

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 kaitseks, 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.

Eelnõuga täiendatakse julgeolekukontrolliga seonduvat regulatsiooni eesmärgiga välistada teatamiskohustusega välisriikide kodakondsust omavate isikute juurdepääs riigisaladusele. Lisaks tehakse veel mõningad muuatused, mis täpsustavad julgeolekukontrolliga seonduvat seoses isikutega, kes viibivad või töötavad suure osa ajast välismaal.

Eelnõu vähendab vähesel määral riigisaladust välismaale edastavate 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 Siseministeeriumi ning KAPO esindajatega.

Eelnõu õiguslikku kvaliteeti on kontrollinud Kaitseministeeriumi õigussakonna nõunik Liina Martinson (liina.martinson@kaitseministeerium.eemailto). Eelnõu ja seletuskirja on keeleliselt toimetanud Luisa Keelelahenduste eesti keele vanemtoimetaja Tiina Alekõrs (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, 03.02.2026, 13;
- 2) avaliku teabe seadus (edaspidi *AvTS*) avaldamismärkega RT I, 06.03.2026, 4;
- 3) Eesti Panga seadus (edaspidi *EPS*) avaldamismärkega RT I, 01.03.2023, 45;
- 4) julgeolekuasutuste seadus (edaspidi *JAS*) avaldamismärkega RT I, 14.03.2023, 25;
- 5) kohtute seadus (edaspidi *KS*) avaldamismärkega RT I, 08.04.2025, 7;
- 6) Riigikogu liikme staatuse seadus (edaspidi *RKLS*) avaldamismärkega RT I, 30.12.2024, 19;
- 7) Riigikontrolli seadus (edaspidi *RKS*) avaldamismärkega RT I, 08.04.2025, 11;
- 8) Vabariigi Valitsuse seadus (edaspidi *VVS*) avaldamismärkega RT I, 07.05.2025, 9;
- 9) õiguskantsleri seadus (edaspidi *ÖKS*) avaldamismärkega RT I, 08.04.2025, 19.

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

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 läbiseigi, 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.

Kodakondsusega kaasneb riigi ja isiku vaheline eriline usaldussuhe, mis toob kaasa teatavad õigused ja kohustused (sõjaväekohustus, lojaalsuskohustus jne). Kehtivas õiguses puuduvad selged õiguslikud alused keeldumaks riigisaladusele juurdepääsu andmisest isikutele, kellel on teatamiskohustusega välisriigi kodakondsus. Eelnõuga lisatakse RSVS-i vastavad alused.

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 rakendamise eesmärgi 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 kümnest paragrahvist: §-dega 1–8 muudetakse RSVS-i, AvTS-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.

Termin „küberturvalisus“ on defineeritud Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) artikli 2 punktis 1 kui tegevused, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid küberohtude eest. Salastatud teabe küberturvalisus on salastatud teabe käideldavuse, konfidentsiaalsuse ja tervikluse tagamine töötlussüsteemis (RSVS § 3 p 10). Määruse (EL) 2019/881 kohase küberturvalisuse termini ja salastatud teabe küberturvalisuse termini puhul on erinevus selles, et esimese puhul on kaitseobjektiks võrgu- ja infosüsteemid, teise puhul salastatud teave ehk riigisaladus või salastatud välisteave. See ei ole siiski selline erinevus, mille tõttu ei peaks elektroonilise teabeturbe termini asemel salastatud teabe küberturvalisuse terminit kasutusele võtma. Nii küberturvalisuse kui salastatud teabe küberturvalisuse puhul on fookuses võrgu- ja infosüsteemide kaitse (töötlussüsteem on võrgu- ja infosüsteem, mida kasutatakse salastatud teabe elektrooniliseks töötlemiseks (RSVS § 3 p 9)). Salastatud teabe küberturvalisuse puhul rõhutatakse salastatud teabe kaitse aspekti, aga olemuselt on tegu sarnase tegevusega. Selleks et võrgu- ja infosüsteemide küberturvalisusega üldiselt ja salastatud teabe töötlemiseks kasutatavate võrgu- ja infosüsteemide (töötlussüsteemide) turvalisusega kitsamalt tegelevad isikud saaks toimida sarnases inforuumis, tuleb terminikasutust ühtlustada ja elektroonilise teabeturbe asendamine salastatud teabe küberturvalisusega on üks viis selle saavutamiseks.

Eelnõu § 1 punktiga 1 asendatakse RSVS-is läbivalt sõnad „elektrooniline teabeturbe“ sõnadega „salastatud teabe küberturvalisus“. Osades kohtades ei ole siiski asendamine ilma täiendavate muudatuste tegemiseta võimalik, sest elektrooniline teabeturbe on tegevus, küberturvalisus aga seisund või olek. Punktiga 5 jäetakse seetõttu salastatud teabe küberturvalisuse definitsioonist välja sõna „tagamine“.

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 toime 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 muudetakse RSVS § 3 punktis 9 töötlussüsteemi 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 kasutamise 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) Kui juurdepääsupiirangu kehtestamise põhjus püsib, võib asutuse juht või tema volitatud isik käesoleva paragrahvi lõike 3 alusel asutusesiseseks kasutamiseks mõeldud teabeks tunnistatud teabe juurdepääsupiirangu tähtaega pikendada kuni viie aasta kaupa, kuid kokku mitte kauemaks kui on käesoleva paragrahvi lõike 1 alusel kehtestatud määrukses sätestatud samadele tunnustele vastava riigisaladuseks oleva teabe salastamise tähtaeg.“.

Muudatuse eesmärk on võimaldada pikendada RSVS § 11 lõike 3 alusel asutusesiseseks kasutamiseks mõeldud teabeks tunnistatud teabele seatud juurdepääsupiirangu tähtaega kuni viie aasta kaupa kuni juurdepääsupiirangu kehtestamise põhjus püsib, kuid kokku mitte kauemaks kui on samadele tunnustele vastava riigisaladuseks oleva teabe salastamise tähtaeg. 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 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. 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.

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 tagatud¹. RSVS-i sätete tunnustele vastava juurdepääsupiiranguga asutusesiseseks kasutamiseks mõeldud teabe puhul võib AvTS-ist tuleneva maksimaalselt kümneaastase 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 dokumendiregistris². Arvestatav uus julgeolekuoht on avaandmete masspäringud, andmete nn kraapimine³ ja allalaadimine eraisikute⁴ ning eri tsiviilasutuste⁵, sealhulgas välisriikides asuvate meediamajade poolt. Riigiasutuste avalikele dokumendiregistritele on juurdepääs igapäev, sealhulgas välisriigi kodanikul. Riigiasutuste avalikule teabele ei ole juurdepääs seaduse tasandil piiratud⁶. 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 kaitsektor ning ettevõtted, mis neid toetavad⁷. Samuti on Eesti näitel leidnud tõendamist, et ka avalikult kättesaadavat infot edastatakse vaenuliku riigi luureteenistusele⁸. Avalikult kättesaadavaid andmeid koos teiste andmetega analüüsides võib jõuda riigi julgeolekut ohustavate tulemusteni. Sarnasel moel võib olla võimalik eri ministriumide valitsemisalade andmeid koos töödeldes teha järeldusi riigi julgeoleku tagamisega seotud võimete ja vahendite kohta. Kehtivas õiguses⁹ 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.

Tromsø konventsioon ei piira riikide võimalusi juurdepääsupiirangu tähtaja pikendamise otsustamiseks. Konventsiooni artikli 3 lõike 1 punkti a kohaselt võib konventsiooniosaline piirata ametlikele dokumentidele juurdepääsu õigust riigi julgeoleku ja riigikaitse ning rahvusvaheliste suhete kaitsmise kaalutlustel. Konventsiooni kohaselt peavad piirangud olema seaduses täpselt sõnastatud, demokraatlikus ühiskonnas vajalikud ja proportsionaalsed.

Eesti Vabariigi julgeoleku kaitsmine on legitiimne eesmärk. Mõne teise (vähem koormava) vahendiga ei ole võimalik piirangu eesmärki saavutada, sest juurdepääsupiirang seatakse ja seda pikendatakse vaid juurdepääsupiirangu seadmise põhjuse olemasolul ning teabe avalikustamine ega kustutamine ei ole juurdepääsupiirangu põhjuse püsimisel sobivad alternatiivid. Eeltoodust tulenevalt on meede mõõdukas, julgeoleku kaitsmine on kaalukas põhjus.

¹ AvTS § 3¹ lg 3.

² AvTS § 28 lg 1 p 31.

³ *web scraping*.

⁴ <https://dokumendiregistrid.karlerss.com/>.

⁵ „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>.

⁶ PS § 44, AvTS § 4.

⁷ RIA [Küberturvalisuse aastaraamat 2025](#), lk 16.

⁸ <https://www.err.ee/1609751085/kohus-saatis-narvalasest-vene-kodaniku-luuramise-cest-vangi>.

⁹ AvTS ning eriseadused.

Samad kaalutlused seoses muudatuste kooskõlast Tromsø konventsiooniga on asjakohased ka juhtudel, kus teavet kaitstakse riigi välissuhtlemise kaitse ja töötleva üksuse ülesannete täitmise tagamise põhjustel.

Eelnõu § 1 punktiga 11 täiendatakse RSVS § 19 lõikega 2¹, mille kohaselt peab isik, kelle juurdepääsuvajadus tuleneb teenistus- või muust lepingulisest suhtest välisriigi töötleva üksuse, rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooniga, esitama RSVS § 19 lõikes 2 nimetatud teavituse enda suhtes julgeolekukontrolli teostamiseks pädevale asutusele.

RSVS § 19 lõike 2 kohaselt on juurdepääsuõigust omav füüsiline isik kohustatud teatama kirjalikku taasesitamist võimaldavas vormis selle töötleva üksuse, kellega teenistus- või muust lepingulisest suhtest tulenevalt on isikul juurdepääsuõigus, riigisaladuse kaitset korraldavale isikule töö- või teenistusülesande välisest kavandatavast viibimisest välisriigis, mille kohta kehtib teatamiskohustus, hiljemalt viis tööpäeva enne kavandatava välisreisi algust. Ettenägematust viibimisest välisriigis, mille kohta kehtib teatamiskohustus, teatab isik riigisaladuse kaitset korraldavale isikule viivitamata. Teates märgitakse isiku nimi, sidevahendite andmed, välisriik ning selles viibimise aeg ja põhjus. Hetkel on teatamiskohustusega riikideks siseministri 29.09.2023 käskkirja nr 1-3/112 alusel Armeenia Vabariik, Aserbaidžaaani Vabariik, Hiina Rahvavabariik (sh Hongkongi ja Macau erihalduspiirkonnad), Iraani Islamivabariik, Kasahstani Vabariik, Kirgiisi Vabariik, Korea Rahvademokraatlik Vabariik, Tadžikistani Vabariik, Türkmenistan, Usbekistani Vabariik, Valgevene Vabariik ja Venemaa Föderatsioon.

Riigisaladuse kaitset korraldava isiku kaudu peaks see teave jõudma julgeolekukontrolli teostava asutuseeni. Kui isiku tööandja on välisriigi töötlev üksus, rahvusvaheline organisatsioon või rahvusvahelise kokkuleppega loodud institutsioon, siis üldjuhul see teave ei jõua julgeolekukontrolli teostava asutuseeni, sest konkreetse välisriigi, rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooni reeglid ei pruugi näha ette salastatud teabe kaitse eest vastutava isiku määramist ja sel juhul ei ole isikul võimalik ka kedagi teavitada. Seetõttu peab juurdepääsuõigust omaval füüsilisel isikul, kelle juurdepääsuvajadus tuleneb teenistus- või muust lepingulisest suhtest välisriigi töötleva üksuse, rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooniga, olema kohustus teatada välisriigis, mille kohta kehtib teatamiskohustus, kavandatavast viibimisest otse enda suhtes julgeolekukontrolli teostamiseks pädevale asutusele.

Eelnõu § 1 punktiga 12 täiendatakse RSVS § 19 lõikega 7¹, mille kohaselt isik, kelle juurdepääsuvajadus tuleneb teenistus- või muust lepingulisest suhtest välisriigi töötleva üksuse, rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooniga, on kohustatud teatama enda suhtes julgeolekukontrolli teostamiseks pädevale asutusele, kui tema suhtes esineb RSVS § 32 lõike 1 punktis 8 või § 32 lõike 2 punktides 3–8 nimetatud asjaolu. Praktikas peab isik teavitama julgeolekukontrolli teostamiseks pädevat asutust, kui ta on kriminaalmenetluses kahtlustatav või süüdistatav, kui tema suhtes viiakse läbi väärteomenetlust ametialase süüteo või korruptiivse teo tunnustel, kui tal on mitu väärteokaristust, kui teda on karistatud tahtlikult toimepandud ametialase süüteo või kuriteo eest, mille isik on toime pannud ametiisikuna, või kui teda on kriminaalkorras karistatud. Sellest, kui isiku suhtes alustatud ametialase kuriteo või riigivastase kuriteo menetlus on lõpetatud kriminaalmenetluse seadustiku § 202, 203, 205 või 205² alusel või kui isiku suhtes

viiakse läbi süüteomenetlust RSVS-i või selle alusel antud õigusakti nõuete rikkumise tunnustel, on julgeolekukontrolli teostamiseks pädev asutus eelduslikult teadlik.

RSVS § 32 lg 4 sätestab, et kui isiku puhul ilmneb § 32 lõikes 1 või 2 nimetatud asjaolu, on isikuga teenistus- või lepingulises suhtes olev töötlev üksus kohustatud sellest viivitamata teatama isiku suhtes julgeolekukontrolli teostamiseks pädevale asutusele. Praktikas saab tööandja teavitada eelkõige isikuga seotud süüteomenetlusest, sest selline teave saab kõige tõenäolisemalt tööandjale teatavaks. Muudatust on vaja, sest kui isik on teenistus- või lepingulises suhtes välismaise tööandjaga, ei edasta tööandja seda teavet julgeolekukontrolli teostamiseks pädevale asutusele ja kehtivas regulatsioonis puudub ka isikul endal teavitamiskohustus.

Isik peab küll ka riigisaladuse juurdepääsuloa taotlemisel või pikendamisel märkima ankeeti endaga seotud süüteomenetlused, kuid see ei ole piisav, sest ankeet tuleb täita üks kord viie aasta jooksul salajase või täiesti salajase taseme riigisaladusele juurdepääsu loa taotlemisel ja kord seitsme aasta jooksul konfidentsiaalse taseme riigisaladusele juurdepääsu loa taotlemisel.

Eelnõu § 1 punktiga 13 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 14 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 ja lisatud on kaitseväeluuret teostavat Kaitseväge struktuuriüksust puudutav punkt. Kolme lõike asemel on uues sõnastuses üks lõige,

millel on neli § 20¹ lõikes 1 sätestatust erinevalt riigisaladuse avaldamise juhtumit kirjeldavat punkti. Sõnastuse muutmise eesmärk on tagada parem arusaadavus. Normide mõte jääb samaks. Punktis 1 ja 2 on sõnastuslikult 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 1 järgi loetakse Euroopa Liidu täitmiseks kohustuslikust õigusaktist tulenevaid nõudeid RSVS-i tähenduses välislepingust tulenevateks nõueteks.

Punkt 4 loob erandi kaitseväeluuret teostava Kaitseväe struktuuriüksuse osas. RSVS-is on kasutatud nii sõnastust „kaitseväeluuret teostav Kaitseväe struktuuriüksus“ kui ka „kaitseväeluurega tegelev Kaitseväe struktuuriüksus“. Neid termineid on oluline eristada. Kaitseväe põhimääruses on kaitseväeluure teostamine üksnes luurekeskuse pädevuses (§ 13 p 2). Lisaks on seoses relvastatud vastupanu ettevalmistamisega antud volitus kaitseväeluuret teostada ka eriooperatsioonide väejuhatusele, sest relvastatud vastupanu ettevalmistamine on eriooperatsioonide väejuhatuse ülesanne (Kaitseväe põhimäärus § 16 lg 2 p 1¹) ja Kaitseväe korralduse seaduse §-s 37 on teabe kogumisega seotud volitusi õigus rakendada ka relvastatud vastupanu ettevalmistamiseks. Seega kaitseväeluuret teostava Kaitseväe struktuuriüksuse all on mõeldud luurekeskust ja eriooperatsioonide väejuhatust. Kaitseväeluurega tegelev Kaitseväe struktuuriüksus hõlmab ka teisi Kaitseväe struktuuriüksusi (nt merevägi või õhuvägi), mis võivad oma ülesannete raames mingil määral kaitseväeluurega tegeleda. Selline eristus on ilmne näiteks RSVKK § 5 lõike 7 ning lõigete 8 ja 10 sissejuhatavates lauseosades. RSVKK § 5 lõiget 7 võivad salastamisalusena kasutada kõik Kaitseväe struktuuriüksused, kellel on ühel või teisel moel kaitseväeluure ülesanded, kuid RSVKK § 5 lõiked 8 ja 10 on üksnes luurekeskuse ja eriooperatsioonide väejuhatuse ehk kaitseväeluuret teostava või selleks volitust omava Kaitseväe struktuuriüksuse loodava teabe salastamisalused.

Kaitseväeluuret teostava Kaitseväe struktuuriüksuse lisamine on tingitud sellest, et sel struktuuriüksusel on oma ülesannete täitmise eesmärgil ja julgeolekuolukorrast tulenevalt põhjendatud vajadus salastatud teabe vahetamiseks välisriikide, rahvusvaheliste organisatsioonide ja rahvusvahelise kokkuleppega loodud institutsioonidega, kellega Eesti Vabariik ei ole seni välislepingut sõlminud. Muutunud julgeolekuolukord maailmas nõuab luure efektiivseks toimimiseks, luurele püstitatud ülesannete täitmiseks ja julgeolekuohtude ennetamiseks ja tõkestamiseks aktiivset rahvusvahelist koostööd ja kiiret reageerimist ning seda selgelt kasvava trendina. Loa taotlemisega kaasneb paratamatult liigne ajakulu ja samuti tekib vastuolu teadmismajaduse põhimõttega. Seega on otstarbekas ja mõistlik, et lisaks RSVS-is juba nimetatud riigiasutustele saab ka kaitseväeluuret teostav Kaitseväe struktuuriüksus edastada riigisaladust iseseisvalt tingimusel, et see on vajalik luure ja vastuluure ülesannete täitmiseks.

Kaitseväeluuret teostava Kaitseväe struktuuriüksuse osas erandi tegemist toetab ka eelnõuga lisatav § 23¹ lõige 4 punkt 2 (kehtiv RSVS § 35 lg 6 p 2), mille alusel RJVE ei korralda ega kontrolli riigisaladuse kaitset, kui Kaitsevägi avaldab välisriigile RSVS § 7 punktides 5¹, 7, 10 ja 11 nimetatud teavet. Sätted viitavad otseselt, et tegemist on kaitseväeluurega tegeleva Kaitseväe struktuuriüksuse kogutud ja sünteesitud teabega, sh rahvusvahelist koostööd käsitleva teabega. Lisaks ei korralda ega kontrolli RJVE ka kaitseväeluurega tegeleva Kaitseväe struktuuriüksuse luuret ja vastuluuret puudutavat salastatud välisteabe vahetust

RSVS § 52 lõike 3 punkti 2 kohaselt. Sarnased erandid on kavandatava § 23¹ lõike 4 punktides 1 ja 3–4 (kehtiv RSVS § 35 lg 6 punktid 1, 3 ja 4) ning RSVS § 52 lõike 3 punktides 1 ja 3–4 tehtud riigiasutuste osas, mida on nimetatud kavandatava § 20¹ lõike 2 punktides 1–3.

Eelnõu § 1 punktiga 15 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 16 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 17 täiendatakse RSVS § 22 uue lõikega 2¹, milles esitatakse tegevused, mida KAPO ja Kaitseväge põhimääruses määratud struktuuriüksus sama paragrahvi lõikes 2 toodud pädevuste täitmisel teevad.

Lõikesse on üle toodud eelneva punktiga kehtetuks tunnistatud lõike 2 punktid 3 ja 5 ning lisatud on kaks uut punkti. Vabariigi Valitsuse julgeolekukomisjonile ettepanekute tegemist sätestavat punkti ei ole üle toodud, kuna Riigikantselei juhtis oma tagasisides tähelepanu, et RSVS § 22 lõike 2 punktis 4, § 23 lõike 3 punktis 4 ja § 52 lõike 1 punktis 7 sätestatakse KAPO, Kaitseväge põhimääruses määratud struktuuriüksuse, VLA ja RJVE kohustus teha Vabariigi Valitsuse julgeolekukomisjonile ettepanekuid puuduste kõrvaldamiseks ja õigusrikkumiste vältimiseks. Selline regulatsioon ei ole aga täpne, sest Vabariigi Valitsuse julgeolekukomisjon kui valitsuskomisjon ei menetle selliseid ettepanekuid. Ettepanekute menetlemine toimub vastavas ministeeriumis või Riigikantseleis.

Punktiga 1 antakse KAPO-le ja Kaitseväge põhimääruses määratud struktuuriüksusele õigus anda töötlevale üksusele teavet ja õigusaktides sätestatud nõuete täitmiseks juhiseid riigisaladuse kaitse nõuete täitmiseks. 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 Välisluureamet ja riigi julgeoleku volitatud esindaja. Tegemist on §-des 23, 23¹ ja 52 nimetatud valdkondades eksporditeadmisi omavate ametkondadega, kelle teadmisi on vaja vastava valdkonnaga seotud rikkumise väljaselgitamiseks ja kahju hindamiseks.

Punktiga 4 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 punktidega 18 ja 19 muudetakse KAPO poolt teostatava riigisaladuse kaitse kontrolli läbiviimiseks moodustatava komisjoniga seotud regulatsiooni.

Kehtiva RSVS § 22 lõike 6 kohaselt kehtestab KAPO poolt teostatava riigisaladuse kaitse kontrolli läbiviimiseks moodustatava komisjoni töökorra valdkonna eest vastutav minister määrusega. KAPO töökorraldust ei ole otstarbekas reguleerida ministri tasemel. Seetõttu tunnistatakse RSVS § 22 lõige 6 kehtetuks.

Küll aga on asjakohane RSVS-is sätestada komisjoni üldine roll ja pädevus ning komisjoni täpsema töökorralduse peaks sätestama KAPO sisemiste õigusaktidega. Sel eesmärgil täiendatakse RSVS § 22 lõigetega 7–10.

Lõikega 7 nähakse ette volitusnorm komisjoni moodustamiseks.

Lõikega 8 sätestatakse ülesanded, mida riigisaladuse kaitse kontrolli komisjon täidab.

Lõikes 9 sätestatakse, et kontrolli läbiviimise kohta koostab komisjon aruande, milles antakse hinnang riigisaladuse kaitse korralduse vastavusele nõuetele.

Lõikes 10 nähakse ette, et aruandes tehtud ettekirjutuste täitmisest tuleb Kaitsepolitseiametile teatada viivitamatult, kuid mitte hiljem kui ühe kuu jooksul arvates ettekirjutuse täitmiseks antud tähtaja möödumisest. Aruanne esitatakse alati enne kinnitamist töötlevale üksusele kommenteerimiseks. RSVS § 22 lõike 3 kohaselt on KAPO-l õigus teha töötlevale üksusele ettekirjutusi. Riigisaladuse kaitse tagamiseks on oluline, et töötlev üksus teavitaks KAPO-t aruandes esitatud ettekirjutuste täitmisest.

Eelnõu § 1 punktiga 20 asendatakse RSVS § 23 lõike 1 punktis 1 sõnad „elektroonilist teabeturvet“ sõnadega „salastatud teabe küberturvalisuse tagamist“. RSVS-is asendatakse läbivalt sõnad „elektrooniline teabeturve“ sõnadega „salastatud teabe küberturvalisus“. Osades kohtades ei ole siiski asendamine ilma täiendavate muudatuste tegemiseta võimalik, sest elektrooniline teabeturve on tegevus, küberturvalisus aga seisund või olek. Salastatud teabe küberturvalisuse definitsioonist tuleb seetõttu välja jätta sõna „tagamine“.

Eelnõu § 1 punktiga 21 muudetakse RSVS § 23 lõiget 2. Lõikes 2 sätestatakse VLA ülesanded salastatud teabe küberturvalisuse tagamise korraldamisel ja kontrollimisel. Selle tagajärjel tekib selge struktuur, kus kõigepealt on lõikes 1 määratud, et VLA-l on pädevus salastatud teabe küberturvalisuse tagamist korraldada, ning seejärel on loetletud konkreetsed ülesanded.

VLA ülesanded salastatud teabe küberturvalisuse tagamise 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. Krüptomaterjalide kaitse

või kiirgusturbe tagamise korraldamine ei tähenda, et Välisluureamet seda töötleva üksuse eest teostaks. Välisluureametil on riigülene suunav ja koordineeriv roll.

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 22 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 23 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.

Vabariigi Valitsuse julgeolekukomisjonile ettepanekute tegemist sätestavat punkti ei ole üle toodud, kuna Riigikantselei juhtis oma tagasisides tähelepanu, et RSVS § 22 lõike 2 punktis 4, § 23 lõike 3 punktis 4 ja § 52 lõike 1 punktis 7 sätestatakse KAPO, Kaitseväge põhimääruses määratud struktuuriüksuse, VLA ja RJVE kohustus teha Vabariigi Valitsuse julgeolekukomisjonile ettepanekuid puuduste kõrvaldamiseks ja õigusrikkumiste vältimiseks. Selline regulatsioon ei ole aga täpne, sest Vabariigi Valitsuse julgeolekukomisjon kui valitsuskomisjon ei menetle selliseid ettepanekuid. Ettepanekute menetlemine toimub vastavas ministeeriumis või Riigikantseleis.

Punktiga 1 antakse VLA-le õigus anda töötlevale üksusele teavet ja õigusaktides sätestatud nõuete täitmiseks juhiseid riigisaladuse kaitse nõuete täitmiseks. 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) soovitude andmist täiendavate turvameetmete rakendamiseks välja toodud, sest see on hõlmatud punktiga 1.

Eelnõu § 1 punktiga 24 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 Kaitseväge 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 Kaitseväge põhimääruses määratud struktuuriüksuse pädevust riigisaladuse kaitseks, 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 tavapärastel vedada. Tegemine 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-s 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 2 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 teadmismajadus 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 25 lisatakse RSVS § 27 lõikesse 5 punkt 3¹, mille tulemusel saab RJVE õiguse anda isikule piiratud taseme riigisaladusele juurdepääsu õigus, kui isiku juurdepääsuvajadus riigisaladusele tuleneb välisriigi, rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooni antud ülesannetest.

Muudatuse eesmärk on vähendada bürokraatiat ja võimaldada isikul saada vajalikud piiratud taseme juurdepääsuõigused ühest kohast. Muudatuse tulemusel on RJVE-l õigus anda isikule piiratud taseme riigisaladusele juurdepääsu õigus järgmistes olukordades.

Esiteks, kehtiva regulatsiooni ja ka kavandatava RSVS § 51 lõike 4 kohaselt on piiratud taseme riigisaladusele juurdepääsu õigus Euroopa Liidu või NATO piiratud taseme salastatud välisteabele juurdepääsu õiguse saamise eeldus. Osadel juhtudel ongi isikul piiratud taseme riigisaladusele juurdepääsu õigust vaja üksnes seetõttu, et muidu ei ole tal võimalik saada Euroopa Liidu või NATO piiratud taseme salastatud välisteabele juurdepääsu õigust. Kehtiva regulatsiooni järgi peab sellisel juhul piiratud taseme riigisaladusele juurdepääsu õiguse andma KAPO ja piiratud taseme Euroopa Liidu või NATO salastatud välisteabele juurdepääsu õiguse RJVE. Muudatuse tulemusel annab isikule mõlemad juurdepääsuõigused RJVE.

Teiseks võib isik vajada piiratud taseme riigisaladusele juurdepääsu õigust selleks, et saada juurdepääs välisriigi piiratud taseme salastatud välisteabele. Välisriigi salastatud välisteabele ei anta eraldi juurdepääsuõigust, vaid juurdepääsuõigus saadakse Eesti juurdepääsuõiguse alusel. Näiteks, kui Eesti kodanik töötab ettevõttes, mis on sõlminud Soome riigiga lepingu, mille täitmine eeldab Soome piiratud taseme salastatud välisteabe töötlemist. Sellises olukorras ei ole otstarbekas, et isikule annab piiratud taseme riigisaladusele juurdepääsu õiguse KAPO, sest selle, kas isikul on Soome piiratud taseme salastatud välisteabele juurdepääsu õigust vaja ja kas vastav leping on sõlmitud, peab välja selgitama RJVE, suheldes Soome RJVE-ga analoogse asutusega. Bürokratiat vähendamise eesmärgil on otstarbekas, et sellisel juhul annab RJVE ka piiratud taseme riigisaladusele juurdepääsu õiguse.

Eelnõu § 1 punktiga 26 asendatakse RSVS § 27 lõike 5 punktis 4 tekstiosa „3“ tekstiosaga „3¹“. Muudatus on seotud eelmise punktiga tehtava muudatusega.

Eelnõu § 1 punktiga 27 täiendatakse RSVS § 31 lõike 1¹, mille tulemusel saab füüsiline isik esitada teatud juhtudel taotluse riigisaladuse juurdepääsuloa saamiseks RJVE kaudu.

Muudatuse eesmärk on võimaldada esitada juurdepääsuloa saamiseks taotlus ka füüsilisel isikul, kellel ei ole riigisisest juurdepääsuloa toetajat. Kehtiva regulatsiooni kohaselt peab isik esitama juurdepääsuloa taotluse juurdepääsuloa toetaja kaudu ja vastavas elektroonilises keskkonnas. Samas kehtiva regulatsiooni ja ka kavandatava RSVS § 51 lõike 4 kohaselt on riigisaladusele juurdepääsu õigus Euroopa Liidu või NATO salastatud välisteabele juurdepääsu õiguse saamise eeldus. Osadel juhtudel ongi isikul riigisaladuse juurdepääsuluba vaja üksnes seetõttu, et muidu ei ole tal võimalik saada Euroopa Liidu või NATO salastatud välisteabele juurdepääsusertifikaati. Teiseks võib füüsiline isik vajada riigisaladuse juurdepääsuluba vaid selleks, et saada juurdepääs välisriigi, näiteks Soome salastatud välisteabele. Sellistel juhtudel ei pruugi isikul olla riigisisest juurdepääsuloa toetajat, kelle kaudu saaks juurdepääsuloa taotluse esitada. Teoreetiliselt võiks isik esitada juurdepääsuloa taotluse elektroonilises keskkonnas, aga sellele keskkonnale peab kõigepealt mõni riigiasutus isikule juurdepääsu andma.

Muudatuse toimetel esitab isik taotluse RJVE-le, mis teeb rahvusvahelise koostöö kaudu kindlaks isiku juurdepääsuvajaduse ja selle olemasolul annab isikule juurdepääsu elektroonilisele keskkonnale, mille kaudu saab isik esitada julgeolekukontrolli teostamiseks pädevale asutusele vajalikud dokumendid.

Eelnõu § 1 punktiga 28 täiendatakse RSVS § 32 lõiget 1 punktiga 11, mille kohaselt juurdepääsuluba ei anta füüsilisele isikule, kellel on sellise välisriigi kodakondsus, mille kohta kehtib teatamiskohustus, või kellel on mitu kodakondsust, millest vähemalt üks on välisriigi kodakondsus, mille kohta kehtib teatamiskohustus.

Riigisaladus on RSVS § 3 punkti 1 kohaselt Eesti Vabariigi julgeoleku või välissuhtlemise tagamise huvides avalikuks tuleku eest kaitset vajav teave. Riigi julgeoleku ja välissuhtlemise tagamiseks on oluline välistada riigisaladusele juurdepääsu loa andmine isikutele, kelle puhul võib eeldada, et nad kujutavad riigisaladuse kaitstusele suuremat ohtu.

Kodakondsusega kaasneb riigi ja isiku vaheline eriline usaldussuhe, mis toob kaasa teatavad õigused ja kohustused (sõjaväekohustus, lojaalsuskohustus jne). Riigisaladusele juurdepääsu loa saamise oluliseks põhimõtteks on tugev usaldussuhe riigi ja riigisaladusele juurdepääsu loa taotleja vahel. Isikute puhul, kellel on sellise välisriigi kodakondsus, mille kohta kehtib teatamiskohustus, esineb suur tõenäosus, et kodakondsusest tulenevast lojaalsuskohustusest tulenevalt võivad nad kujutada ohtu riigisaladuse kaitstusele. Kui isikul on mitu kodakondsust, siis on tal lojaalsuskohustus lisaks Eesti Vabariigile ka välisriigi ees. Riigisaladuse kaitse kontekstis peetakse välisriigis, mille kohta kehtib teatamiskohustus, viibimist või muul moel seotust sellise riigiga oluliseks riskiks. Julgeolekukontrollis pööratakse nendele asjaoludele erilist tähelepanu. Isikute puhul, kellel on sellise välisriigi kodakondsus, mille kohta kehtib teatamiskohustus, või lisaks Eesti Vabariigi kodakondsusele sellise välisriigi kodakondsus, mille kohta kehtib teatamiskohustus, esineb suur tõenäosus, et välisriigi kodakondsusest tulenevast lojaalsuskohustusest tulenevalt võivad nad kujutada ohtu riigisaladuse kaitstusele. Seetõttu ei ole põhjendatud anda riigisaladusele juurdepääsu luba isikutele, kellel on välisriigi, mille kohta kehtib teatamiskohustus, kodakondsus, või kellel on lisaks Eesti Vabariigi kodakondsusele sellise välisriigi, mille kohta kehtib teatamiskohustus, kodakondsus.

Eelnõu § 1 punktiga 29 asendatakse RSVS § 32 lõike 2 punktis 20 tekstiosa „1 või 2“ tekstiosaga „1, 2, 2¹ või 7¹“.

Muudatust on vaja, kuna eelnõuga lisatakse § 19 kaks lõiget, mis näevad ette teavitamiskohustuse.

Eelnõu § 1 punktiga 30 täiendatakse RSVS § 32 lõiget 2 punktiga 21, mille kohaselt võib riigisaladuse juurdepääsuloa andmisest keelduda isikule, kes regulaarselt suhtleb julgeolekukontrolli teostavale asutusele esitatud juurdepääsuloa taotleja ankeedis või pikendaja ankeedis märgitud sugulase, hõimlase või muu lähedase isikuga, kes elab välisriigis, mille kohta kehtib teatamiskohustus.

Eesti Vabariigi julgeolekut ohustavate välisriigi luureteenistuste eesmärk on värvata isikuid luureteenistuse huvides erinevate ülesannete täitmiseks. Riigisaladuse kaitse kontekstis peetakse suurema riskiga välisriikideks neid riike, mille kohta kehtib teatamiskohustus. Kuigi Eesti Vabariigi julgeolekut ohustavad välisriigi luureteenistused ei tunne huvi pelgalt riigisaladuse vastu, vaid igasuguse info vastu, on juurdepääsu saamine riigisaladusele üks olulisemaid eesmärke. Värbamise sihtmärgiks on tihti just inimesed, kes külastavad sellise luureteenistuse päritoluriiki või kellel on luureteenistuse päritoluriigiga alaline seos (nt seal elavate sugulaste kaudu). Kui isiku sugulane (nt ema, isa, õde, vend, laps) või lähedalt seotud isik (nt elukaaslane) elab sellises välisriigis, siis annab see selle välisriigi luureteenistustele võimaluse isikut vajaduse korral survestada. See kujutab riigisaladuse kaitstusele ohtu, sest seeläbi võib olla võimalik mõjutada isikut asuma välisriigi luureteenistusega koostööle.

Seetõttu tuleb isiku sugulase, hõimlase või lähedase isikuga seotud asjaolusid arvesse võtta julgeolekuriskide hindamisel. Välisriigis, mille kohta kehtib teatamiskohustus, elav sugulane, hõimlane või lähedane isik ei välista riigisaladuse juurdepääsuloa saamist. Oluline on hinnata isikute vahelise suhte tugevust ja konkreetset välisriiki, milles sugulane, hõimlane või lähedane isik elab. Regulaarne on kindla aja tagant toimuv suhtlus. Ka kord aastas toimuv suhtlus võib olla sõltuvalt asjaoludest regulaarne. Regulaarne suhtlus viitab, et tegu on isikuga, kellel on taotleja elus teatav roll ja keda võib seeläbi kasutada tema mõjutamisel või survestatamisel. Konkreetsemalt tuleb isikutevahelise seose tugevust ja sellest tulenevat võimalikku ohtu riigisaladusele hinnata ja põhjendada igal juhul eraldi. Kui julgeolekukontrolli käigus kogutud asjaolude pinnalt on põhjust arvata, et riigisaladuse kaitstus võib sattuda välisriigis elava sugulase, hõimlase või lähedase isiku tõttu ohtu, peab olema võimalik isikule juurdepääsuloa andmisest keelduda.

Otstarbekas on piiritleda sugulaste, hõimlaste ja lähedaste isikute ring isikutega, kes tuleb märkida juurdepääsuloa taotleja ankeeti või juurdepääsuloa pikendaja ankeeti. Sel viisil on hõlmatud isikud, kelle kaudu võib kõige tõenäolisemalt olla võimalik juurdepääsuloa taotlejat mõjutada ja samas on lähedaste isikute ring juurdepääsuloa taotleja jaoks üheselt kindlaks määratud.

Lähedaste isikutega seonduva hindamine juurdepääsuõiguse andmisel on välja toodud ka NATO personalijulgeoleku direktiivi punktis 18, mille alapunkti 1 kohaselt on üks peamine kriteerium, mille põhjal tuvastatakse isiku lojaalsus, usaldusväärsus ja kindlus isikule juurdepääsuloa andmiseks see, kas isik võib sugulaste või lähedalt seotud isikute kaudu olla haavatav või survestatav välisriikide luureteenistuste, terrorirühmituste või muude õonestusega tegelevate organisatsioonide või isikute poolt, kelle huvid võivad ohustada NATO ja/või NATO liikmesriikide julgeolekuhuve.

Eelnõu § 1 punktiga 31 täiendatakse RSVS § 33 lõikega 5¹, mille kohaselt võib julgeolekukontrolli teostav asutus jätta taotluse läbi vaatamata, kui juurdepääsuloa taotleja ei ole Eestis püsivalt elanud vähemalt viimased viis aastat.

Riigisaladus on RSVS § 3 punkti 1 kohaselt Eesti Vabariigi julgeoleku või välissuhtlemise tagamise huvides avalikuks tuleku eest kaitset vajav teave. Riigisaladuse kaitse tagamiseks on ette nähtud julgeolekukontrolli teostamine, mis seisneb üksnes RSVS §-s 32 nimetatud asjaolude esinemise kontrollimises. RSVS §-s 32 nimetatud asjaolude kontrollimise eesmärk on veenduda, et isiku puhul ei esine asjaolusid, millest tulenevalt võib ta tõenäoliselt ohustada riigisaladuse kaitstust. RSVS §-s 32 nimetatud asjaolude esinemist on võimalik kontrollida ennekõike isiku puhul, kes elab püsivalt Eestis, s.o tema peamine elukoht on Eestis. Valdavalt kontrollitakse viimase viie aasta andmeid, seega peaks isik olema Eestis elanud vähemalt mingi ajaperioodi viimase viie aasta jooksul. Kui juurdepääsuloa taotleja ei ela Eestis, võib RSVS §-s 32 nimetatud asjaolusid olla keeruline või osadel juhtudel võimatu kontrollida. Julgeolekukontroll on riigisisene haldusmenetlus. Julgeolekukontrolli raames võib küll teha päringuid välisriikidesse, aga välisriikide isikutel ei ole kohustust päringutele vastata. Kui juurdepääsuloa taotleja puhul ei ole võimalik veenduda, kas esineb RSVS §-s 32 nimetatud asjaolusid, siis ei saa talle riigisaladusele juurdepääsu luba anda. Eestis viimase viie aasta jooksul püsivalt mitte elanud juurdepääsuloa taotleja juurdepääsuloa saamise taotluse läbivaatamata jätmine ei ole siiski alati põhjendatud. Kui välisriigist on võimalik saada piisaval hulgal RSVS §-s 32 nimetatud asjaolude kontrollimiseks vajalikku teavet, ei ole taotluse läbi vaatamata jätmine põhjendatud. Samuti tuleb arvestada, et haldusmenetluses on isikul kaasaaitamiskohustus ja isik saab osa julgeolekukontrolli läbiviimiseks mõeldud teabest ka ise

Julgeolekukontrolli läbiviivale asutusele esitada. Eelkõige saab sellel alusel jätta läbi vaatamata sellise juurdepääsuloa taotleja taotluse juurdepääsuloa saamiseks, kes on pikaajaliselt viibinud välisriikides ja kelle side Eestiga on nõrk või puudub. Näiteks isikud, kelle kohta ei ole Eesti andmekogudes muid andmeid peale isikut tõendavate dokumentide väljastamise andmete. Sel juhul puudub julgeolekukontrolli teostaval asutusel võimalus ankeedis ja vestlusel esitatud andmete usaldusväärsuse kontrolliks. Eestist lähetatud inimeste puhul, isegi kui lähetus on kestnud järjest üle viie aasta, ei ole juurdepääsuloa taotluse läbi vaatamata jätmise üldjuhul õigustatud, sest neil oli ja säilib ka lähetuse ajal tugev side Eestiga ja nende poolt esitatud andmeid on võimalik kontrollida.

Lõiget ei kohaldata riigiasutuse poolt pikaajalisse välislähetusse saadetud ametniku või töötaja suhtes.

Eelnõu § 1 punktiga 32 täiendatakse RSVS § 34² lõikega 4¹, mille kohaselt kaitsevæeluuret teostava Kaitsevæe struktuuriüksuse töötlussüsteemi, mida kasutatakse riigisaladuse edastamiseks välisriigi luure- või vastuluureülesannet täitvale asutusele, võib kasutada Kaitsevæe juhataja otsuse alusel, kus määratakse töötlussüsteemis töötlemiseks lubatud riigisaladuse tase, töötlussüsteemi kasutamise tähtaeg ning käesolevas seaduses ja selle alusel antud õigusaktides sätestatud salastatud teabe küberturvalisuse nõuete täitmise ja kontrollimise eest vastutavad struktuuriüksused.

Muudatuse tulemusel saab kaitsevæeluuret teostav Kaitsevæe struktuuriüksus analoogse erandi akrediteerimise nõudest, nagu on RSVS § 34² lõikes 4 ette nähtud julgeolekuasutuste puhul. Kaitsevæe luuret teostava ja Kaitsevæe luurega tegeleva Kaitsevæe struktuuriüksuse erinevust on selgitatud § 20¹ puudutavate selgituste juures. Rahvusvahelise koostöö raames on kaitsevæeluure valdkonnas vajadus erinevate töötlussüsteemide kasutamiseks. Kaitsevæeluuret teostav Kaitsevæe struktuuriüksus teeb igapäevaselt koostööd välisriikide partnerteenistustega. Sageli töödeldakse sel juhul riigisaladust eelkõige konkreetse koostöö kontekstis. Kaitsevæeluuret teostaval Kaitsevæe struktuuriüksusel peab olema võimalus enda ehitatud töötlussüsteeme koostöö raames partnerteenistusele kasutada anda. Sellistele töötlussüsteemidele ei peaks kehtima akrediteerimise nõue, kuivõrd tuleb arvestada teadmishajaldamise põhimõttega (*sama põhimõte, mis rakendub teabele, mille osas puudub RJVE-l korraldamise funktsioon – uus RSVS § 23¹ lõige 4*).

Arvestades asjaolu, et RJVE ei korralda ega kontrolli kaitsevæeluuret teostava Kaitsevæe struktuuriüksuse luuret ja vastuluuret puudutava riigisaladuse ja salastatud välisteabe vahetust, kui välislepingust ei tulene teisiti, on põhjendatud, et VLA ei akrediteeri selleks otstarbeks kasutatavaid töötlussüsteeme. Näiteks ei pea riigisaladuse edastamist registreerima riigi julgeoleku volitatud esindaja juures, kui välisriigile edastatakse muuhulgas kaitsevæeluurega tegeleva Kaitsevæe struktuuriüksuse kogutud ja sünteesitud teavet (*RSVS § 35 lõige 6*) ja RJVE ei kinnita rahvusvahelisi külastustaotluseid RSVS § 52 lõikes 3 sätestatud juhul (*RSVKK § 122²*). Tulenevalt eeltoodust ei peaks VLA akrediteerima töötlussüsteeme, mis on ette nähtud kaitsevæeluuret teostava Kaitsevæe struktuuriüksuse poolt teabe vahetamiseks välisriigi luure- või vastuluureülesannet täitva asutusega.

Oluline on rõhutada, et töötlussüsteemid, kus töödeldakse Euroopa Liidu või NATO salastatud välisteavet või mille puhul on rahvusvahelises formaadis kokku lepitud akrediteerimiskohustus, tuleb akrediteerida tavapärasel korras Välisluureameti poolt.

Eelnõu § 1 punktiga 33 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 34 täiendatakse RSVS § 35 lõikega 7. Säte reguleerib tööstusjulgeoleku olukordi, kus koostöö põhineb tsiviilõiguslikul või halduslepingul ning kus üheks pooleks on juriidiline isik, näiteks ettevõtte 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 35 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 36 muudetakse RSVS § 50 lõikeid 1 ja 2. Lõike 1 muudatusega kirjutatakse selgemalt lahti salastatud välisteabe kaitsmise loogika. Praegu ei ole see rakendajate jaoks üheselt arusaadav.

Esiteks, kehtivas § 50 lõikes 1 on kasutusel sõnastus „salastatud välisteabele kohaldatakse selle salastatuse tasemele vastavale riigisaladusele kohaldatavaid sätteid“. Sellise sõnastuse puhul ei ole üheselt selge, kas säte kohaldub salastatud välisteabe kaitsega seotud tegevustele, mille raames otseselt salastatud välisteavet ei töödelda. 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. Seepärast on kasutatud sõna „kaitse“, mis hõlmab salastatud välisteabe töötlemist ja muid tegevusi, mis on vajalikud

salastatud välisteabe kaitseks. Sarnaselt on töötlemine ja muud tegevused hõlmatud riigisaladuse kaitse alla RSVS 2. peatüki 3. jaos „Riigisaladuse kaitse“. Nii on selgelt hõlmatud ka turva- ja administratiivalade loomisega seotud tegevused.

Teine eesmärk on sõnastada selgemalt põhimõte, et salastatud välisteabe kaitsmisel tuleb esmalt lähtuda välislepingus sätestatud nõuetest ning alles seejärel RSVS-i 3. peatükis sätestatud salastatud välisteabe kaitse erisustest ja riigisaladuse kaitse nõuetest. Kehtiva RSVS § 50 lõike 1 lõpuosa sõnastusest „kui välislepingust ei tulene teisiti“ ei ole see rakendajatele selgelt välja loetav. Levinud on ekslik arusaam, et välislepingust tuleb lähtuda ainult juhul, kui seal on sätestatud võrreldes RSVS-iga rangemad või täiendavad nõuded. Tegelikult tuleb esmajoonel kohaldada välislepingust tulenevaid nõudeid ja see, mil määral need kohalduvad, sõltub salastatud välisteabe liigist.

Välisriikidega sõlmitud salastatud teabe vastastikuse kaitse kokkulepetes on teise poole salastatud välisteabe kaitsega seonduvat reguleeritud üldiselt vähesel määral. Tavaliselt on reguleeritud mõningal määral näiteks salastatud teabe töötlemist hõlmavate külastuste korda, salastatud teavet sisaldavate lepingutega seonduvat ja salastatud teabe vahetamist. Ülejäänud osas tuleb rakendada RSVS-i 3. peatükki ja RSVS-is ette nähtud riigisaladuse kaitse nõudeid, sest enamasti on kokkuleppes kirjas, et üks pool kaitseb teise poole salastatud teavet samamoodi kui enda salastatud teavet.

Euroopa Liit, Euroopa Kosmoseagentuur ja NATO on kehtestanud oma salastatud välisteabe kaitsmiseks eraldi regulatsioonid. Nimetatud organisatsioonide salastatud välisteabe kaitsel tuleb kohaldada enamjaolt vastava organisatsiooni poolt ette nähtud nõudeid. RSVS-i 3. peatükis ja RSVS-is sätestatud nõudeid kohaldatakse eelkõige juhul, kui vastava organisatsiooni nõuetes viidatakse riigisisestes õigusaktides sätestatud korrale või ei ole mingit küsimust reguleeritud.

RSVS-i 3. peatükis sätestatud salastatud välisteabe kaitse erisusi ja riigisaladuse kaitse nõudeid kohaldatakse salastatud välisteabe kaitseks juhul kui välislepingus ei ole salastatud välisteabe kaitse nõudeid sätestatud, välislepingus on kirjas, et kohaldatakse riigisisest korda, või kui välislepingust ei ole sõlmitud. Viimasel juhul peab RJVE või RSVS § 52 lõikes 3 nimetatud asutus olema määranud riigisaladuse ja salastatud välisteabe salastatuse tasemete vastavuse. Esmajoonel tuleb kohaldada RSVS-i 3. peatükis või selle alusel antud õigusaktides sätestatud salastatud välisteabe kaitse erisusi. Kui RSVS-i 3. peatükis või selle alusel antud õigusaktides ei ole salastatud välisteabe kaitse erisusi ette nähtud, tuleb kohaldada riigisaladuse kaitse nõudeid.

Kolmandaks 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.

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

sisepääsukontrollisüsteem 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 turvaalaid loodud Kaitseväes ning see on reguleeritud RSVKK §-dega 39–40, mis reguleerivad isikute viibimist turvaalal ja iseseisva sisepääsuõigusega 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 ajal 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 ebanõistlik. Eesti Vabariik lepib välisriigiga salastatud teabe vastastikusel kaitsmises kokku üldjuhul salastatud teabe vastastikusel 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, rahvusvahelise organisatsiooni või institutsiooni salastatud välisteavet riigisaladusega sarnaselt kaitsta. Sellise välisriigi, rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooni poolt edastatud salastatud välisteave tuleb lugeda AvTS § 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 vastastikusel 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 täpsustata osalisriikide ja kohtu salastatud teabe võrdvärsust 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. Selline võimalus on vajalik, sest 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 ressursi 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.¹⁰ 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, et RJVE määrab taseme vastavuse, kui taseme vastavuse määramiseks vajalik teave on kättesaadav. Seda on oluline rõhutada, sest taseme vastavuse määramise eeldus on see, et selleks vajalik teave on RJVE-le kättesaadav. Kui teine pool ei avalda tema poolt salastatud teabe osas rakendatavaid kaitsemeetmeid või kui salastatuse tasemete vastavust pole määranud ka nt Euroopa Liit ja/või NATO, ei ole RJVE-l võimalik tasemete vastavust määrata.

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 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 või mis on nendega sõlminud salastatud teabe vastastikuse kaitse kokkuleppe, 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. Samuti võrreldakse Euroopa Liidu või NATO salastatud teabe kaitsemeetmeid ja välisriigi salastatud välisteabe kaitsemeetmeid enne Euroopa Liidu või NATO ja vastava välisriigi vahel salastatud teabe vastastikuse kaitse kokkuleppe sõlmimist. Seega saab taseme vastavuse riigisaladuse tasemele määrata ilma kaitsemeetmete võrdlust tegemata.

¹⁰ RJVE veebileht: nsa.valisluureamet.ee/õigusaktid.html.

Eelnõu § 1 punktiga 37 täiendatakse RSVS § 50 lõigetega 2¹ ja 2².

Lõike 2¹ lisamine on vajalik selleks, et RSVS § 52 lõikes 3 nimetatud asutus saaks vajaduse korral määrata riigisaladuse ja talle edastatud salastatud välisteabe salastatuse taseme vastavuse. RSVS § 52 lõike 3 kohaselt ei korralda ega kontrolli RJVE sättes nimetatud asutuste salastatud välisteabe vahetust. Erand RJVE pädevuses on tehtud seetõttu, et RSVS § 52 lõikes 3 nimetatud asutustele edastatakse üldjuhul salastatud välisteavet, mille puhul on teadmishajutus äärmiselt piiratud, ja seetõttu ei ole otstarbekas, et RJVE teenistujad sellest teadlikuks saaks. RSVS § 52 lõikes 3 nimetatud asutustele võidakse salastatud välisteavet edastada ka sellistest välisriikidest, millega Eesti ei ole sõlminud salastatud teabe vastastikuse kaitse kokkulepet ja mille osas ei ole ka RJVE teinud riigisaladuse ja salastatud välisteabe salastatuse taseme vastavuse määramise otsust. Sellisel juhul on otstarbekas, et vastav asutus saab vajadusel ise määrata riigisaladuse ja talle edastatud salastatud välisteabe salastatuse taseme vastavuse. Nii tagatakse, et teave on vajalikul määral kaitstud ja et teabele ei saa juurdepääsu teadmishajutuseta isikud. Taseme vastavuse määramine ei ole asutuse kohustus. Kui asutus seda ei tee, siis rakendub RSVS § 50 lõige 2².

Sätte rakendamiseks peab asutus määrama iga konkreetse salastatud välisteabe avaldaja poolt kasutatavale salastatuse tasemele vastava riigisaladuse salastatuse taseme. Edaspidi saab vastava otsuse võtta selle salastatud välisteabe avaldaja edastatud salastatud välisteabe kaitsmisel aluseks.

Oluline on rõhutada, et asutuse otsusel ei ole üleriigilist mõju. Otsus kohaldub vaid sellele konkreetsele asutusele konkreetse salastatud välisteabe avaldaja poolt edastatavale salastatud välisteabele. Juhul kui sama salastatud välisteabe avaldaja edastab enda salastatud välisteavet mõnele teisele töötlevale üksusele, rakendub RSVS § 50 lõige 2².

Lõike 2² lisamine on vajalik selleks, et ilma täienduseta võib seaduse rakendajatele jääda arusaamatuks, kuidas tuleb käituda salastatud välisteabega, mille kohta § 50 lõigete 2 või 2¹ alusel otsust ei ole tehtud. Segaduse vältimiseks viidatakse lõikes 2² AvTS-le, mis sellist olukorda reguleerib. Keskne säte on AvTS § 35 lõige 3, mille kohaselt välisriigi või rahvusvahelise organisatsiooni poolt edastatud juurdepääsupiirangu märkega teave, mida ei kaitsta vastavalt riigisaladuse ja salastatud välisteabe seadusele, loetakse asutusesiseseks kasutamiseks mõeldud teabeks. Lisaks on asjakohased veel AvTS § 40 lõige 1¹, § 41 lõige 3 ja § 42 lõige 2¹.

Eelnõu § 1 punktiga 38 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 39 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. Praktikast on teisi loetletud rolle täitnud samuti RJVE ja VLA, kuid õigusakti tasandil ei ole seda sätestatud. Muudatuse toimetel saab Vabariigi Valitsus õiguse määrata rollide täitjad RSVKK-s.

Eelnõu § 1 punktiga 40 muudetakse RSVS § 50 lõiget 7. Kehtivas sõnastuses on loetletud hulk norme, mille alusel kehtestatud määrustes võib Vabariigi Valitsus teha erisusi salastatud välisteabe kaitsel. Tegelikult 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 41 muudetakse RSVS § 51. Kuna muudatused ja täiendused on suuremahulised, on otstarbekas kehtestada paragrahv tervikuna uuesti. RSVS §-le 51 teistes RSVS-i sätetes ja muudes õigusaktides viidatud ei ole. 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 alguses tekstis. RSVKK 05.06.2023 jõustunud muudatustega eristati RSVKK-s täiendavalt juurdepääsusertifikaat ja

töötlemisertifikaat. Enne seda anti nii juurdepääsuõigus kui ka töötlemisõigus juurdepääsuserifikaadiga. 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 töötlemisertifikaadi 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 põhimõtte 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 teadmismajaduse 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. 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. Kaitseväge juhatajal ja Andmekaitse Inspeksiooni 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.

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 staatusseadus) 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, kui seda ei ole julgeolekukontrolli käigus kontrollitud, ning on esitanud nõutud dokumendid, läbinud salastatud välisteabe kaitse nõuete tutvustuse ja allkirjastanud salastatud välisteabe hoidmise kinnituse). Oluline on rõhutada, et kui füüsilisel isikul on riigisaladuse juurdepääsuluba vaja vaid selleks, et saada juurdepääsuõiguse salastatud välisteabele, peaks julgeolekukontrolli teostamiseks pädev asutus pöörduma RJVE poole, et see teeks kindlaks salastatud välisteabele juurdepääsuvajaduse olemasolu. Vastasel korral on oht, et isiku suhtes teostatakse julgeolekukontroll, kuigi see tegelikult põhjendatud ei ole.

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 töötlemisertifikaadi.

Lõikega 9 antakse KAPO-le pädevus väljastada enda ametnikele ja töötajatele juurdepääsusertifikaate. See on tingitud vajadusest kaitsta KAPO teenistujate ja koosseisu andmeid. Tegemist on (kogumis) salajase taseme riigisaladusega. Seni kehtinud regulatsiooni kohaselt tuli KAPO teenistujal, kellel on vajalik juurdepääsuõigus Euroopa Liidu või NATO salastatud teabele, pöörduda RJVE poole, kes väljastab juurdepääsusertifikaadi. Samas eelnõuga tehtavate muudatuste toimetel teeb juurdepääsuõiguse andmiseks vajaliku julgeolekukontrolli üldjuhul KAPO. RJVE juurdepääsuvajadus KAPO teenistujate andmetele ei ole vältimatult vajalik, sest ka ülejäänud juurdepääsusertifikaadi väljastamiseks vajalikud toimingud on võimalik teha KAPO-l. Muudatuse tulemusena on riigisaladuse kaitse paremini tagatud. KAPO teenistujale otsustab juurdepääsu õiguse andmise ja väljastab juurdepääsusertifikaadi KAPO. Samal põhjusel teostab VLA teenistujate julgeolekukontrolli VLA.

VLA teostab julgeolekukontrolli RSVS § 48 lõike 3 punktis 3 nimetatud KAPO teenistujate suhtes, millest tulenevalt on asjakohane, et nende teenistujate juurdepääsusertifikaate väljastab ka edaspidi RJVE. RJVE poolt juba KAPO teenistujatele väljastatud juurdepääsusertifikaadid jäävad kehtima kuni nende kehtivuse tähtaja lõpuni.

NATO julgeolekudirektiivi lisa AC/35-D/2000-REV8 punkti 3 kohaselt antakse PSC (juurdepääsusertifikaat) pärast kõigile NATO Security Policy-s sätestatud nõuetele vastava julgeolekukontrolli läbiviimist, mis hõlmab asjaomase riigi julgeoleku volitatud esindaja (inglise keeles National Security Authority (NSA)) või volitatud julgeolekuasutuse (inglise keeles Designated Security Authority (DSA)) või muu pädeva julgeolekuasutuse kinnitust selle kohta, et isikule võib lubada juurdepääsu NATO salastatud teabele. Punkti 14 kohaselt on PSC (juurdepääsusertifikaadi) andmine NSA/DSA või muu pädeva julgeolekuasutuse pädevuses.

Euroopa Liidu julgeolekueeskirjades (2013/488/EL) on juurdepääsuloa andmise kontekstis nimetatud pädevat asutust konkretiseerimata, kes see pädev asutus on. NATO julgeolekudirektiivi lisaga sarnane säte on tööstusjulgeolekut reguleeriva artikli 11 lõikes 5. Lepinglase või all-lepinglase töötajatele, kes vajavad salastatud lepingu täitmiseks juurdepääsu CONFIDENTIEL UE/EU CONFIDENTIAL või SECRET UE/EU SECRET tasemel salastatud teabele, väljastab juurdepääsuloa asjaomane riiklik julgeolekuasutus, määratud julgeolekuasutus või muu pädev julgeolekuasutus vastavalt riigisisestele õigusaktidele ja I lisas sätestatud miinimumstandarditele.

Eeltoodust tulenevalt on juurdepääsusertifikaadi andmiseks pädeva asutuse määramine riigi enda pädevuses. EL/ESA/NATO julgeolekureeglitega on kooskõlas, kui liikmesriigis väljastab juurdepääsusertifikaate mitu asutust.

Muudatuse rakendamisel tuleb arvestada järgmisi aspekte:

- 1) järgida tuleb rahvusvahelisi reegleid;
- 2) üleriigiline praktika peab jääma ühetaoliseks;
- 3) RJVE-le jääb järelevalve juurdepääsuõiguse andmise üle;
- 4) KAPO antav juurdepääsusertifikaat peab olema piiratud ulatusega;

5) NATO erimärgistusega salastatud teabele juurdepääsuks juurdepääsusertifikaatide andmine jääb RJVE pädevusse.

KAPO antavad juurdepääsusertifikaadid on ameti- või töökohaga seotud. Seni kehtis põhimõte, et reeglina jääb RJVE antud juurdepääsusertifikaat kehtima ka siis, kui isik vahetab ameti- või töökohta ning ka uuel töökohal on isikul juurdepääsuvajadus. Edaspidi, kui KAPO ametnik või töötaja lahkub KAPO-st ja asub ameti- või töökohale, kus tal on samuti juurdepääsuvajadus, või töötab lisaks KAPO-le juurdepääsuvajadusega sõjaaja ametikohal või teise tööandja juures juurdepääsuvajadusega ametikohal, peab isik taotlema juurdepääsusertifikaati lisaks RJVE-lt. Kui KAPO teenistuja liigub KAPO-st ära teisele juurdepääsuvajadusega ametikohale, siis peab KAPO tema juurdepääsusertifikaadi kehtetuks tunnistama ning uus tööandja peab RJVE-lt taotlema uue juurdepääsusertifikaadi. Vastasel korral puudub RJVE-l vajalik tervikülevaade riigiasutustes (va KAPO) ja erasektoris töötavate isikute juurdepääsusertifikaatidest.

KAPO peab oma ametnike ja töötajate juurdepääsusertifikaatide kinnitamisel järgima rahvusvaheliselt kokkulepitud norme. Rahvusvahelises suhtluses võib siiski tekkida vajadus, et juurdepääsusertifikaadi olemasolu ja külastustaotluse kinnitab RJVE, sest KAPO vastav pädevus ei ole rahvusvahelistele partneritele teada. Selliseks juhuks lepivad RJVE ja KAPO kokku tegutsemisviisi rahvusvahelistele päringutele vastamiseks.

RJVE-le jääb ülesanne tagada salastatud välisteabe juurdepääsuõiguste andmise ühetaoline praktika ja järelevalve. Eesmärk on tagada:

- 1) EL/ESA/NATO nõuetest kinnipidamine;
- 2) EL/ESA/NATO nõuete sarnane tõlgendus;
- 3) ühetaoline menetluspraktika, seal hulgas:
 - nõuete tutvustamine;
 - testid;
 - juurdepääsusertifikaadi kinnitused;
 - külastustaotlused;
- 4) dokumentide standardne vorm, seal hulgas:
 - nõuetega tutvumise kinnitus;
 - juurdepääsusertifikaat;
- 5) ülevaade varasemalt antud juurdepääsusertifikaatidest.

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 42 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 43 täiendatakse RSVS § 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 ettevõtte 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 tavapärastel viisidel 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-1 § 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 neli punkti.

Punktiga 1 antakse RJVE-le õigus anda töötlevale üksusele teavet ja õigusaktides sätestatud nõuete täitmiseks juhiseid riigisaladuse kaitse nõuete täitmiseks. 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.

Punkt 3 on sama sisuga nagu kehtiva § 52 lõike 1 punkt 6.

Punktiga 4 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.

Vabariigi Valitsuse julgeolekukomisjonile ettepanekute tegemist sätestavat punkti ei ole üle toodud, kuna Riigikantselei juhtis oma tagasisides tähelepanu, et RSVS § 22 lõike 2 punktis 4, § 23 lõike 3 punktis 4 ja § 52 lõike 1 punktis 7 sätestatakse KAPO, Kaitseväge põhimääruses määratud struktuuriüksuse, VLA ja RJVE kohustus teha Vabariigi Valitsuse julgeolekukomisjonile ettepanekuid puuduste kõrvaldamiseks ja õigusrikkumiste vältimiseks. Selline regulatsioon ei ole aga täpne, sest Vabariigi Valitsuse julgeolekukomisjon kui valitsuskomisjon ei menetle selliseid ettepanekuid. Ettepanekute menetlemine toimub vastavas ministeeriumis või Riigikantseleis.

Eelnõu § 1 punktiga 44 asendatakse RSVS § 52 lõike 3 punktis 2 sõnad „välisriigi luure- või vastuluureülesannet täitva asutusega“ sõnadega „välisriigi asutuse, rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooniga“.

Muudatuse eesmärk on välistada RJVE kontroll ka sellise kaitseväge luurega tegeleva Kaitseväge struktuuriüksuse teabevahetuse üle, mis toimub rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooniga. Sarnases ulatuses on RJVE kontroll teabevahetuse üle välistatud teiste RSVS § 52 lõikes 3 nimetatud riigiasutuste puhul. Ka kaitseväge luurega tegeleval struktuuriüksusel on vaja vahetada rahvusvaheliste organisatsioonide ja rahvusvahelise kokkuleppega loodud institutsioonidega teavet, mille puhul on teadmismajadus äärmiselt piiratud. Oluline on siiski arvestada sellega, et kui

välislepingu kohaselt peab RJVE teatud liiki salastatud välisteabe vahetust korraldama ja kontrollima, siis tuleb lähtuda välislepingust.

Eelnõu § 1 punktiga 45 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 §-ga 2 muudetakse AvTS-i § 2 lõike 2 punkti 1 ja § 35 lõiget 3. Muudatuse eesmärk on viia AvTS-i sõnastus kooskõlla salastatud välisteabe definitsiooniga.

RSVS § 3 punkti 2 kohaselt on salastatud välisteabe välisriigi, Euroopa Liidu, NATO või mõne muu rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooni poolt salastatud ja Eestile avaldatud teave ning Eesti Vabariigi poolt välislepingu täitmiseks loodud teave, mis tuleb salastada välislepingu kohaselt. Definitsioonist nähtub, et salastatud välisteave on teave, mille välisriik, rahvusvaheline organisatsioon või rahvusvahelise kokkuleppega loodud institutsioon on salastanud ja Eestile avaldanud. See, kas Eesti kaitseb seda teavet RSVS-ist või AvTS-ist lähtudes, ei oma teabe salastatud välisteabena defineerimise mõttes tähtsust. Ka AvTS-i alusel kaitstav teave võib olla salastatud välisteave, kui selle avaldaja seda ise salastatud teabeks peab.

Eelnõu §-dega 3 ja 5–9 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 4 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 § 10 kohaselt jõustub eelnõukohane seadus 2027. aasta 1. jaanuaril.

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 koostõla 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 töökoormusele** tänu seaduse selgemale sõnastusele ning pädevuste-ülesannete-tegevuste selgusele. Sellega ei kaasne olulisi riske ega negatiivseid kõrvalmõjusid.

Sihtrühm, kellele muudatused mõju avaldavad, on eelkõige salastatud teavet töötlevad riigiasutused ja muud töötlevad üksused RSVS § 3 punkti 15 mõttes. Teine sihtrühm on riigisaladuse juurdepääsuluba taotlevad füüsilised isikud. Mõju ulatus ja esinemise sagedus on väike, sest riigisaladuse juurdepääsuluba taotlevad harva isikud, kellel on teatamiskohustusega välisriigi kodakondsus, kes on pikalt välismaal elanud või kelle lähedased isikud elavad teatamiskohustusega välisriigis.

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.

Seaduse rakendamiseks tuleb muuta ka NATO tugidokumenti AC/35-D/1043, kuhu NATO on kogunud andmed, milline asutus võib igas liikmesriigis juurdepääsusertifikaate väljastada, juurdepääsusertifikaadi olemasolu kinnitada ja külastustaotlusi kinnitada.

Lisaks peab KAPO sisse seadma juurdepääsusertifikaadi andmisega seotud protsessid (juurdepääsusertifikaadi vorm, briifingumaterjal, küsimustik ja kinnitusvorm).

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 (lisa 1).

Eelnõuga luuakse RSVS-is kolm uut volitusnormi: § 35 lg 7, § 50 lg 5² ja § 51 lg 14.

RSVS § 35 lõikega 7 antakse Vabariigi Valitsusele õigus kehtestada riigisaladuse tsiviilõigusliku või halduslepingu alusel välisriigi töötlevale üksusele, rahvusvahelisele organisatsioonile või rahvusvahelise kokkuleppega loodud institutsioonile edastamise nõuded. Välisriikidega sõlmitud salastatud teabe kaitse kokkulepetes on üldjuhul ette nähtud, et tsiviilõigusliku või halduslepingu juurde, mis eeldab salastatud teabe edastamist teise riigi töötlevale üksusele, tuleb koostada julgeolekunõudeid sisaldav osa (*julgeolekulisa*), kus kirjeldatakse konkreetse projekti raames loodavat salastatud teavet ning teabe salastatuse tasemeid. Volitusnorm annab Vabariigi Valitsusele õiguse kehtestada sellise julgeolekulisa nõuded, kui riigisaladust edastatakse välismaale. Kehtivas õiguses on välismaale riigisaladuse edastamist käsitlevat julgeolekulisa reguleeritud RSVKK §-s 122¹, kuid tegemist on salastatud välisteabe töötlemist reguleerivas RSVKK osas paikneva sättega, mis ei tohiks reguleerida riigisaladuse töötlemist. Samuti puudub riigisaladuse välismaale edastamist käsitleva julgeolekulisa reguleerimiseks praegu RSVS-is volitusnorm, mis RSVS § 35 lõikega 7 luuakse.

RSVS § 50 lõikega 5² antakse Vabariigi Valitsusele õigus määrata RSVKK-s Euroopa Liidu ja NATO õigusaktide kohaselt nõutud pädevad asutused ja ühtsed kontaktpunktid. 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 toime saab Vabariigi Valitsus õiguse määrata rollide täitjad RSVKK-s.

RSVS § 51 lõikega 14 nähakse Vabariigi Valitsusele ette võimalus nimetada RSVKK-s 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 jõustumisel muutub kehtetuks siseministri 11. jaanuari 2008. a määrus nr 4 „Riigisaladuse kaitse kontrolli läbiviimiseks moodustatava komisjoni töökord“ (RTL 2008, 6, 67).

9. Seaduse jõustumine

Seadus jõustub 2027. aasta 1. jaanuaril. Kuupäeva sätestamine on vajalik, kuna on vaja muuta ka Vabariigi Valitsuse 20. detsembri 2007. aasta määrust nr 262 „Riigisaladuse ja salastatud välisteabe kaitse kord“, mille ettevalmistamine võtab aega.

10. Eelnõu kooskõlastamine

Eelnõu esitati kooskõlastamiseks eelnõude infosüsteemi (EIS) kaudu [26-0124](#) ning arvamuse avaldamiseks Eesti Pangale, Kaitseliidule, Riigikogu Kantseleile, Riigikohtule, Riigikontrollile, Vabariigi Presidendi Kantseleile ja Õiguskantsleri Kantseleile. Kaitseliidul, Riigikogu Kantseleil ja Vabariigi Presidendi Kantseleil ei olnud eelnõu kohta märkusi. Riigikohus esitas eelnõule ettepanekud. Ettepanekutega on võimaluse korral arvestatud ning kooskõlastustabel on lisatud käesolevale seletuskirjale (lisa 2).

Algatab Vabariigi Valitsus 18. mail 2026. a

Vabariigi Valitsuse nimel

(allkirjastatud digitaalselt)

Heili Tõnisson

Valitsuse nõunik