



Riigikogu Põhiseaduskomisjon
Lossi plats 1a
riigikogu@riigikogu.ee

07.10.2026 nr 5-1/26/2-14

Riigisaladuse ja salastatud välisteabe seaduse muutmise ning sellega seonduvalt teiste seaduste muutmise seaduse eelnõu (920SE) muudatusettepanekud

Riigikogu põhiseaduskomisjoni menetluses on riigisaladuse ja salastatud välisteabe seaduse muutmise ning sellega seonduvalt teiste seaduste muutmise seadus (edaspidi *eelnõu 920 SE*), mille põhieesmärk on luua ühtne struktuur teabe kaitset korraldavate ametkondade reeglites.

Alljärgnevalt esitame eelnõule 920 SE muudatusettepanekud ning loodame, et saate nimetatud ettepanekutega eelnõu menetlemisel arvestada.

1. Täiendada eelnõu § 1 uue punktiga 11 ning muuta § 1 järgnevat numeratsiooni vastavalt:

„11) paragrahvi 17 täiendatakse lõigetega 4–6 järgmises sõnastuses:

„(4) Salastatud teabekandjat tuleb kaitsta käesolevas seaduses ja selle alusel antud õigusaktides sätestatud nõuete kohaselt.

(5) Salastatud teavet või salastatud teabekandjat sisaldava relvasüsteemi, mida selle kasutusotstarbe või muu eripära tõttu ei ole võimalik või otstarbekas kaitsta käesolevas seaduses ja selle alusel antud õigusaktides sätestatud viisil, kaitse tuleb tagada muude meetmetega. Sellise relvasüsteemi kaitse meetmed kooskõlastatakse vastavalt Kaitsepolitsei ameti, Kaitseväe, Välisluureameti või riigi julgeoleku volitatud esindajaga.

(6) Vabariigi Valitsus võib riigisaladuse ja salastatud välisteabe kaitse korras ette näha käesoleva paragrahvi lõikes 5 nimetatud meetmete kohaldamise alused ja korra.“.

Selgitus

Eesti riigisaladuse kaitse süsteem põhineb valdavalt teabekesksel lähenemisel. Salastatud teabeks on õigusaktides sätestatud tunnustele vastav teave ning salastatud teabekandjaks on mis tahes objekt, millele selline teave on jäädvustatud. Riigisaladuse ja salastatud välisteabe seaduse (edaspidi ka RSVS) ja selle rakendusaktid on kujundatud eelkõige dokumentide, andmekandjate ja töötlussüsteemide kaitseks, st selline regulatsioon võimaldab tõhusalt kaitsta dokumente, andmekandjaid ja infosüsteemides sisalduvat salastatud teavet, kuid tekitab mitmeid õiguslikke ja praktilisi küsimusi kaasaegsete relvasüsteemide osas. Eelkõige tekib küsimus, kas ja millistel tingimustel on võimalik käsitada relvasüsteemi ennast salastatud teabekandjana või salastatud teabe töötlussüsteemina ning kuidas tagada selles sisalduva või selle kaudu töödeldava salastatud teabe piisav kaitse ja selle süsteemi sihipärane kasutamine olukorras, kus kõiki salastatud teabe kaitse nõudeid ei ole võimalik rakendada, kuna kaasaegsete relvasüsteemide areng on olukorda oluliselt muutnud. Tänapäevased relvasüsteemid ühendavad endas füüsilise relva, sõiduki, tarkvara, sensorid, sidevõrgud, juhtimissüsteemid, andmetöötlusvõimekused ja sageli ka autonoomsed funktsioonid. Sellest tulenevalt ei ole relvasüsteem enam käsitav üksnes relva või info/töötlussüsteemina, vaid kujutab endast mitmekihilist tehnoloogilist süsteemi, mille kaudu realiseeritakse sõjaline võimekus.

Seetõttu on salastatud teavet sisaldavate relvasüsteemide regulatsiooni kujundamisel esmase tähtsusega küsimus, kuidas relvasüsteemi salastatud teabe valdkonnas õiguslikult käsitada. Sellest sõltub, kas ja millised Eesti seadusandlusega ettenähtud salastatud teabe kaitse meetmed sellele kohalduvad, milline on selle töötlemise kord, kas süsteem vajab akrediteerimist ning millised on selle kasutamise, säilitamise, vedamise ja hävitamise nõuded. Samas ei ole salastatud teavet sisaldav relvasüsteem tavapärane süsteem, sest selle põhieesmärk ei ole ainult teabe töötlemine/hoiustamine, vaid hoopis sõjalise mõju tekitamine ja seda ka asukohtades ning olukordades, kus ei pruugi olla võimalik täita RSVS-is või selle alusel kehtestatud õigusaktides sätestatud nõudeid (nt kasutamine turvaalal). Seetõttu peavad salastatud teabe kaitse regulatsioonid võimaldama kasutada salastatud teavet sisaldavat relvasüsteemi nii nagu seda on loodud/mõeldud kasutama. Seega on vajalik salastatud teabe kaitse regulatsiooni täiendamine salastatud teavet sisaldavate relvasüsteemide eripäradega.

Probleemi aktuaalsust suurendab asjaolu, et Kaitsevägi on viimastel aastatel kasutusele võtnud või kasutusele võtnud mitmeid kõrgtehnoloogilisi relvasüsteeme, mille toimimine põhineb keerukatel sensoritel, sidevõrkudel, tulejuhtimissüsteemidel, tarkvaral ja andmetöötlusel. Nende süsteemide sõjaline väärtus ei seisne üksnes füüsilises relvas, vaid suurel määral ka nende tehnoloogilistes lahendustes, tarkvaras, andmetes ja kasutamise põhimõtetes. Seetõttu on vajalik, et salastatud teavet sisaldavaid relvasüsteeme saaks kasutada vastavalt nende otstarbele, kuna see otseselt suurendab Eesti kaitsevõimet, parandab liitlassuhteid ja tõstab riiklikku julgeolekut.

Kuna relvasüsteem võib ise olla salastatud teabekandja või sisaldada salastatud teabekandjat, siis arusaadavalt ei ole alati võimalik relvasüsteemi hoida ja kasutada eesmärgipäraselt, nt turvaalale ettenähtud tingimustes. Relvasüsteemi lahingumoon, mis on või mis sisaldab salastatud teabekandjat, hävimine/hävitamine toimub selle eesmärgipärase kasutamise käigus, samuti ei ole (topelt)pakendamise nõude täitmine mõeldav, kui toimub teatud suuruses relvasüsteemi vedu. Relvasüsteemi eesmärgipärasel kasutamisel, st sõjaväelisel väljaõppel osalemisel, aga ka riigi sõjalisel kaitsmisel on vaja nendega liikuda või neid kasutada avalikus ruumis. Üldistatud kujul eluline näide on relvasüsteem, mille juhtimispuht/tulejuhtimisseade (mis on selle süsteemi oluline osa) tuleb süsteemi kasutamiseks viia sõidukist/platvormist eemale ja kuivõrd selline vajadus võib tekkida mh ootamatult ja ettevalmistamata asukohas, siis ei ole alati võimalik selleks kehtestada ajutist turva- ega ka administratiivala ning juhtimispuhtiga tuleb nt kuni SALAJASEL tasemel salastatud teavet töödelda avalikus ruumis. Sisuliselt tuleb keset metsa jalastuda ja relvasüsteemi kasutada sellise (mehitatud) valvega, mis parajasti võtta on.

Relvasüsteem on enamasti kompleksne süsteem ja koosneb paljudest erinevatest (sh liikuvatest) osadest, mis täiendavad/täiustavad teineteist ning nende erinevate osade kasutamine toimub paralleelselt. Seega on relvasüsteemi sihipäraseks kasutamiseks oluline mõista, et antud erandi eesmärk on katta ka relvasüsteemi juurde kuuluvad olulised osad, mis ise on või sisaldavad salastatud teavet. Nendeks võivad olla relvasüsteemi vajalikud varuosad, aga ka dokumentatsioon (nt kasutusjuhendid, tehnilised joonised) ja lahingumoon, mis on vajalikud relvasüsteemi efektiivseks kasutamiseks ning millega tuleb vajaduse korral relvasüsteemi või selle ümber avalikus ruumis tutvuda/kasutada. Relvasüsteemi salastatud osad võivad olla nt laskeseadmed, radarid, tulejuhtimiskeskus, sõidukid, raketid, mobiilsed ja mittemobiilsed tulejuhtimisseadmed jne. Täpset loetelu, mis on relvasüsteemi juurde kuuluv oluline osa, ei ole mõistlik seaduses ammendava loeteluna määratleda, kuna iga relvasüsteem ja selle kasutamise tingimused ning selle juurde kuuluvad osad on erinevad. Seetõttu on mõistlik, et relvasüsteemi juurde kuuluvaid olulisi osasid ei hakata õigusakti tasandil eraldi nimetama, vaid see on iseenesest mõistetav, et erandi alla läheb kogu relvasüsteem ehk ka kõik süsteemi vajalikuks toimimiseks ettenähtud osised.

Et Eesti salastatud teabe kaitse õigusruum vastaks paremini kaasaegsete relvasüsteemide olemusele, on vaja luua erand, kus salastatud teavet või salastatud teabekandjat sisaldava relvasüsteemi kasutamisel on võimalik teha teatud erisusi salastatud teabe kaitse nõuetes. Salastatud teavet või salastatud teabekandjat sisaldavate relvasüsteemide erandi rakendamine siiski ei tähenda, et reegleid üldse ei ole või et neid ei pea järgima, vaid vastava relvasüsteemi kasutamine, mille puhul ei ole võimalik salastatud teabe kaitse õigusaktides toodud kaitse meetmeid kohaldada, siis nende kaitse nõuded tuleb kooskõlastada järelevalvet tegeva asutusega, kes seda tehes peab olema veendunud, et kasutusele

võetavad kaitse meetmed on piisavad tagamaks relvasüsteemi enda ning ka salastatud teabe vajaliku kaitse. Selliste relvasüsteemide puhul tuleb kooskõlastamise käigus välja tuua, milliseid õigusaktides nimetatud kaitse meetmeid ei kasutata ja samas kirjeldatakse, kuidas ning milliste muude meetmetega tagatakse teabe (sh teabekandja) vajalik kaitse. Antud muude meetmete eesmärk on tagada, et vajalik kaitsetase oleks vähemalt samaväärne, kui RSVS-is või nt Vabariigi Valitsuse 20. detsembri 2007. a määruses nr 262 „Riigisaladuse ja salastatud välisteabe kaitse kord“ (edaspidi ka RSVKK) on toodud. Kui kooskõlastamise protsessi käigus ei ole konkreetset erandit loodud, kohalduvad õigusaktides toodud kaitsemeetmed. Nt, kui sellise relvasüsteemi kaitse puhul rakendatakse RSVS-i ja RSVKK-d, siis ei pea nendes õigusaktides toodud ja rakendatavaid kaitsemeetmeid eraldi kooskõlastama ning seda isegi, kui muus osas erandit küsitakse (st kooskõlastada on vaja ainult erandlikud kaitsemeetmed). Nt relvasüsteemi sihipäraseks kasutamiseks Kaitseväe territooriumil ei ole erandi küsimise vajalik, aga avalikus ruumis kasutamiseks on mingi kaitsemeetme erand vajalik, siis tuleb kooskõlastada vaid see konkreetne kaitsemeetme erand. Järelevalveasutus oma kooskõlastuse kaudu saab anda hinnangu, kas ettenähtud meetmete kogum, tagab piisava salastatud teabe kaitse. Nimetatud kooskõlastust ei ole siiski vaja teha kõikide loetletud asutustega, vaid kooskõlastajad sõltuvad teabe liigist või töötlevast üksusest, nt 1) Kaitseväe struktuuriüksuse poolt kasutatav relvasüsteem, mis töötleb salastatud välisteabega, siis sellisel juhul on muude kaitse meetmete kooskõlastajateks luurekeskus (kui riigisaladuse kaitse korraldaja Kaitseväes) ja Riigi julgeoleku volitatud esindaja (kui salastatud välisteabe kaitse korraldaja ja kontrollija); 2) Kaitseväe struktuuriüksuse poolt kasutatav relvasüsteem, mis töötleb salastatud välisteavet ja on ühtlasi ka töötlussüsteem, siis sellisel juhul on muude kaitse meetmete kooskõlastajateks luurekeskus (kui riigisaladuse kaitse korraldaja Kaitseväes) ja Riigi julgeoleku volitatud esindaja (kui salastatud välisteabe kaitse korraldaja ja kontrollija) ning Välisluureamet (kui elektroonilise teabeturbe korraldaja ja selleks kehtestatud nõuete täitmise kontrollija).

Relvasüsteemi kasutamisel (nt taktikalistes situatsioonides) on Kaitseväe struktuuriüksusel, kes sellist süsteemi kasutab, olemas standardprotseduurid, mis tavapäraselt saadakse relvasüsteemi väljaõppe käigus tootja poolt või veelgi varem (nt relvasüsteemi kohta käiva dokumentatsiooni tutvumise raames). Siis neid samu protseduure saab planeeritava erandi rakendamise raames kasutada, nt Kaitseväe struktuuriüksus fikseerib need konkreetse relvasüsteemi kasutusloos ja ühtlasi kirjeldab, kuidas relvasüsteemi kasutatakse ja kuidas (relvasüsteemiga seotud) salastatud teavet töödeldakse ning seda kaitstakse (sh määratleb ka relvasüsteemi juurde kuuluvad olulised osad). Otstarbekas on kirjeldada igat toimingut, mille puhul ei järgita RSVS-is ja selle alusel antud õigusaktides sätestatud nõudeid (nt märgistamist, hoiustamist, hävitamist, vedamist jne) ning koheselt kirjeldatakse, milliste meetmetega tagatakse vajalik turvalisus, et tagada salastatuse vajalik konfidentsiaalsus, terviklus ja käideldavus. Relvasüsteemi kui salastatud teabekandja suhtes RSVS-is ja selle alusel antud õigusaktides sätestatud käitlemise nõuete kohaldamata jätmine ei tohi viia salastatud teabe kaitse ärajätmiseni, vaid selle kaitset on nt Kaitseväe struktuuriüksusel võimalik tagada teistes õigusaktides sätestatud meetmetega. Eelkõige on selleks Kaitseväe julgeolekuala, Kaitseliidu valvatav objekt ja muud sellised regulatsioonid, mille kaudu on relvasüsteemile võimalik tagada piisav kaitse, kuid puuduvad otsesed RSVS-ist ja selle alusel antud õigusaktidest tulenevad nõuded nt turvaalale, vedamisele, pakendamisele, hävitamisele vms. Selline erand annab võimaluse nt riskipõhiselt luua üldistest nõuetest teistsugused kaitsemeetmed, mis arvestavad relvasüsteemi kasutuslooga. Samuti on salastatud teabe töötlemisega seonduv võimalik kokku leppida eraldi hankelepingle juurde lisatavates julgeolekutingimustes. Sellisel juhul ei ole mõistlik, kui relvasüsteemi täpsem kasutamine on juba kokku lepitud, et hakatakse veel eraldi täiendavaid erandeid uuesti kirjeldama, vaid kasutada saab juba kokkulepitud julgeolekutingimusi.

Samuti antakse Vabariigi Valitsusele võimalus RSVKKS-s ette näha kompenseerivate meetmete kohaldamise üldised alused ja kord. Vabariigi Valitsus saab vajaduse korral kehtestada need kaitse meetmed, millest mingil juhul ei tohi kõrvale kalduda või siis vastupidi, loetleda need meetmed, mida on lubatud asendada muude meetmetega.

2. Sõnastada eelnõu § 1 punktis 14 (uue numeratsiooniga 15) esitatud riigisaladuse ja salastatud välisteabe seaduse § 20¹ lõike 1 punkt 2 järgmiselt:

„2) valdkonna eest vastutava ministri otsuse alusel, mis on tehtud pärast Siseministeeriumi, Välisministeeriumi, julgeolekuasutuste ja riigi julgeoleku volitatud esindaja arvamuste ärakuulamist, ning tingimusel, et teabe vastuvõtja tagab kaitse avaldatava teabe avalikuks tuleku eest.“.

Selgitus:

01.10.2026 kehtima hakanud kriisiolukorra ja riigikaitse seadusega (KORKS) tehti muudatused ka RSVS-is, mille tulemusel jäeti RSVS-ist välja Vabariigi Valitsuse julgeolekukomisjoni (edaspidi VVJK) pädevust ja ülesandeid reguleerivad sätted. Põhjendusena on toodud, et VVJK ülesanded on kavas sätestada VVJK põhimääruses, sest ükski neist ülesannetest pole selline, mille üle peab otsustama seadusandja. Soovitus on vaadata VVJK ülesanded üle, lähtudes sellest, et VVJK peaks ennekõike tegelema üldiste, strateegiliste teemadega ning mitte konkreetseid kaasusi puudutavate küsimustega (KORKS seletuskiri lk 450).

Erandina on VVJK-d endiselt mainitud RSVS § 35 lõike 4 punktis 2. Eelnõuga 920 SE tõstetakse RSVS § 35 lõike 4 punkti 2 regulatsioon RSVS § 20¹ lõike 1 punkti 2, mille kohaselt võib töötlev üksus avaldada riigisaladust välisriigi töötlevale üksusele, rahvusvahelisele organisatsioonile või rahvusvahelise kokkuleppega loodud institutsioonile VVJK otsuse alusel, kui teabe vastuvõtja tagab kaitse avaldatava teabe avalikuks tuleku eest.

Kehtiva RSVS-i seletuskirjas on märgitud, et VVJK peaks iga kord teabega tutvuma, et anda hinnang. See on VVJK olemust arvestades ebaoproportsionaalselt detailne ülesanne. Laiemas vaates peaks VVJK roll olema poliitika suunamine, mitte tehniliste üksikjuhtumite lahendamisega tegelemine.

Ettepanek on asendada VVJK valdkonna eest vastutava ministriga. See tähendab, et kui soovitakse avaldada välissuhtlemisega seotud riigisaladust, siis teeb otsuse välissuhtlemise valdkonna eest vastutav minister ning kui soovitakse avaldada kaitsekoostööga seonduvat riigisaladust, siis teeb otsuse kaitsevaldkonna eest vastutav minister jne. Sel viisil on tagatud, et otsuse langetaja võtab otsuse eest poliitilise vastutuse. Samas eeldab teabe kaitstuse sisuline hindamine erialast kompetentsi ning järeldusi tuleb sisuliselt põhjendada. Asjakohase hinnangu saavad anda vaid pädevad asutused.

Seetõttu tuleb ministril enne otsuse langetamist ära kuulata järgmiste asutuste arvamus:

- 1) Siseministeerium – riigisaladuse kaitse eest vastutav ministeerium;
- 2) Välisministeerium – välissuhtlemise eest vastutav ministeerium;
- 3) riigi julgeoleku volitatud esindaja – riigisaladuse avaldamine välisriigile, rahvusvahelisele organisatsioonile ja rahvusvahelise kokkuleppega loodud institutsioonile;
- 4) Välisluureamet – ohuhinnang;
- 5) Kaitsepolitsei – riigisaladuse kaitse ja ohuhinnang.

Nimetatud asutused omavad kogumis vajalikku kompetentsi, et hinnata konkreetse välisriigi, rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooni suhteid Eestiga ning laiemalt teiste riikide, rahvusvaheliste organisatsioonide ja rahvusvahelise kokkuleppega loodud institutsioonidega, näiteks Euroopa Liidu või Põhja-Atlandi Lepingu Organisatsiooniga (NATO). Samuti omavad nimetatud asutused kompetentsi, et hinnata välisriigi, rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooni poolt avaldatava riigisaladuse kaitseks rakendatavaid kaitsemeetmeid ning tahet ja võimekust avaldatavat riigisaladust kaitsta. See tagab ministrile võimaluse langetada informeeritud otsus. Ministri ülesanne ei ole tutvuda detailselt avaldatava teabega, vaid kujundada ülalnimetatud asutuste abiga arusaam konkreetse välisriigi, rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooni välissuhete ja salastatud teabe kaitseks rakendatavate kaitsemeetmete osas ning selle pinnalt langetada otsus, kas riigisaladuse avaldamise korral on see tõenäoliselt kaitstud või mitte. Oluline on rõhutada, et minister ei pea otsustama iga üksiku riigisaladust sisaldava teabekandja edastamist, vaid annab loa riigisaladuse avaldamiseks konkreetse projekti või koostöösuhte (nt relvajõudude koostöö) raames.

Juhtumeid, kus ministril tuleb riigisaladuse avaldamise osas otsus langetada, esineb tõenäoliselt harva. Enamiku Eesti jaoks oluliste välisriikidega on juba sõlmitud salastatud teabe vastastikuse kaitse kokkulepped ja mitmed sellised kokkulepped on veel sõlmimisel. Eesti jaoks oluliste rahvusvaheliste organisatsioonide ja rahvusvahelise kokkuleppega loodud institutsioonide salastatud teabe kaitse reeglite järgimise kohustuse on Eesti üldjuhul võtnud nendega ühinedes. Seega peab minister riigisaladuse avaldamise otsustama väga harvadel juhtudel.

3. Täiendada eelnõu § 1 uue punktiga 27 (uue numeratsiooniga 28) ning muuta § 1 järgnevat numeratsiooni vastavalt:

„27) paragrahvi 30¹ lõikes 1 asendatakse sõna „riigikaitse“ sõnadega „kriisiolukorra ja riigikaitse“;“.

Selgitus:

01.10.2026 kehtima hakanud KORKS-iga muudetakse ka RSVS § 7 pealkirja, aga RSVS § 30¹ lõike 1 sõnastuse loogikas on kasutatud just RSVS §-de 7 ja 10 pealkirja sõnastust, seega on vaja muuta ka RSVS § 30¹ lõike 1 sõnastust ning lisada sõna „riigikaitse“ ette sõnad „kriisiolukorra ja“. Selle muudatusega tagatakse, et RSVS § 30¹ toodud põhimõtte jääks alles ja rakendatavaks.

4. Täiendada eelnõu § 1 uue punktiga 32 (uue numeratsiooniga 34) ning muuta § 1 järgnevat numeratsiooni vastavalt:

„32) paragrahvi 34² lõikes 1 asendatakse tekstiosa „lõikes 4“ tekstiosaga „lõigetes 4 ja 4¹“;“.

Selgitus:

Muudatusettepaneku eesmärk on anda kaitseväeluuret teostavale Kaitseväe struktuuriüksusele analoogne erand akrediteerimise nõudest, nagu on RSVS § 34² lõikes 4 ette nähtud julgeolekuasutuste puhul. RSVS § 34² lõige 1 sätestab riigisaladuse elektroonse töötlemise lubatavuse. Kehtiva õiguse kohaselt võib riigisaladust elektrooniliselt töödelda töötlussüsteemis, millele on antud vastav sertifikaat või kasutusluba, v.a sama paragrahvi lõikes 4 sätestatud juhul, mille kohaselt julgeolekuasutuse töötlussüsteemi, mida kasutatakse riigisaladuse edastamiseks välisriigi politsei- või julgeolekuasutusele, võib kasutada julgeolekuasutuse juhi otsuse alusel, kus määratakse töötlussüsteemis töödelda lubatud riigisaladuse tase, töötlussüsteemi kasutamise tähtaeg ning käesolevas seaduses ja selle alusel antud õigusaktides sätestatud elektroonilise teabeturbe nõuete täitmise ja kontrollimise eest vastutavad struktuuriüksused. Muudatusettepanekuga täiendatakse erandi tegemist ka Kaitseväeluuret teostava Kaitseväe struktuuriüksuse töötlussüsteemile, mis on kavandatud eelnõuga 920 SE muudatava RSVS § 34² lõikes 4¹.

5. Sõnastada eelnõu § 1 punktis 32 (uue numeratsiooniga 35) esitatud riigisaladuse ja salastatud välisteabe seaduse § 34² lõige 4¹ järgmiselt:

„(4¹) Kaitseväe põhimääruses määratud kaitseväeluuret teostava Kaitseväe struktuuriüksuse töötlussüsteemi, mida kasutatakse riigisaladuse edastamiseks välisriigi luure- või vastuluureülesannet täitvale asutusele, võib kasutada Kaitseväe juhataja või tema poolt volitatud Kaitseväe põhimääruses määratud kaitseväeluuret teostava struktuuriüksuse ülema 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.“

Selgitus:

Muudatusettepaneku eesmärk on kaitseväeluuret teostavale Kaitseväe struktuuriüksusele anda analoogne erand akrediteerimise nõudest, nagu on RSVS § 34² lõikes 4 ette nähtud julgeolekuasutuste puhul. Rahvusvahelise koostöö raames on kaitseväeluure valdkonnas ja luure koostöö arendamise huvides vajadus erinevate töötlussüsteemide kasutamiseks. Kaitseväeluuret teostav Kaitseväe struktuurüksus teeb igapäevaselt koostööd välisriikide partnerteenistustega ning infot vahetatakse töötlussüsteemides, mis on teiste riikide poolt Eestile usaldatud ja kus töödeldakse riigisaladust eelkõige konkreetse koostöö kontekstis. Samuti peab kaitseväeluuret teostaval Kaitseväe struktuuriüksusel olema võimalus enda ehitatud töötlussüsteeme koostöö raames partnerteenistusele kasutada anda. Sellistele töötlussüsteemidele ei peaks kehtima akrediteerimise nõue, kuivõrd tuleb arvestada teadmisyajaduse põhimõttega (sama põhimõtte, mis rakendub teabele, mille osas puudub RJVE-l korraldamise funktsioon – uus RSVS § 23¹ lõige 4). Kaitseväe juhatajal on ka teistest õigusaktidest nagu näiteks Kaitseväe korralduse seadusest tulenevalt võimalus teatud juhtudel pädevaid ülemaid volitada konkreetseid ülesandeid tegema. Volitusnormi eesmärk on tagada Kaitseväe tõhus, paindlik ja operatiivne korraldus olukordades, kus töötlussüsteemide kasutusele võtmine puudutab kaitseväeluuret teostava struktuuriüksuse tööülesandeid ja vastutusvaldkonda luuret ja vastuluuret puudutavas salastatud teabe

vahetuses välisriigi luure- või vastuluureülesannet täitva asutusega. Kaitseväge juhatajal asutuse juhina lasub üldvastutus asutuse tegevuse ja infosüsteemide õiguspärase ning eesmärgipärase kasutamise eest, kuid praktikas ei ole otstarbekas ega alati võimalik, et kõik töötlussüsteemide kasutuselevõtmise otsused tehakse üksnes asutuse juhi tasandil. Struktuuriüksuste juhid omavad vahetut ülevaadet oma valdkonna tööprotsessidest ja vajadustest ning suudavad hinnata, milliste töötlussüsteemide kasutuselevõtmine on vajalik põhimäärustes sätestatud ülesannete tõhusaks ja eesmärgipäraseks täitmiseks. Volitamise võimaldamine aitab kiirendada töökorralduslike ja tehniliste otsuste tegemist, vähendada asutuse juhi halduskoormust, tagada paindlikuma ja vajaduspõhisema juhtimise, et otsuseid teeksid isikud, kellel on vastava valdkonna sisuline pädevus ja praktiline teadmine. Kaitseväge põhimääruses määratud kaitsevägehuuret teostav struktuuriüksus on muuhulgas riigisaladuse kaitset korraldav ja järelevalvet teostav struktuuriüksus Kaitseväes ja Kaitsealiidus ning omab pädevust hinnata salastatud teabe töötlemiseks mõeldud töötlussüsteemides salastatud teabe kaitse tagamiseks rakendatavaid vajalikke nõudeid ja meetmeid. Samas ei vabasta volitamine Kaitseväge juhatajat vastutusest asutuse tegevuse seaduslikkuse ja teenistuslikku järelevalvet tegemise eest Kaitseväge struktuuriüksustes. Arvestades asjaolu, et riigi julgeoleku volitatud esindaja (edaspidi ka RJVE) ei korralda ega kontrolli kaitsevägehuuret teostava Kaitseväge struktuuriüksuse huuret ja vastuluuret puudutava riigisaladuse ja salastatud välisteabe vahetust, on põhjendatud, et Välisluureamet (edaspidi VLA) ei akrediteeri selleks otstarbeks kasutatavaid töötlussüsteeme. Näiteks ei pea riigisaladuse edastamist registreerima RJVE juures, kui välisriigile edastatakse muuhulgas kaitsevägehuuret teostava Kaitseväge struktuuriüksuse kogutud ja sünteesitud teavet (RSVS § 35 lõige 6) ja RJVE ei kinnita rahvusvahelisi külastustaothuseid RSVS § 52 lõikes 3 sätestatud juhul (RSVKK § 122²). Tulenevalt eeltoodust ei peaks VLA akrediteerima töötlussüsteeme, mis on ette nähtud RSVS § 7 punktides 7, 10 ja 11 nimetatud teabe vahetamiseks välisriigi luure- või vastuluureülesannet täitva asutusega.

6. Täiendada eelnõu § 1 uue punktiga 41 (uue numeratsiooniga 44) ning muuta § 1 järgnevat numeratsiooni vastavalt:

„**41)** paragrahvi 50 täiendatakse lõikega 9 järgmises sõnastuses:

„(9) Salastatud välisteavet sisaldava teabekandja, mida selle kasutusotstarbe või omaduse tõttu ei ole võimalik või otstarbekas töödelda käesolevas seaduses ja selle alusel kehtestatud õigusaktides sätestatud nõuete kohaselt, töötlemise nõuded võib kooskõlastatult riigi julgeoleku volitatud esindaja ja välisriigi pädeva asutuse, rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooniga leppida kokku tsiviilõiguslikus või halduslepingus.““

Selgitus:

Paragrahvi 50 lõike 9 sõnastus salastatud välisteabe erisuse osas on teadlikult formuleeritud laiemalt, kuna selle eesmärk ongi laiendada RSVS-is toodud salastatud välisteabe kaitse erisusi ka teistele teabekandjatele, mitte ainult relvasüsteemidele. Salastatud välisteavet võivad sisaldada ka muud teabekandjad, mis ei ole seotud ainult relvasüsteemidega (nt raadiosaatjad ning muud sidevahendid ja kaasaskantavad töötlussüsteemid) ning selliste toodete/objektide puhul võib tekkida vajadus rakendada teistsuguseid töötlemise/kaitse nõudeid ehk selliseid nagu tootjariik seda ette näeb. Paragrahvi 17 lõike 5 erandit rakendatakse olukorras, kus tootjariik ei ole Eestile salastatud teabe kaitse nõudeid relvasüsteemi kasutamisel nii detailselt lepinguga ette kirjutanud, mille tõttu peab Eesti vastavad erandlikud nõuded ise kehtestama. Paragrahvi 50 lõike 9 erandi kohaldamisala on küll laiem, kuid erandi mõte on kaitsta salastatud välisteavet täpselt nii nagu tootjariik on Eestile lepinguliselt ette näinud ehk mitte Eesti üldiste salastatud teabe kaitse nõuete kohaselt.

Lugupidamisega
(allkirjastatud digitaalselt)

Martin Herem
minister