAPO ja RJVE vahel. Uue sõnastuse kohaselt tuleb RJVE-le kindlasti üle anda vaid salastatud teabekandjad, mis sisaldavad üksnes salastatud välisteavet.

Teiseks ei ole töötleva üksuse tegevuse lõpetamine ainus juhtum, kus RJVE-le tuleks salastatud teabekandjad üle anda. Selline vajadus võib tekkida ka juhul, kui lõppeb isiku salastatud välisteabele juurdepääsu õigus või salastatud välisteabe töötlemise õigus. Seda juhul, kui salastatud teabekandjaid ei saa üle anda isikule, kelle jaoks või ülesandel salastatud välisteavet loodi või töödeldi. Seetõttu on uues sõnastuses tehtud viide § 19 lõikele 8 ning § 20 lõigetele 8 ja 9.

Kolmandaks ei paikne kehtiv RSVS § 52 lõige 5 õiges kohas. RSVS §-s 52 on sätestatud RJVE pädevus. RSVS § 52 lõige 5 sobitub olemuselt RSVS §-s 50 toodud üldsätete alla.

RSVS § 50 täiendatakse uue lõikega 52. Euroopa Liidu ja NATO õigusaktidest tulenevalt tuleb igal liikmesriigil määrata riigi julgeoleku volitatud esindaja, riigi töötlussüsteemide akrediteerimise volitatud esindaja, riigi turbelahenduste volitatud esindaja, riigi krüptohalduse volitatud esindaja ja riigi kiirgusturbe volitatud esindaja.

Lisaks eelnevatele võib liikmesriik määrata riigi tööstusjulgeoleku volitatud esindaja, mille on määranud enamik Euroopa Liidu ja NATO liikmesriike ning mille määramine Eestis on otstarbekas selleks, et luua selgus pädeva asutuse ja ühtse kontaktpunkti osas.

Seni on Eestis õigusakti tasandil määratud vaid RJVE. Praktikas on teisi loetletud rolle täitnud samuti RJVE ja VLA, kuid õigusakti tasandil ei ole seda sätestatud. Muudatuse toimel saab Vabariigi Valitsus õiguse määrata rollide täitjad RSVKK-s.

**Eelnõu § 1 punktiga 28** muudetakse RSVS § 50 lõiget 7. Kehtivas sõnastuses on loetletud hulk norme, mille alusel kehtestatud määrustes võib Vabariigi Valitsus teha erisusi salastatud välisteabe kaitsel. Tegelikkuses on normide alusel kehtestatud üks määrus – RSVKK. Arusaadavuse huvides tuleb selgelt viidata RSVKK-le, nagu on paljudes teistes RSVS-i normides tehtud.

**Eelnõu § 1 punktiga 29** muudetakse RSVS § 51. Kuna muudatused ja täiendused on suuremahulised, on otstarbekas kehtestada paragrahv tervikuna uuesti. Suuremad muudatused on järgmised:

Esiteks reguleeritakse paragrahvis edaspidi salastatud välisteabele juurdepääsu õiguse andmise kõrval selgelt ka salastatud välisteabe töötlemise õiguse andmist. Seni on salastatud välisteabele juurdepääsu õiguse ja salastatud välisteabe töötlemise õiguse andmist eristatud ainult RSVKK tasemel. Eristus tehti juba RSVKK algses tekstis. RSVKK 05.06.2023 jõustunud muudatustega eristati RSVKK-s täiendavalt juurdepääsusertifikaat ja töötlemissertifikaat. Enne seda anti nii juurdepääsuõigus kui ka töötlemisõigus juurdepääsusertifikaadiga. Selleks et rakendajate jaoks selgelt eristada juurdepääsuõigus ja töötlemisõigus, tuleb eristus teha juba RSVS-i tasemel.

Teiseks sätestatakse RSVKK asemel RSVS-i tasandil RJVE õigus anda isikule Euroopa Liidu või NATO salastatud välisteabele juurdepääsuõigus või salastatud välisteabe töötlemise õigus ning eristatakse juurdepääsu- või töötlemisõiguse andmise otsustamine julgeolekukontrolli läbimise otsustamisest. Juurdepääsu- või töötlemisõiguse andmise otsustaja on praegu nimetatud RSVKK-s. RSVKK § 129 lõike 2 kohaselt otsustab juurdepääsu- või töötlemissertifikaadi andmise või sellest keeldumise RJVE. RSVKK §-s 1291 on sama õigus antud RJVE-le teatud juhtudel piiratud taseme Euroopa Liidu või NATO salastatud välisteabe puhul. Julgeolekukontrolli läbimise otsustaja on ära toodud eriseadustes, näiteks kohtute seaduse § 81 lõikes 5, Vabariigi Valitsuse seaduse § 31 lõikes 5 ja Riigikogu liikme staatuse seaduse § 19 lõikes 8, kuid RSVS-i tasandil ei ole seda nimetatud. Et tagada rakendajatele selgus, tuleb RSVS-i tasandil sätestada, kes otsustab julgeolekukontrolli läbimise üldjuhul.

Kolmandaks sätestatakse juurdepääsu- või töötlemisõiguse kehtetuks tunnistamise ja kehtivuse lõppemise alused RSVKK asemel RSVS-i tasandil. Kuna juurdepääsu- või töötlemisõiguse kehtetuks tunnistamisega või kehtivuse lõppemisega kaasneb sarnaselt juurdepääsu- või töötlemisõiguse andmisest keeldumisega isiku põhiõiguste piiramine, siis tuleb vastavad alused sätestada RSVS-i tasandil. Vastavad RSVKK normid tunnistatakse kehtetuks.

Neljandaks ei reguleerita paragrahvis enam seda, millistest RSVS-i sätetest tuleb salastatud välisteabele juurdepääsu õiguse või salastatud välisteabe töötlemise õiguse andmisel lähtuda. Vastav üldreegel kehtestatakse edaspidi RSVS § 50 lõikega 1. Lähtuda tuleb RSVS-i juurdepääsuloa, töötlemisloa ja julgeolekukontrolliga seonduvat reguleerivatest normidest, arvestades RSVS §-s 51 sätestatud erisusi ja RSVS § 51 lõike 13 alusel RSVKK-s sätestatud korda.

Viiendaks ei ole paragrahvis edaspidi enam välja toodud seda, et kui välislepingust tulenevad juurdepääsuõiguse andmisest keeldumise alused on rangemad võrreldes RSVS-is sätestatud alustega, siis kontrollitakse julgeolekukontrolli teostades ka välislepingust tuleneva asjaolu esinemist ja vastava asjaolu esinemine on salastatud välisteabele juurdepääsu õiguse andmisest keeldumise alus. Vastav põhimõte tuleneb edaspidi § 51 lõike 1 teisest lausest. Rangemad või täiendavad nõuded hõlmavad ka seda, kui juurdepääsuõiguse või töötlemisõiguse andmisest keeldumise alused on rangemad võrreldes RSVS-is sätestatud keeldumise alustega.

Kuuendaks ei ole paragrahvis enam lauset, milles on sätestatud, et kui salastatud välisteabe avaldaja keelab isikule juurdepääsuõiguse andmise, ei anta isikule õigust juurdepääsuks vastavale salastatud välisteabele. Sellist olukorda praktikas ei esine. On ka raske näha, et salastatud välisteabe avaldajal oleks põhimõtteliselt võimalik keelata isikule salastatud välisteabele juurdepääsu õiguse või salastatud välisteabe töötlemise õiguse andmine. Kui mõni salastatud välisteabe avaldaja peaks soovima mõne isiku õigust enda avaldatud salastatud välisteabele juurde pääseda piirata, lahendatakse see teadmisvajaduse põhimõtte alusel.

Seitsmendaks on kustutatud kehtiv § 51 lõige 5, kuna praktikas seda ei rakendata. Julgeolekukontrolli teostavad asutused ei soovi saada RJVE-lt infot füüsilistele või juriidilistele isikutele salastatud välisteabele juurdepääsu sertifikaatide ja salastatud välisteabe töötlemise sertifikaatide andmise või nende kehtetuks tunnistamise kohta.

Kokkuvõtlikult on RSVS-is edaspidi reguleeritud juurdepääsu- ja töötlemisõiguse saamise eeltingimused, juurdepääsu- või töötlemisõiguse andmisega seotud erisused ning juurdepääsu- või töötlemisõiguse lõppemise alused. RSVKK-s on edaspidi reguleeritud Euroopa Liidu või NATO salastatud välisteabele juurdepääsu õiguse ja salastatud välisteabe töötlemise õiguse taotlemine, kehtivusaja määramine, taotluses puuduste kõrvaldamine ja otsuse tegemise tähtaeg, Euroopa Liidu ja NATO salastatud välisteabe kaitse nõuete tutvustamine, sertifikaadi vormistamine ja edastamine ning taotleja teavitamiskohustus andmete muutumisest.

Järgnevalt on selgitatud muudatusi lõigete kaupa.

Lõikega 1 sätestatakse erand § 50 lõikes 1 sätestatud üldreeglist, mille järgi kohaldatakse salastatud välisteabe kaitsel välislepingust tulenevaid nõudeid. RSVS § 51 lõike 1 toimel kohaldatakse salastatud välisteabele juurdepääsu õiguse ja salastatud välisteabe töötlemise õiguse andmisel riigisaladusele juurdepääsuõiguse ja riigisaladuse töötlemise õiguse andmise nõudeid. Välislepingust tulenevaid nõudeid kohaldatakse vaid juhul, kui need on rangemad kui RSVS-is või selle alusel antud õigusaktides sätestatud nõuded või kui RSVS-is või selle alusel antud õigusaktides ei ole nõudeid sätestatud. Näiteks piiratud tasemel Euroopa Liidu või NATO salastatud välisteabe töötlemisõiguse saamiseks ei ole Euroopa Liidu ja NATO regulatsiooni kohaselt vaja julgeolekukontrolli läbida. Piiratud tasemel salastatud riigisaladuse töötlemisõiguse saamiseks tuleb aga julgeolekukontroll läbida ehk RSVS-i nõuded on selles osas rangemad. RSVS § 51 lõike 1 toimel tuleb seega ka Euroopa Liidu või NATO piiratud tasemel salastatud välisteabe töötlemisõiguse saamiseks julgeolekukontroll läbida.

Lõike 2 eesmärk on sätestada kohustus tutvustada isikule enne salastatud välisteabele juurdepääsu õiguse andmist salastatud välisteabe kaitse nõudeid ja võtta selle kohta kinnitus, kui välisleping seda nõuab. Salastatud välisteabe kaitse nõuete tutvustuse läbimise nõue on ära toodud lisaks Euroopa Liidu ja NATO regulatsioonidele ka mitmes Eesti Vabariigi poolt välisriigiga sõlmitud salastatud teabe vastastikuse kaitse kokkuleppes (nt Iisrael, Ühendkuningriik). Kui muus osas kaitstakse salastatud teabe vastastikuse kaitse kokkulepete kohaselt välisriigi salastatud välisteavet üldjuhul nagu riigisaladust, siis see on oluline erisus ning seetõttu on normi sõnastuses lisaks Euroopa Liidu ja NATO salastatud välisteabele nimetatud ka muud salastatud välisteavet.

Euroopa Liidu ja NATO salastatud välisteabe puhul tuleb tutvustada vastava organisatsiooni salastatud välisteabe kaitse nõudeid ja võtta kinnitus RSVKK lisas 13 sätestatud vormil.

Muu salastatud välisteabe puhul tuleb tutvustada RSVS §-s 19 sätestatud kohustusi ja võtta RSVS § 27 lõike 10 punktis 2 nimetatud kinnitus RSVKK lisas 6 sätestatud vormil. Kuna salastatud välisteabele juurdepääsu õiguse saamise eeltingimus on vastava taseme riigisaladusele juurdepääsu õiguse omamine, siis üldjuhul on nõuded juba tutvustatud ja isik kinnituse allkirjastanud. Nimetatud toiminguid uuesti teha ei ole vaja. Kaitseväe juhatajal ja Andmekaitse Inspektsiooni juhil on aga ametikohajärgne juurdepääsu õigus salastatud välisteabele, mille tõttu ei tutvustata neile RSVS §-s 19 sätestatud nõudeid ega võeta kinnitust. Nendele salastatud välisteabe nõuete tutvustamist ei reguleeri ka ükski eriseadus. Kui nimetatud isikutel on vaja juurdepääsu salastatud välisteabele, millele juurdepääsu saamise eeltingimus on välislepingu kohaselt tutvustuse läbimine, siis tuleb neile tutvustada RSVS §‑s 19 sätestatud nõudeid ja võtta selle kohta kinnitus.

Vabariigi Presidendile ei tutvustata salastatud välisteabe kaitse nõudeid ega võeta kinnitust. Sarnaselt ei pea Vabariigi President läbima salastatud välisteabele juurdepääsu õiguse saamiseks julgeolekukontrolli, isegi kui see on välislepingu järgi kohustuslik.

Lõikega 3 luuakse õiguslik alus salastatud välisteabele juurdepääsu õiguse andmisest keeldumiseks isikule, kes ei nõustu endale salastatud välisteabe kaitse nõuete tutvustamise või kinnituse allkirjastamisega. Kehtivas õiguses selleks selge õiguslik alus puudub. Kuigi keelduda saaks põhimõtteliselt ka välislepingu alusel, on selguse huvides mõistlik alus RSVS‑is eraldi välja tuua.

Lõikega 4 tuuakse RSVS-i tasemele seni RSVKK §-des 123–124 reguleeritud Euroopa Liidu ja NATO salastatud välisteabele juurdepääsu õiguse ja salastatud välisteabe töötlemise õiguse saamise eeltingimused.

Lõikega 5 analoogne norm on kehtivas õiguses sätestatud RSVKK §-s 1291. Vastav norm tunnistatakse RSVKK-s kehtetuks.

Lõikega 6 tuuakse välja, et Euroopa Liidu või NATO konfidentsiaalsel või kõrgemal tasemel salastatud välisteabele juurdepääsu õiguse ja salastatud välisteabe töötlemise õiguse saamise eeltingimus on julgeolekukontrolli läbimine. Juurdepääsuõiguse saamiseks ei pea julgeolekukontrolli läbima § 27 lõikes 1 nimetatud isikud, sest neil on seadusest tulenevate ülesannete täitmiseks ametikohajärgne juurdepääsuõigus kõigile salastatud välisteabe tasemetele. Lõike esimene lause ei sätesta otseselt erisust võrreldes riigisaladusele juurdepääsu õiguse või riigisaladuse töötlemise õiguse saamisega, kuid selguse huvides tuleb see välja tuua.

Lõike teise lause kohaselt peavad erandina ka § 27 lõikes 1 nimetatud isikud, välja arvatud Vabariigi President, juurdepääsuõiguse saamiseks julgeolekukontrolli läbima, kui välislepingu kohaselt on julgeolekukontrolli läbiviimine salastatud välisteabele juurdepääsu õiguse andmise kohustuslik eeltingimus. Sama sisuga säte on kehtivas RSVS-is § 51 lõige 3.

Lõige 7 on sama sisuga nagu kehtiva § 51 lõige 41. Normi mõte on sama, aga võrreldes kehtiva sõnastusega on normi uues sõnastuses räägitud Euroopa Liidu ja NATO salastatud välisteabest. Normi kohta on antud selgitus eelnõu 410 SE (riigisaladuse ja salastatud välisteabe seaduse, avaliku teabe seaduse ning avaliku teenistuse seaduse muutmise seadus) seletuskirjas (lk 53).

Lõikega 8 sätestatakse, et julgeolekukontrolli läbimise otsustab üldjuhul julgeolekukontrolli teostav asutus. Tegemist ei ole otseselt erisusega võrreldes riigisaladuse kaitse nõuetega. Ka riigisaladusele juurdepääsuõiguse või riigisaladuse töötlemise õiguse taotlemise korral otsustab julgeolekukontrolli läbimise üldjuhul julgeolekukontrolli teostav asutus. See tuleb siiski eraldi välja tuua, et oleks selge, et RJVE õigus otsustada Euroopa Liidu või NATO konfidentsiaalsel või kõrgemal tasemel salastatud välisteabele juurdepääsu õiguse või salastatud välisteabe töötlemise õiguse andmist ei hõlma õigust otsustada, kas isik on julgeolekukontrolli läbinud. Selle otsuse teeb enne juurdepääsu- või töötlemisõiguse andmise otsustamist julgeolekukontrolli teostav asutus või eriseaduses (näiteks Vabariigi Valitsuse seadus, Riigikogu liikme staatuse seadus) nimetatud pädev otsustaja. Sisuliselt on otsuse näol tegemist eelhaldusaktiga. RJVE võtab otsuse aluseks ja kontrollib muude juurdepääsuõiguse või töötlemisõiguse saamise eeltingimuste täidetust (näiteks kas isik omab juurdepääsuvajadust ning on esitanud nõutud dokumendid, läbinud salastatud välisteabe kaitse nõuete tutvustuse ja allkirjastanud salastatud välisteabe hoidmise kinnituse).

Lõigetega 9–10 sätestatakse Euroopa Liidu ja NATO salastatud välisteabele juurdepääsu õiguse ja salastatud välisteabe töötlemise õiguse andmisega seotud erisused võrreldes riigisaladusele juurdepääsu õiguse ja riigisaladuse töötlemise õiguse andmisega. Erisusi sätestamata annaks lõigetes 8 ja 9 kirjeldatud juhul juurdepääsu- või töötlemisõiguse julgeolekukontrolli läbi viinud asutus, kui eriseaduses ei ole sätestatud teisiti. Riigi julgeoleku volitatud esindaja väljastab juurdepääsuõiguse ja töötlemisõiguse tõendamiseks vastavalt juurdepääsu- või töötlemissertifikaadi.

Lõiked 11 ja 12 on üle toodud RSVKK-st. Kuna juurdepääsu- või töötlemisõiguse kehtetuks tunnistamise või kehtivuse lõppemisega kaasneb sarnaselt juurdepääsu- või töötlemisõiguse andmisest keeldumisega isiku põhiõiguste piiramine, siis tuleb vastavad alused sätestada RSVS-i tasandil. Vastavad RSVKK normid tunnistatakse kehtetuks. Lõikes 10 välja toodud põhimõtted on sarnased riigisaladuse puhul kehtivate põhimõtetega, kuid eraldi normi on siiski vaja, sest riigisaladuse ja salastatud välisteabe juurdepääsu- või töötlemisõiguse kehtetuks tunnistamise puhul on mõningad erinevused. Näiteks ei ole riigisaladuse töötlemisõiguse saamise eeltingimuseks töötlemisvajaduse olemasolu. Samuti võivad Euroopa Liidu või NATO salastatud välisteabele juurdepääsu õiguse või salastatud välisteabe töötlemise õiguse kehtetuks tunnistamise alused tuleneda välislepingust.

Lõige 13 on sarnane kehtiva § 51 lõikega 6. Võrreldes kehtiva normiga on uuest sõnastusest välja jäetud andmisest keeldumine, kehtivuse pikendamine ja kehtivuse lõppemine, sest juurdepääsu- või töötlemisõiguse andmise või sellest keeldumise otsustajad ja kehtivuse lõppemise alused on sätestatud RSVS-is ning pikendamist RSVKK-s ei reguleerita.

Lõikega 14 nähakse Vabariigi Valitsusele ette võimalus nimetada riigisaladuse ja salastatud välisteabe kaitse korras täiendavaid rahvusvahelisi organisatsioone või rahvusvahelise kokkuleppega loodud institutsioone, mille salastatud välisteabele juurdepääsu õiguse ja salastatud välisteabe töötlemise õiguse andmisel kohaldatakse RSVS § 51 lõigetes 4–13 sätestatud nõudeid. Eesti võib lisaks Euroopa Liidule ja NATO-le ühineda teiste rahvusvaheliste organisatsioonide või rahvusvahelise kokkuleppega loodud institutsioonidega, mis on kehtestanud enda salastatud välisteabe kaitseks oma reeglid. Praegu on selline rahvusvaheline organisatsioon vaid Euroopa Kosmoseagentuur, kuid kõiki niisuguseid rahvusvahelisi organisatsioone ja rahvusvahelise kokkuleppega loodud institutsioone ei ole mõistlik Euroopa Liidu ja NATO kõrval seaduses loetleda, sest see muudaks organisatsioonide ja institutsioonide lisandumisel sätted väga pikaks ja raskesti loetavaks.

**Eelnõu § 1 punktiga 30** muudetakse RSVS § 52 lõiget 1. Muudatuse eesmärk on tekitada seadusesse sarnane struktuur RJVE pädevuse, ülesannete ja nende täitmiseks tehtavate tegevuste osas, nagu on sätestatud §-des 22, 23 ja 231.

Seni lõikes 1 olnud ülesanded ja tegevused viiakse üle teistesse sätetesse. Lõikes 1 sätestatakse RJVE pädevus – salastatud välisteabe kaitse korraldamine ja nõuetele vastavuse kontroll.

**Eelnõu § 1 punktiga 31** täiendatakseRSVS § 52 lõigetega 11 ja 12. Täiendusega luuakse olukord, kus konkreetsed ülesanded pädevuse täitmiseks ja ülesannetega seotud tegevused on esitatud eraldiseisvate sätetena.

Lõikes 11 on kaheksa punkti.

Punktid 1, 6, 7 ja 8 vastavad kehtiva RSVS § 52 lõike 1 punktidele 1, 4, 3 ja 8 muudetud sõnastuses, arvestades eelnevaid muudatusi, eelkõige juurdepääsuõiguse ja töötlemisõiguse andmise otsustamisel ning salastatud välisteabe avaldaja teavitamisel.

Punkti 2 järgi korraldab RJVE salastatud teabe vastastikuse kaitse kokkulepete sõlmimist ning sarnane ülesanne on RJVE-le antud § 231 lõike 2 punktis 1.

Punkti 3 järgi määrab RJVE riigisaladuse ja salastatud välisteabe taseme vastavuse. Ülesande ulatust täpsustab § 50 lõige 2.

Punktiga 4 reguleeritakse tööstusjulgeoleku olukordi, kus koostöö põhineb tsiviilõiguslikul või halduslepingul ning kus üheks pooleks on juriidiline isik, näiteks ettevõte või avalik-õiguslik ülikool. Kuivõrd tegu ei ole riigiasutuste ega rahvusvahelise õiguse subjektidega, siis on salastatud teabe kaitse kokkulepete ning rahvusvahelise praktika järgi nende poolt salastatud teabe töötlemisele kehtestatud täiendavad nõuded. Riigisaladuse avaldamise olukorras on RJVE-l § 231 lõike 2 punkti 2 järgi samasisuline ülesanne.

Punkti 5 kohaselt korraldab ja kontrollib RJVE salastatud välisteavet sisaldava salastatud teabekandja vedamist kaubana ehk juhtusid, kui teabekandjat ei ole selle suuruse, kuju, paigutuse, kaalu, sisu olemuse või suure koguse tõttu võimalik tavapäraselt vedada. RJVE poolt salastatud välisteavet sisaldavate salastatud teabekandjate rahvusvaheliselt kaubana vedamise korraldamine ei tähenda seda, et RJVE organiseerib ise veo. Veo korraldamine, sealhulgas vedajaga lepingu sõlmimine, on töötleva üksuse ülesanne. Korraldamine hõlmab selles kontekstis näiteks töötleva üksuse juhendamist ja vajadusel asjakohaste välismaiste ametkondadega suhtlemist. Riigisaladuse avaldamise olukorras on RJVE-l § 231 lõike 2 punkti 3 järgi samasisuline ülesanne.

Kehtiva RSVS § 52 lõike 1 punkti 5, mille kohaselt RJVE teavitab töötlevaid üksuseid salastatud välisteabe salastamisaluse, -taseme ja -tähtaja muutusest, ei ole üle toodud. Selle eraldi väljatoomine ei ole vajalik, sest see on hõlmatud muude ülesannetega.

Lõikes 12 on viis punkti.

Punktiga 1 antakse RJVE-le õigus anda töötlevale üksusele teavet ja täitmiseks kohustuslikke juhiseid riigisaladuse kaitse nõuete täitmiseks. Kohustuslike juhiste andmise õigus on vajalik selleks, et oleks võimalik suunata töötlevaid üksusi parimal võimalikul viisil salastatud välisteavet kaitsma. Teavet antakse selleks, et töötlevatel üksustel oleks võimalik salastatud välisteavet paremini kaitsta.

Punkti 2 kohaselt osaleb RJVE salastatud välisteabega seotud rikkumiste väljaselgitamisel ja kahju hindamisel. Rikkumisi uurib KAPO, sest RSVS § 19 lõike 1 punkti 4 kohaselt tuleb RSVS-i ja selle alusel antud õigusakti nõuete rikkumisest teavitada KAPO-t. Kuna RJVE on aga salastatud välisteabe osas eksperditeadmisi omav VLA struktuuriüksus, tuleb RJVE rikkumiste uurimisse ja kahju hindamisse kaasata.

Punktid 3 ja 4 on sama sisuga nagu kehtiva § 52 lõike 1 punktid 6–7.

Punktiga 5 lisatakse tegevusena koostöö tegemine salastatud välisteabe kaitse korraldamiseks ja kontrollimiseks riigiasutuste ning välisriikide, rahvusvaheliste organisatsioonide ja rahvusvahelise kokkuleppega loodud institutsioonidega, sest salastatud välisteabe kaitseks on vaja vahetada teavet välisriikide salastatud teabe kaitsega tegelevate asutuste ning rahvusvaheliste organisatsioonide ja rahvusvahelise kokkuleppega loodud institutsioonidega.

**Eelnõu § 1 punktiga 32** tunnistatakse RSVS § 52 lõige 5 kehtetuks. Lõikega 5 samalaadne norm on käesoleva eelnõuga § 50 lisatav lõige 51. Olemuselt sobitub norm §-s 50 sätestatud salastatud välisteabe üldsätete alla.

**Eelnõu §-dega 2 ja 4–8** muudetakse EPS-i, KS-i, RKLS-i, RKS-i VVS-i ja ÕKS-i. Kuna muudatused on sarnased, on nende kohta esitatud ühine selgitus.

Esiteks sätestatakse kohustus tutvustada enne salastatud välisteabele juurdepääsu õiguse andmist salastatud välisteabe kaitse nõudeid ja võtta selle kohta kinnitus, kui välisleping seda nõuab. Salastatud välisteabe kaitse nõuete tutvustuse läbimise nõue on ära toodud lisaks Euroopa Liidu ja NATO regulatsioonidele ka mitmes Eesti Vabariigi poolt välisriigiga sõlmitud salastatud teabe vastastikuse kaitse kokkuleppes (nt Iisrael, Ühendkuningriik). Rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooni salastatud välisteabe puhul tutvustab RJVE vastava organisatsiooni salastatud välisteabe kaitse nõudeid ja võtab kinnituse RSVKK lisas 13 sätestatud vormil. Välisriigi salastatud välisteabe puhul tutvustab töötlev üksus RSVS §-s 19 sätestatud kohustusi ja võtab RSVS § 27 lõike 10 punktis 2 nimetatud kinnituse RSVKK lisas 6 sätestatud vormil.

Teiseks luuakse õiguslik alus salastatud välisteabe juurdepääsu andmisest keeldumiseks isikutele, kes ei nõustu endale salastatud välisteabe kaitse nõuete tutvustamise või kinnituse allkirjastamisega. Eelnõu §-des 2 ja 4–8 toodud seadustes nimetatud isikutel on ametikohajärgne juurdepääsu õigus salastatud välisteabele. Juurdepääsuõigus tekib ametikohale asumisega ja seda eraldi ei vormistata. Kui aga välislepingu kohaselt on salastatud välisteabe kaitse nõuete tutvustamine kohustuslik, kuid isik keeldub nõuete tutvustamisest või kinnituse allkirjastamisest, ei ole võimalik talle konkreetsele salastatud välisteabele juurdepääsu anda vaatamata ametikohajärgse juurdepääsuõiguse olemasolule.

**Eelnõu §-ga 3** muudetakse JAS-i, mille § 7 lõike 1 punktis 4 asendatakse sõnad „elektrooniline teabeturve“ sõnadega „salastatud teabe küberturvalisus“. Muudatus on tingitud samasisulistest muudatustest RSVS-is.

**Eelnõu § 9** kohaselt jõustub eelnõukohane seadus 2026. aasta 1. juulil.

**4. Eelnõu terminoloogia**

Eelnõus võetakse kasutusele uus termin „pädev asutus ja ühtne kontaktpunkt“, mis on asutus või üksus, mis täidab rahvusvahelisest õigusest tulenevaid kohustusi riigi esindamisel vastava rolli täitmisel.

**5. Eelnõu vastavus Euroopa Liidu õigusele**

Eelnõu ei mõjuta ega muuda RSVS-i kooskõla Euroopa Liidu õigusega. Seaduse uue § 50 lõike 1 sõnastuse järgi loetakse käesoleva seaduse tähenduses välislepinguks muuseas ka Euroopa Liidu täitmiseks kohustuslikke õigusakte. Senises rakenduspraktikas on segadust tekitanud, kas sellistest õigusaktidest tulenevad nõuded on täitmiseks kohustuslikud.

**6. Seaduse mõjud**

Muudatustel on **vahetu positiivne mõju riigi julgeolekule**. Muudatustega ajakohastatakse salastatud teabe kaitset reguleerivat regulatsiooni. Seaduse struktuur muudetakse ühetaoliseks kõigi salastatud teabe kaitsega seotud osapoolte suhtes.

Samuti antakse Vabariigi Valitsusele volitus määrata rollide täitjad, mis on vajalikud rahvusvahelises koostöös salastatud teabe kaitse valdkonnas. Sellel on **positiivne mõju Eesti riigi välissuhetele**.

Muudatusel on **mõju riigiasutuste korraldusele ja halduskoormusele** tänu seaduse selgemale sõnastusele ning pädevuste-ülesannete-tegevuste selgusele. Sellega ei kaasne olulisi riske ega negatiivseid kõrvalmõjusid.

**7. Seaduse rakendamisega seotud tegevused, vajalikud kulud ja määruse rakendamise eeldatavad tulud**

Seaduse rakendamisega ei kaasne otseseid kulusid rakendavatele ametkondadele. Ametkonnad täidavad neid ülesandeid enamjaolt juba praegu, kuid nüüd muutub selgemaks nende ülesannete struktuur ja jaotus.

Seaduse rakendamisega kaasnevat tulu ei ole võimalik prognoosida, kuna seadusest tuleneva sunniraha määramine ei ole kohustus, vaid võimalus, samuti sõltub sunniraha suurus iga kord selle määramisega seotud asjaoludest.

**8. Rakendusaktid**

Eelnõu rakendamiseks on vaja muuta Vabariigi Valitsuse 20. detsembri 2007. aasta määrust nr 262 „Riigisaladuse ja salastatud välisteabe kaitse kord“.

Rakendusakti kavand on lisatud seletuskirjale.

**9. Seaduse jõustumine**

Seadus jõustub 2026. aasta 1. juulil. Eesmärk on võimalikult kiiresti kõrvaldada eelnõus mainitud kitsaskohad.

**10. Eelnõu kooskõlastamine**

Eelnõu esitatakse eelnõude infosüsteemi kaudu kooskõlastamiseks Riigikantseleile ja ministeeriumidele ning arvamuse avaldamiseks Välisluureametile, Kaitseväele, Kaitseliidule, Riigikontrollile, Riigikogu Kantseleile, Riigikohtule, Õiguskantsleri Kantseleile, Eesti Pangale ja Vabariigi Presidendi Kantseleile.

Algatab Vabariigi Valitsus 2026

(allkirjastatud digitaalselt)

Lauri Hussar

Riigikogu esimees

1. AvTS § 31 lg 3. [↑](#footnote-ref-1)
2. AvTS § 31 lg 3. [↑](#footnote-ref-2)
3. AvTS § 28 lg 1 p 31. [↑](#footnote-ref-3)
4. *web scraping*. [↑](#footnote-ref-4)
5. <https://dokumendiregistrid.karlerss.com/>. [↑](#footnote-ref-5)
6. „Riigiandmete kogumine meedias kajastamise jaoks“ – Delfi Meedia ettekanne 2025. a konverentsil „A2: avalik teave ja avaandmed“, kättesaadav: <https://worksup.com/app/#/event/A2KONVERENTS/agenda/plan>. [↑](#footnote-ref-6)
7. PS § 44, AvTS § 4. [↑](#footnote-ref-7)
8. RIA [Küberturvalisuse aastaraamat 2025](https://www.ria.ee/kuberturvalisuse-aastaraamat-2025), lk 16. [↑](#footnote-ref-8)
9. <https://www.err.ee/1609751085/kohus-saatis-narvalasest-vene-kodaniku-luuramise-eest-vangi>. [↑](#footnote-ref-9)
10. AvTS ning eriseadused. [↑](#footnote-ref-10)
11. RJVE veebileht: nsa.valisluureamet.ee/õigusaktid.html. [↑](#footnote-ref-11)