

Väljatöötamiskavatsus
Riigihangete seaduse muutmine
 (tarneahela arvestamine IKT riigihangetes)

1. Lahendatav probleem

Kehtiv õigus ei piira ega keela riskiriikide tehnoloogia kasutamist Euroopa Liidu (EL) või riiklikul tasandil. Hetkel ei ole Euroopa-üleselt riiklikku kokkulepet, tehnoloogilisi piiranguid (nt lubatud ja keelatud tehnoloogiate/toodete nimekirju) ega kehtestatud juhiseid kolmandate, see tähendab väljapoolt Euroopa Liitu, riikide tehnoloogia välistamiseks. Riskipõhise lähenemise kontekstis käsitletakse muu hulgas ka tarneahelaga seotud riske.

Riskiriikidest¹ sõltuvuste vähendamist arutas Vabariigi Valitsus oma 2023. a mai kabineti nõupidamisel, kus võeti teadmiseks Riigi Infosüsteemi Ameti (RIA) ülevaade ja ettepanekud ning soovitused valitsussektori sõltuvust vähendamiseks kolmandate riikide tehnoloogiast. Ettepanekud keskendusid riski haldamisele ja infoturbemeetmetele sh riski- ja ohuhinnangud, teavitust, regulatiivsetele võimalustele sh hangetes geopoliitilise või julgeolekuriski arvestamine ning tehnilistele meetmetele, ennekõike seadmete keskhaldus. 2025. aasta juunis antud soovituste järgimise ülevaates tõdeti riskiriikide tehnoloogia osakaalu vähendamine ei ole toiminud loodetud ulatuses ning mitmed ettepanekuid ei oldud üldse rakendatud. Peamise põhjusena toodi rakendajate poolt välja õigusruumi vähenemine või puudumine.

Riigihangete seadus (RHS) ning sellega seotud riigihangete korralduslikud meetmed ei taga Eestis tehnoloogiaga seotud riigihangete puhul piisavat ja ühtset kaitset riskiriikidest pärit tehnoloogia kasutuselevõtu takistamiseks. Kuigi kehtivad regulatsioonid (nt RHS või kavandatavad elutähtsa teenuse toimepidevuse nõuded) võimaldavad teatud juhtudel arvestada julgeoleku- ja turberiskidega, esineb puudujääke olemasolevate õiguslike aluste selguses ja praktilises rakendatavuses. Eelkõige ei ole piisavalt üheselt määratletud, millistel tingimustel ja milliste kriteeriumite alusel saavad hankijad riskiriikidega seotud tehnoloogiat tuvastada, sellega kaasnevaid riske hinnata ning vajaduse korral sellise tehnoloogia kasutamist välistada. Selle tulemusel on hankijate praktikad ebaühtlased ning riskiriikide tehnoloogia käsitlemine sõltub suuresti konkreetse hanke iseloomust, hankija riskitaluvusest ja õigusnormide tõlgendamisest.

¹ Riskiriigina on käsitletav eelkõige riik:

- 1) mis ei ole Euroopa Liidu, Põhja-Atlandi Lepingu Organisatsiooni või Majandusliku Koostöö ja Arengu Organisatsiooni liikmesriik;
- 2) kus ei järgita demokraatliku õigusrõõgi põhimõtteid ja ei austata inimõigusi;
- 3) kus ei kaitsta Eesti isikute intellektuaalomandit, isikuandmeid ja ärisaladust;
- 4) mis käitub küberruumis agressiivselt;
- 5) millele on Euroopa Liit, Põhja-Atlandi Lepingu Organisatsioon või Majandusliku Koostöö ja Arengu Organisatsioon omistanud küberrünnakuid;
- 6) kus puudub sõltumatu kohtulik kontroll asukohariigi või valitsusele või riigiasutuse üle;
- 7) mis võib oma kodanikku või juriidilist isikut kohustada tegutsema Eesti Vabariigi julgeolekut ohustaval viisil;
- 8) kus majandustegevus ei järgi turupõhise konkurentsi põhimõtteid või ei ole piisavaid tingimusi turupõhise konkurentsi põhimõtete järgimiseks.

Riskiriigina käsitletakse ka eelpool nimetatud tingimustele vastavaid territooriume, mis on välisriigi poolt okupeeritud või annekteeritud või välisriik omab olulist mõju territooriumi üle (nt Transnistria Moldaavia Vabariik)

Praktikas mõjutab erandite rakendamist ka järelevalvepraktika, mille järgi peavad põhjendused olema konkreetsed ning seotud konkreetse toote või teenusega. Tooteomanik peab koostama tootjapõhise riskianalüüsi, milles peab välja tooma toote tehnilise ohu ja mõju kirjelduse, kuidas konkreetne tehnoloogia kujutab endast julgeolekuriski. Siinkohal on vastutus infoturbejuhtidel, kes peavad asutuse töötajaid harima ning ohuteadmust vastutavate töötajatega (tooteomanik, hankija) jagama ning kehtestama praktikad, mis kaitsevad asutust julgeoleku riskide realiseerumise eest.

Riigikontrolli varasemad auditid on näidanud, et olukorras, kus riskide hindamise ja turvameetmete rakendamise nõuded ei ole piisavalt selgelt määratletud, võib riskide käsitlemise praktika olla ebaühtlane. Näiteks elektriga varustavate objektide turvalisuse auditis leidis Riigikontroll, et väljaspool selgelt reguleeritud objekte oli ohtude analüüsimine ja meetmete rakendamine suuresti ettevõtjate enda otsustada ning see ei olnud taganud piisavat valmisolekut erinevate ohtude realiseerumiseks.²

Rahandusministeerium (RaM) on algatanud riigihangete seaduse muudatuse, millega nähakse ette hankijatele kohustus arvestada riigihangetes julgeolekuriskidega, seega on õigusraamistiku täiendamine juba käimas. RaM eestveetava seadusemuudatus jõustub 1. november 2026. Lisaks on Euroopa Komisjoni välja kuulutanud riigihangete direktiivi muutmissetepanekud (COM(2026) 590)³ 9. septembril 2026. Justiits- ja Digiministeerium on andnud oma soovitusel RaMile EL riigihangete direktiivi muutmissetepanekute kogumise protsessis.

Riiklike teenuste toimimine sõltub järjest enam info- ja kommunikatsioonitehnoloogia (IKT) süsteemidest, toodetest ja teenustest, mille kaudu osutatakse avalikke teenuseid, hallatakse riigi võrgu- ja infosüsteeme ning töödeldakse suures mahus tundlikke ja riigisaladusega seotud andmeid. Sellest tulenevalt ei ole tehnoloogia valik enam üksnes majanduslik või tehniline küsimusi, vaid sellel on otsene mõju riigi julgeolekule, avalikule korrale, avalike või elutähtsate teenuste toimepidevusele⁴ ja strateegilisele sõltumatusle.

Viimastel aastatel on rahvusvaheline julgeolekuolukord oluliselt muutunud. EL, Põhja-Atlandi Lepingu Organisatsioon (NATO) ja mitmed nimetatud organisatsioonide liikmesriigid on korduvalt juhtinud tähelepanu, et autoritaarsed riigid võivad kasutada tehnoloogiaettevõtteid oma välis- ja julgeolekupoliitiliste eesmärkide saavutamiseks. Risk ei seisne üksnes toodete tehnilistest omadustes või võimalikes turvanõrkustes, vaid ka tootjate õiguslikus ja poliitilises keskkonnas. Mitmes sellises riskiriigis kehtivad õigusnormid, mis võimaldavad riskiriigil kohustada ettevõtjaid tegema koostööd nende julgeolekuasutustega, sealhulgas võimaldama ligipääsu ettevõtja klientide andmetele ja klientide töödeldavatele andmetele või osalema luuretegevuses. Samuti võib selline koostöökohustus hõlmata võimalust sekkuda tehnoloogia või seadmete toimimisse, sealhulgas võtta üle nende haldamine, piirata nende funktsionaalsust või need välja lülitada. Sellest tulenevalt võib teatud riikidest pärineva tehnoloogia kasutamine kujutada endast strateegilist julgeolekuriski ka juhul, kui konkreetse toote tehnilist kompromiteerimist ei ole võimalik tõendada. EL tasandil puudub praegu avalike hangete jaoks üldkohaldatav ja kõiki liikmesriike siduv raamistik, mis kehtestaks riskiriikidest pärineva

²https://www.riigikontroll.ee/sites/default/files/documents/2026-01/AK-ta%20KV_KA_80138_Elektriga%20varustavate%20objektide%20turvalisus_09.01.2025_AK_LOPP.pdf

³ [EUR-Lex - 52026PC0590 - EN - EUR-Lex](#)

⁴ Toimepidevuse all mõeldakse eelkõige toimepidevust kriisiolukorra ja riigikaitse seaduse § 23 lõike 1 tähenduses.

tehnoloogia kasutamise üldise keelu või sisaldaks ammendavat nimekirja⁵ lubatud ja keelatud tehnoloogiatest. Samas on teatud strateegilistes valdkondades, eelkõige elektroonilise side ning laiemalt IKT-valdkonnas, välja töötatud riskihindamise ja riski maandamise mehhanismis, mis võimaldavad hinnata kõrge riskiga tarnijatest tulenevaid julgeoleku- ja tarneahelariske ning piirata nende tarnijate kasutamist. Näiteks on ELi tasandil välja töötatud 5G võrkude küberturvalisuse meetmete kogub (5G Toolbox⁶) ning 2026. aasta veebruaris vastuvõetud IKT-tarneahela turvalisuse meetmete kogum (EU ICT Supply Chain Security Toolbox⁷), mis pakuvad liikmesriikidele ühiseid põhimõtteid tarnijate ja tarneahelatega seotud riskide tuvastamiseks, hindamiseks ja maandamiseks. Need meetmekogumid ei ole siiski õiguslikult siduvad ega kehtesta kõigile liikmesriikidele ühetaolisi tehnoloogia kasutamise piiramist

Sarnane olukord on ka Eestis. Õigusaktid võimaldavad teatud juhtudel arvestada julgeoleku- ja tarneahelariskidega, kuid riskiriikidega seotud tehnoloogia välistamiseks ette nähtud selgemaid õiguslikke võimalusi saavad kasutada üksnes julgeolekuasutused. Teistel hankijatel puuduvad ühtsed ja piisavalt selged õiguslikud alused selliste tehnoloogiate riskide hindamiseks ning vajaduse korral nende välistamiseks riigihangetes. Kuigi RHS võimaldab teatud juhtudel arvestada julgeolekuriskidega ning erinevates valdkondlikes õigusaktides käsitletakse tarneahela turvalisust, puuduvad ühtsed kriteeriumid, meetodika ja praktika, mille alusel hinnata konkreetsest tehnoloogiast, teenusest või tootjast tulenevat riski avalikule korrale ning julgeolekule.

Selle tulemusena sõltub riskiriikidega seotud tehnoloogia hanke käsitlemine suuresti üksiku hankija teadmistest, riskitaluvusest ja õigusnormide tõlgendamisest. Praktikast tähendab see, et samasuguse tehnoloogia suhtes võivad erinevad asutused teha erinevaid otsuseid. Osa hankijaid võib pidada konkreetset tehnoloogiat vastuvõetavaks, samal ajal kui teine asutus välistab sama tehnoloogilise lahenduse julgeolekuriskidele viidates. Selline ebaühtlane praktika vähendab ettevõtjate õigusselgust, suurendab hangete vaidluste riski ning võib viia olukorrani, kus strateegiliselt olulistest võrgu- ja infosüsteemides kasutatakse tehnoloogiat, millega seotud julgeolekuriskid on jäänud tuvastamata või mille võimalikku mõju ei ole vähese teadlikkuse või riskiteabe puudumise tõttu täielikult teadvustatud. Samuti võib hankijate erinev riskitaluvus kaasa tuua olukorra, kus samalaadseid julgeolekuriske käsitletakse asutustes erinevalt ning aktsepteeritakse riske, mida teise hankija puhul peetaks vastuvõetamatuks.

Riskiriikidega seotud tehnoloogia puhul tähendab vajadus piiranguid piisavalt põhjendada praktikast seda, et hankijal peab olema võimalik tugineda asjakohasele riskihinnangule ning näidata, milles seisneb tehnoloogia, tootja või teenusepakkujaga seotud risk ja milline võib olla selle mõju konkreetsele kasutuskeskonnale. Vajalik hinnang võib hõlmata lisaks tehnilistele riskidele ka tootja omandi- ja kontrollisuhteid, tarneahelat, andmete või süsteemidele ligipääsu võimalusi ning muid julgeolekuriske.

Seetõttu eeldab julgeolekuriskide arvestamine riigihangetes mitme valdkonna kompetentsi ja spetsialistide koostööd. Hankekorraldajatel ja tooteomanikel peab olema võimalik saada vajalikku sisendit infoturbe-, julgeoleku-, riskijuhtimise, andmekaitse ja õigusvaldkonna spetsialistidelt, kuna ühelt spetsialistilt ei saa eeldada kõigi geopoliitiliste, tehniliste, tarneahela- ja õiguslike riskide terviklikuks hindamiseks vajalikku pädevust. Praktikast ei ole selline valdkondade ülene kompetents kõigis asutustes ühtlaselt kättesaadav. Selle tulemusena sõltub riskide tuvastamise, hindamise ja maandamise võimekus suuresti konkreetse hankija

⁵ Artikkel 102-107 https://eur-lex.europa.eu/resource.html?uri=cellar:03aee288-f75c-11f0-b9bc-01aa75ed71a1.0021.02/DOC_1&format=PDF

⁶ [The EU toolbox for 5G security | Shaping Europe's digital future](#)

⁷ [Toolbox to improve ICT supply chain security | Shaping Europe's digital future](#)

olemasolevatest teadmistest ja ressurssidest ning asutuste riskijuhtimise kvaliteet võib oluliselt erineda.

Probleemi on kinnitanud ka varasemad riiklikud tegevused. RIA koostas riskiriikidest sõltuvuse vähendamiseks ettepanekud ja soovitused. Soovitused keskendusid riskihaldusele, infoturbemeetmetele, regulatiivsetele võimalustele ning tehnilistele kaitsemeetmetele. 2025. aasta juunis tehtud järelkontroll näitas, et mitmed soovitused olid jäänud rakendamata ning sõltuvus riskiriikide tehnoloogiast ei olnud soovitud ulatuses vähenenud, mis viitab sellele, et üksnes soovitustest ja juhendmaterjalidest ei piisa ning vajadus on selgemate õiguslike aluste ja ühtsemate rakenduspõhimõtete järele.

Senise olukorra kestmisel suureneb risk, et avaliku sektori asutustes kasutatakse jätkuvalt tehnoloogiaid, mille tarneahel või tootjariik võib kujutada endast julgeolekuohtu. See tähendab, et suurema riskiga tehnoloogia kasutamise tulemusel võib suurened küberintsidentide esinemine ning mõju, raskeneda kriisilukordades teenuste toimepidevuse tagamine ning süveneda strateegiline sõltuvus riikidest, kelle huvid ei pruugi kattuda Eesti ega EL julgeolekuhuvidega, aga ka olulise teabe, sealhulgas isikuandmete edasikandmine riskiriikidesse.

Lisaks eespool kirjeldatud julgeolekuohule jääb hankijatele õigusselgusetus, mis võib kaasa tuua rohkem vaidlusi riigihangetes ja erinevaid praktikaid samalaadsete riskide hindamisel.

Kokkuvõtteks seisneb probleem eelkõige selles, et kuigi riskiriikides pärineva tehnoloogia kasutamisega seotud julgeolekuriske teadvustatakse üha enam, puudub praegu piisavalt selge, ühtne ja praktiliselt rakendatav õigusnorm ja metoodika nende riskide ühtseks hindamiseks ning vajaduse korral konkreetsete tehnoloogiate välistamiseks või kasutamise piiramiseks. Selle tulemusena on hankijate praktika ebaühtlane, õiguskindlus on piiratud ning riigi julgeoleku seisukohalt oluliste tehnoloogiliste teenuste kvaliteet sõltub liigselt üksikute asutuste võimekusest ja õiguse tõlgendustest.

2. Eesmärgid

Eesmärk on luua Eestis ühtne õiguslik ja praktiline hankemenetluse raamistik riskiriikidega seotud tehnoloogia ja teenusepakkujate riskide hindamiseks ning vajaduse korral nende välistamiseks kriitilise taristu ja elutähtsate teenuste valdkonnas. Eesmärk on tagada, et julgeolekuriskidega seotud otsused oleksid läbipaistvad, põhjendatud ja õiguslikult kaitstavad ning et kriitilises taristus ei võetaks kasutusele tehnoloogiaid, mis võivad kujutada ohtu riigi julgeolekule, toimepidevusele või strateegilisele autonoomiale.

Eesmärgi saavutamiseks töötatakse välja selged otsustusloogikad, rakendusjuhised ja õiguslikud muudatused, mis võimaldavad hankijatel ning pädevatel asutustel arvestada julgeolekukaalutlusi tehnoloogiate ja teenusepakkujate valikul. Eelnõu ettevalmistamisele kaasatakse hankepartner, kelle ülesanne on analüüsida kehtiva õigusraamistiku võimalusi ja piiranguid ning teha ettepanekud õigusraamistiku täiendamiseks. Analüüsi üheks sisendiks on selles väljatöötamiskavatsuses (VTK) kirjeldatud probleemistik, eesmärgid ja lahendusvariandid ning VTK avaliku konsultatsiooni käigus saadud tagasiside. Hankepartneri töö tulemusi kasutatakse eelistatud lahenduse õiguslikuks täpsustamiseks ja RHSi muutmise eelnõu koostamiseks.

Eesmärgi saavutamist hinnatakse selle kaudu, kas valmivad rakendatavad juhised, otsustusmudelid ja õiguslikud alused, mis võimaldavad hankijatel ning kriitilise taristu ettevõtjatel riskiriikidega seotud tehnoloogiaid ühtsetel alustel hinnata. Samuti hinnatakse, kas loodud raamistik vähendab õiguslikku ebakindlust ning suurendab riigi võimekust maandada julgeolekuriske strateegiliselt oluliste tehnoloogiate kasutamisel.

- Toetab „Eesti 2035“ eesmärgi tagada turvaline, vastupidav ja hästi toimiv riik, mis suudab kaitsta oma julgeolekuhuve ning pakkuda usaldusväärseid avalikke teenuseid ka kiiresti muutuvus julgeoleku- ja tehnoloogiakeskkonnas. Eesti 2035 üheks aluspõhimõtteks on demokraatlik ja turvaline riik, mis põhineb õigusriigil ning on võimeline toime tulema nii sisemiste kui väliste riskidega. Riskiriikidega seotud tehnoloogiate kasutamisest tulenevate julgeolekuriskide parem hindamine ja maandamine aitab tugevdada kriitilise taristu ning elutähtsate teenuste toimepidevust, vähendada strateegilisi sõltuvusi ning suurendada riigi vastupanuvõimet.
- toetab ka „Eesti 2035“ eesmärki arendada usaldusväärset digiühiskonda, kus digitaalsete lahenduste kasutamine põhineb turvalisusel, töökindlusel ja ühiskonna usaldusel. Kriitilise taristu ja riigi jaoks oluliste teenuste puhul on oluline, et kasutatavad tehnoloogiad ei looks täiendavaid julgeoleku- ega sõltuvusriske. Seetõttu aitab algatus kaasa Eesti digiriigi pikaajalise usaldusväärse ja julgeoleku tagamisele ning toetab laiemalt riigi strateegilist eesmärki suurendada ühiskonna turvalisust ja vastupidavust.
- **Küberturvalisuse 2. direktiivi** eesmärkidega tugevdada kriitiliste ja oluliste üksuste küberturvalisust ning parandada tarneahela riskide juhtimist. Küberturvalisuse 2. direktiiv kohustab organisatsioone rakendama riskijuhtimismeetmeid, mis hõlmavad muu hulgas tarnijatest, teenusepakkujatest ja tarneahelatest tulenevate riskide hindamist. Riskiriikidega seotud tehnoloogiate ja teenusepakkujate hindamise ning vajadusel välistamise raamistik toetab nende nõuete rakendamist, aidates asutustel ja maandada julgeolekuriske, mis võivad mõjutada nende võrkude ja infosüsteemide turvalisust ning teenuste toimepidevust.
- Euroopa Liidu kriitiliste üksuste toimepidevuse direktiivi (**CER**) (2022/2557) eesmärkidega tugevdada kriitiliste üksuste vastupidavust ning vähendada riske, mis võivad mõjutada elutähtsate teenuste osutamist. Riskiriikidega seotud tehnoloogiate ja teenusepakkujate hindamise ning vajadusel välistamise raamistik aitab maandada kriitilise taristu toimepidevust mõjutavaid julgeolekuriske ning toetab seeläbi CER-direktiivist tulenevate eesmärkide saavutamist.
- Euroopa Liidu küberkerksuse määruse (**CRA**) (2024/2847) eesmärkidega suurendada digielementidega toodete küberturvalisust kogu nende elutsükli vältel ning tagada, et turule lastavad tooted vastaksid ühtsetele küberturbenõuetele. CRA näeb ette, et digielementidega toodete hankimisel tuleb arvesse võtta nende vastavust määruses sätestatud küberturbenõuetele, sealhulgas tootja võimekust haavatavusi tõhusalt hallata. Samuti võimaldab CRA liikmesriikidel kehtestada digielementidega toodete hankimiseks või kasutamiseks konkreetsetel eesmärkidel täiendavaid küberturbenõudeid, tingimusel et need on kooskõlas Euroopa Liidu õigusega ning vajalikud ja proportsionaalsed. Riskiriikidega seotud tehnoloogiate riskipõhine hindamine täiendab CRA-st tulenevaid tootepõhiseid küberturbenõudeid, võimaldades arvesse võtta ka tootja, teenusepakkuja, tarneahela ja muude mittetehniliste asjaoludega seotud julgeolekuriske.
- **Euroopa Liidu strateegiline tegevuskava 2024-2029** a. Euroopa Liidu majandusjulgeoleku ja strateegilise autonoomia eesmärgi, mille järgi tuleb vähendada kriitilisi sõltuvusi, tugevdada kriitilise taristu vastupidavust ning maandada kõrge riskiga tehnoloogiate ja teenusepakkujatega seotud julgeolekuriske.

- Panustab ka Vabariigi Valitsuse eesmärki tugevdada Eesti küberturvalisust ja kriitilise taristu kaitset.

Algatus on kooskõlas ka Euroopa Komisjoni 2026. aastal avaldatud riigihangete määruse ettepanekuga, mille eesmärk on muuta avalikud hanked senisest strateegilisemaks ning võimaldada suuremal määral arvestada julgeoleku-, vastupidavus- ja tarneahela kaalutlustega. Euroopa Parlamendi 2026. aasta analüüsi järgi ei peaks avalikud hanked lähtuma üksnes madalaimast hinnast, vaid toetama Euroopa majandusjulgeolekut, kriitiliste tarneahelate vastupidavust ning strateegiliste sõltuvuste vähendamist. Sellest tulenevalt nähakse riigihankeid üha enam strateegilise poliitikavahendina, mille kaudu saab tugevdada Euroopa julgeolekut ja vastupanuvõimet.

3. Võimalikud lahendused

Kirjeldatud probleemi lahendamiseks on võimalik kasutada nii regulatiivseid kui mitteregulatiivseid meetmeid. Lahendusvariantide puhul tuleb arvestada, et riskiriikidega seotud tehnoloogiate ja teenusepakujate kasutamine võib põhjustada riigi julgeoleku, kriitilise taristu toimepidevuse ja tarneahelate usaldusväärsusega seotud riske. Samal ajal võivad tehnoloogiate, tootjate või teenusepakujate kasutamise piirangud mõjutada ettevõtlusvabadust, konkurentsi, turulepääsu ja ettevõtjate võrdset kohtlemist.

Seetõttu peab lahendus võimaldama julgeolekuriske tõhusalt maandada, kuid olema samal ajal selge, proportsionaalne, läbipaistev ja kontrollitav. Riigihangete korraldamisel tuleb järgida ettevõtjate võrdse kohtlemise, diskrimineerimiskeelu, läbipaistvuse ja proportsionaalsuse põhimõtteid. Need põhimõtted tulenevad nii Euroopa Liidu aluslepingutest, riigihankeõigusest kui ka Eesti riigihangete seadusest.

Võimalik lahendus 1

Keelatud ja lubatud toodete või teenuste loetelu kehtestamine (nõ *black and white list*)

Ühe võimaliku regulatiivse lahendusena saaks kehtestada keelatud ja lubatud toodete või teenuste loetelud ehk nn musta ja valge nimekirja. Keelatud toodete või teenuste loetelusse kantud lahendusi ei oleks lubatud võtta kasutusele kindlaksmääratud valdkondades või teatud kasutusjuhtudel hankida. Lubatud toodete või teenuste loetelu annaks omakorda hankijale kinnituse, et loetellu kantud lahenduse suhtes on vajalik hindamine tehtud ning selle kasutamine on aktsepteeritav.

Kehtiv Euroopa Liidu riigihangete direktiiv 2014/24/EL ei näe ette üldist õiguslikku alust keelatud või lubatud toodete ja teenuste loetelude kehtestamiseks. Samas võimaldab direktiivi artikli 15 lõige 2 teha erandeid riigihangete reeglite kohaldamisest, kui see on vajalik liikmesriigi oluliste julgeolekuhuvide kaitseks ning neid huve ei ole võimalik tagada vähem piiravate meetmetega. Seega ei ole julgeolekukaalutlustel teatud tehnoloogiate või tarnijate kasutamise piiramine põhimõtteliselt välistatud, kuid selliste piirangute kehtestamiseks peab olema piisavalt selge riigisisene õiguslik alus ning tagatud kooskõla Euroopa Liidu õiguse ja proportsionaalsuse põhimõttega.

Loetelupõhise regulatsiooni võimalikkust toetavad ka Euroopa Komisjoni 2026. aastal esitatud õigusaktide ettepanekud. Euroopa Komisjoni 9. septembril 2026 avaldatud riigihangete määruse ettepaneku (COM(2026) 590) artiklis 66 nähakse ette võimalus arvestada hankemenetluses julgeolekuriskidega, sealhulgas tehnoloogia päritolu, tarnijate omandi- ja

kontrollstruktuuri ning kolmandatest riikidest tulenevate strateegiliste sõltuvustega. Artikli 66 lõige 5 näeb ette kõrge riskiga tarnijate kohustusliku kõrvaldamise teatud IKT-komponentidega seotud hangetest. Seejuures on vastavate tarnijate määratlemine seotud Euroopa Komisjoni küberturvalisuse määrase muutmise ettepanekuga (COM(2026) 11), mille artiklid 102–104 näevad ette kriitiliste IKT-varade määratlemise, kõrge riskiga tarnijate tuvastamise ja loetelude koostamise ning nende tarnijate komponentide kasutamise piiramise.

Nimetatud ettepanekud ei ole veel jõustunud ega anna iseseisvat õiguslikku alust riigisiseste loetelude kehtestamiseks, kuid näitavad Euroopa Liidu õigusraamistiku arengusuunda, milles julgeolekuriskide maandamiseks nähakse ette riskipõhiseid tarnijate ja tehnoloogiate kasutamise piiranguid.

Loetelupõhise lahenduse rakendamine eeldaks riigisiseses õiguses selgete hindamiskriteeriumide, otsustuspädevuse, loetelude koostamise ja ajakohastamise korra ning vaidlustamisvõimaluste sätestamist. Seejuures tuleks tagada, et piirangud oleksid põhjendatud, proportsionaalsed ning seotud konkreetsete julgeolekuriskidega. Eraldi tuleks hinnata lubatud toodete ja teenuste loetelu õiguslikku tähendust, kuna lahenduse eelnev positiivne riskihinnang ei pruugi välistada täiendavate riskide tekkimist või vajadust hinnata selle sobivust konkreetsetes kasutuskeskonnas.

Positiivne mõju

Lahenduse peamine eelis on selle selgus ja lihtne rakendatavus. Hankijal oleks võimalik loetelust lähtudes kiiresti kindlaks teha, kas konkreetse toote või teenuse kasutamine on lubatud või keelatud. See vähendaks üksikute hankijate analüüsikoormust, ühtlustaks praktikat ning aitaks vältida olukordi, kus erinevad asutused jõuavad sama tehnoloogia suhtes erinevatele järeldustele.

Keelatud toodete või teenuste loetelu annaks hankijale selgema aluse pakkumuse tagasilükkamiseks või hanketingimustes konkreetse lahenduse välistamiseks. Ühtlasi suureneks otsuste prognoositavus ning hankijad ei peaks iga hanke puhul iseseisvalt tegema täielikku tehnilist, õiguslikku ja geopoliitilist riskide hindamist.

Negatiivne mõju

Loetelupõhise lahenduse rakendamine eeldaks keskse ja püsiva hindamisvõimekuse loomist. Vajalik oleks määrata asutus, kes jälgiks tehnoloogiate arengut, koguvad julgeolekuinfot, hindavad tooteid ja teenuseid ning ajakohastavad seejärel loetelusid. Kuna tehnoloogiad, omandisuhted, tarneahelad ja turvaomadused muutuvad kiiresti, peaks hindamine olema järjepidev.

Staatiline loetelu võib kiiresti vananeda. Keelatud toodete või teenuste loetellu võib jääda toode või teenus, mille puhul on varasemad riskid kõrvaldatud või mille kasutamiseks on välja töötatud piisavad maandamismeetmed, kuid mida ei ole veel uuesti hinnatud. Samal ajal võib loetelus püsida toode või teenus, mille suhtes on pärast loetellu lisamist ilmnunud riske, mida ei ole jõutud hinnata.

Lubatud toodete või teenuste loetelu võib hakata kaudselt piirama selliste uute lahenduste kasutamist, mida ei ole ressursipuuduse või hindamise järjekorra tõttu veel loetellu lisatud. See võib kahjustada innovatsiooni, vähendada turule sisenevate ettevõtjate võimalusi ning soodustada juba turul tegutsevaid suuri ettevõtjaid.

Lisaks ei arvesta üldine toote- või teenusepõhine loetelu piisavalt konkreetset kasutuskeskonda. Sama tehnoloogia risk võib olla väga erinev sõltuvalt sellest, kas seda kasutatakse tavapärasel arvutitöökohas, avalikus veebiteenuses, elutähtsa teenuse juhtimises või mõnes kriitilises sidevõrgus. Jäik loetelu ei pruugi piisavalt arvestada, et sama tehnoloogia

riskitase võib erinevates kasutuskeskkondades olla erinev. Näiteks võib tehnoloogia kasutamisega seotud riski vähendada võrgu segmenteerimise, keskhalduse, ligipääsupiirangute, andmete lokaliseerimisega.

Lahendus võib oluliselt mõjutada konkurentsi ja ettevõtlusvabadust, eriti juhul kui loetellu kandmise kriteeriumid või menetlusviis ei ole piisavalt selged ja läbipaistvad. Seetõttu peaks ettevõtjal olema võimalik saada teavet loetellu kandmise põhjuste kohta, esitada omapoolseid selgitusi ning taotleda otsuse uuesti hindamist.

Võimalik lahendus 2

a) Riskiriikide, tootjate või teenuseosutajate loetelu kehtestamine

Riskiriikide loetelus määratakse riigid, millega seotud tehnoloogiate või teenuste soetamisel tuleb rakendada piiranguid, täiendavat riskihindamist või välistamist

Positiivne mõju

Riskiriikide loetelu annaks hankijale selge lähtekoha, milliste riikidega seotud tehnoloogiate või teenusepakkujate puhul tuleb rakendada kõrgendatud tähelepanu. See vähendaks hankijate vajadust iseseisvalt hinnata iga riigi poliitilist ja õiguslikku keskkonda ning aitaks ühtlustada geopoliitiliste riskide käsitlemist.

Negatiivne mõju

Riigipõhine lähenemine võib olla liiga üldistav. Ühes riigis toodetud tooted või seal asutatud ettevõtjad ei ole tingimata võrdselt riskantsed ning konkreetse lahenduse risk sõltub ka selle tehnilistest omadustest, kasutusotstarbest, andmete ligipääsust ja rakendatud turvameetmetest.

Samuti võib olla keeruline määratleda tehnoloogia tegelikku päritoluriiki. Toode võib olla projekteeritud ühes riigis, selle komponendid võivad pärineda mitmest teisest riigist ning tootmine võib toimuda kolmandas riigis ja lõplik kokkupanek neljandas riigis. Toodet turule tuua või teenust võib pakkuda ka ELs registreeritud ettevõtja, kuid selle emaettevõtja võib paikneda riskiriigis.

Tootja või teenusepakkuja võib viia tootmise või teenuse osutamise formaalselt teise riiki, muutmata tegelikku kontrolli, juhtimist, tarneahelat ega julgeolekuriski. Seetõttu ei pruugi üksnes tootmis- või teenuse osutamise riigist lähtumine anda piisavat alust tehnoloogia või teenuse tegeliku julgeolekuriski hindamiseks.

b) Loetelu tootjatest või teenuseosutajatest, kelle toodete või teenuste soetamine ei ole julgeolekuriske arvestades soovitatav

Selle lahenduse puhul koostatakse loetelu konkreetsetest tootjatest või teenuseosutajatest, kelle toodete või teenuste kasutamist peetakse julgeolekuriski tõttu ebaturvaliseks või lubamatuks.

Positiivne mõju

Tootja või teenuseosutaja põhine lähenemine oleks riigipõhisest loetelust täpsem, sest piirang ei laieneks automaatselt kõigele konkreetsetes riigis tegutsevatele ettevõtjatele. Otsus oleks võimalik siduda konkreetse ettevõtja omandisuhete, juhtimise, riikliku mõjutatavuse, varasema tegevuse või toodete ja teenustega seotud riskidega.

Hankijal oleks loetelust lähtudes võimalik teha selgem ja kiiremini põhjendatav otsus vastava pakkumuse või tehnoloogia välistamiseks.

Negatiivne mõju

Ettevõtja või tootjapõhisest piirangust võib olla võimalik mööda minna uute juriidiliste isikute, tütarettevõtjate, vahendajate või kaubamärkide loomise kaudu. Teenuse osutamiseks või toodete turustamiseks võib kasutada mitmekordseid omandiahelaid või variettevõtteid, mille tõttu on tegeliku kontrolli ja kasusaajate kindlakstegemine raskendatud.

Samuti võib toode sisaldada riskantse tootja komponente, kuigi lõpptoote müüja või kaubamärgi omanik ise loetellu ei kuulu. Keerukate rahvusvaheliste tarneahelate puhul võib tegeliku tootja, arendaja, hooldaja või andmetele ligipääsu omava isiku tuvastamine nõuda põhjalikku analüüsi.

Võimalik lahendus 3

Riigihanke protsessi muudatus, mis võimaldaks ühtsetel alustel kasutada info- ja kommunikatsioonitehnoloogiaga (IKT) seotud hangetes asutuse riskihinnagut ja seeläbi välistada riskiriikide IKT-tooteid ja -teenuseid.

Eesmärk on tagada IKT-toodete ja -teenuste riigihangete korraldamise kooskõla asutuses juba rakendatava infoturbe riskijuhtimisega. Küberturvalisuse seadus (KüTS) kohustab selle kohaldamisalasse kuuluvaid üksusi hindama ja juhtima võrgu- ja infosüsteemide turvalisusega seotud riske, sealhulgas rakendama asjakohaseid meetmeid tuvastatud riskide maandamiseks. Seetõttu on oluline tagada, et hankijal oleks ka riigihangete korraldamisel selge õiguslik võimalus arvestada KüTS-i alusel tehtud riskihinnangute tulemusi ning lähtuda neist IKT-toodete ja -teenuste hankimisega seotud otsuste tegemisel.

Selle lahenduse juurde jäämisel täiendatakse RHSi viisil, mis võimaldab hankijal riigihankest kõrvaldada riskiriigi päritolu IKT-toote- või -teenuse pakkuja, mille toote või teenuse hankimisega võib kaasneda risk hankija võrgu- ja infosüsteemi toimepidevusele ja see kaudu kaasneda oluline mõju avalikule korrale ning julgeolekule. Lahenduse puhul ei loodaks riigihangete jaoks eraldiseisvat riskihindamise süsteemi. Hankija lähtuks eelkõige Eesti infoturbestandardi (E-ITS) või muu talle kohalduva infoturbe riskijuhtimise raames tehtud riskihinnangust. Kui asutus on oma võrgu- ja infosüsteemi, teenuse või vara suhtes juba hinnanud konkreetse IKT-toote, -teenuse või teenusepakkujaga seotud riski ning tuvastanud, et selle kasutamine põhjustaks riske asutusele, saaks sama riskihinnangut kasutada ka vastava IKT-toote või -teenuse hankimisel.

RHSi muudatusega antaks hankijale selge võimalus võtta sellist riskihinnangut arvesse kogu hankemenetluse vältel, alates hanke kavandamisest kuni hankelepingu täitmiseni. Riskihinnangu tulemusi oleks võimalik kasutada hanketingimuste kujundamisel, sealhulgas tehnilise kirjelduse, kvalifitseerimistingimuste ja hankelepingu täitmise tingimuste kehtestamisel, samuti pakkuja kõrvaldamise, pakkumuse vastavuse hindamise ja pakkumuse tagasilükkamisega seotud otsuste tegemisel, kui selleks on seaduses asjakohane õiguslik alus. Muudatuse eesmärk võimaldab hankijal järjepidevalt arvestada juba tuvastatud riskidega ning vajaduse korral välistada vastuvõetamatu riskiga IKT-toote või -teenuse hankimine või kasutamine. Sellega saaks vältida olukorda, kus asutus on riskijuhtimise käigus juba tuvastanud tehnoloogia kasutamisega seotud vastuvõetamatu riski, kuid riigihanke tegemisel peab sama riski eraldiseisvalt uuesti hindama ja põhjendama. Varasemat riskihinnangut saaks kasutada

ulatuses, milles see on ajakohane ja konkreetse hanke seisukohast vajalik, tagades see juures tehtavate otsuste põhjendatuse, proportsionaalsuse ja kooskõla riigihangete üldpõhimõtetega.

Positiivne mõju

Tekib täiendav meede, mida kasutada IKT-toote- või -teenuse hankemenetluses. Tekib seos asutuse infoturbe riskijuhtimise ja riigihanke protsessi vahel ning vähendab dubleerivat tööd. Hankija ei pea koostama riigihanke jaoks eraldiseisvat riskianalüüsi juhul, kui sama risk on riskijuhtimise raames juba hinnatud.

Lahendus annab riskihinnangule selgema praktilise väljundi. Kui hankija on varasemalt tuvastanud, et teatud tehnoloogia kasutamine kriitilises süsteemis tekitab riske, saab seda hinnangut arvestada juba tehnoloogia hankimisel, mitte alles pärast selle hankimist.

Ühtne protsess parandab koostööd tooteomaniku, infoturbejuhi ja hankespetsialisti vahel. Tooteomanik ja infoturbejuht vastutavad sisulise riski tuvastamise ja käsitlemise eest ning hankespetsialist saab kasutada selle tulemust hankemenetluse tingimuste ja otsuste kujundamisel.

Lahendus võimaldab säilitada riskipõhise lähenemise. Konkreetset tehnoloogiat või teenusepakkujat ei välistata automaatselt tema päritolu tõttu, vaid hinnatakse, millist riski IKT-toote või -teenuse kasutamine konkreetsetes võrgu- või infosüsteemis põhjustab ning kas seda riski on võimalik piisavalt maandada. Seejuures arvesse ei võeta vaid tehnilisi riske vaid ka muid riske, mis tulenevad tootjast või teenusepakkujast endast.

Negatiivne mõju

Lahenduse rakendamine eeldab riigihangete ja infoturbe protsesside senisest tihedamat sidumist ning asutusesiseste rollide ja vastutuse selget määratlemist. Hankemenetluse protsessi tuleb vajaduse korral kaasata infoturbe eest vastutavad juba enne hanketingimuste koostamist. Samuti tuleb kehtestada miinimumnõuded sellele, millal saab olemasolevat riskihinnangut pidada hankemenetluses kasutamiseks piisavaks ja ajakohaseks. Liiga üldine või konkreetse hanke esemega mitteseotud riskihinnang ei saa automaatselt olla ettevõtja või pakkumuse välistamise aluseks.

Üleminekuperioodil võib suureneda hankespetsialistide, tooteomanike ja infoturbejuhtide töökoormus, sest tuleb kujundada ühine rakenduspraktika ning töötada välja juhendid riskihinnangu tulemuste hankemenetlusse ülekandmiseks.

Õiguslikult on vaja selgelt määratleda, millise hankemenetluse otsuse tegemiseks riskihinnangut kasutatakse.

Võimalik lahendus 4

Olemasoleva ja tulevase regulatsiooni jätkuva rakendamine ja mitteregulatiivsed meetmed

Selle lahenduse juurde jäämisel ei kehtestataks uusi riigisiseseid õiguslikke aluseid, kohustuslikke hindamiskriteeriume ega keskseid otsustusmudeleid. Hankijad ja kriitilise taristu ettevõtjad jätkaksid riskide hindamist kehtiva riigihangete seaduse, küberturvalisuse nõuete, asutusesiseste riskihaldusreeglite ja üldiste infoturbepõhimõtete järgi.

Positiivne mõju

Lahendusega ei kaasneks riigile vahetuid õigusloome ega ka rakenduskulusid ning puuduks vajadus luua kesksel hindamisstruktuuri. Samuti ei seataks ettevõtjatele uusi turule pääsu piiranguid ning ei suurendataks hankijate halduskoormust.

Hankijatel säilib paindlikkus hinnata iga tehnoloogiat ja teenust vastavalt oma teenustele, kasutusotstarbele ja riskitaluvusele.

Negatiivne mõju

Sekkumata jätmine ei lahendaks kirjeldatud probleeme. Hankijatel puuduksid jätkuvalt piisavalt selged ja ühtsed õiguslikud alused riskiriikidega seotud tehnoloogiate hindamiseks ja välistamiseks. Praktika sõltuks endiselt konkreetse asutuse kompetentsist, ressurssidest ja riskitaluvusest.

Asutused peaksid jätkuvalt ise koguma teavet tootjate, teenusepakkujate, omandisuhete, tarneahelate ja geopoliitiliste riskide kohta. See tooks kaasa dubleeriva töökorralduse ning olukorra, kus sama tehnoloogia suhtes koostatakse eri asutustes eraldi analüüse, mis võivad jõuda erinevate tulemusteni.

Kehvema infoturbe- või õigusvõimekusega hankijad võivad julgeolekuriskide käsitlemisest loobuda, kasutada üksnes tavapäraseid tehnilisi nõudeid või valida majanduslikult soodsaima lahenduse ka juhul, kui sellega kaasneb strateegiline või pikaajaline risk.

Säilib risk, et kriitilises taristus ja elutähtsate teenuste osutamisel võetakse kasutusele tehnoloogiaid mille tarneahela, tootja kontrolli või andmetele ligipääsuga seotud riske ei ole piisavalt hinnatud. Samuti säilib õiguslik ebakindlus, sest hankijad ei pruugi olla kindlad, millises ulatuses saab geopoliitilisi või riigi julgeolekuga seotud kaalutlusi kasutada pakkumuste tagasilükkamiseks või hanketingimuste kehtestamiseks.

4. Uuringud ja kaasatud osapooled

VTK koostamisel on tuginetud Justiits- ja Digiministeeriumi senistele analüüsidele ning riigis tehtud riskihinnangutele, mis käsitlevad riskiriikidega seotud tehnoloogiate kasutamist avalikus sektoris ja kriitilises taristus.

Oluliseks sisendiks on olnud RIA 2023. aastal Vabariigi Valitsuse kabinetinõupidamisel esitatud ülevaade ühe võimaliku riskiriigi näitel esitatud valitsussektori sõltuvuste vähendamisest riskiriigis toodetud, arendatud või kontrolli all olevast tehnoloogiast. Ülevaates tehti ettepanekud riskijuhtimise, infoturbe, hangete ning tehniliste meetmete tugevdamiseks. 2025. aasta juunis tehtud soovitude täitmise järelkontroll näitas, et mitmed soovitatud meetmed on jäänud rakendamata ning riskiriikidega seotud tehnoloogiate kasutamise vähendamine ei ole toimunud soovitud ulatuses.

VTK koostamisel on arvestatud ka kehtiva õigusraamistiku analüüsiga. Senine analüüs näitab, et kuigi RHS ja muud julgeolekut käsitlevad õigusaktid võimaldavad teatud juhtudel arvestada julgeoleku- ja tarneahelariskidega, puuduvad hankijatel ühtsed, selged, õiguslikud alused riskiriikidega seotud tehnoloogiate tuvastamiseks, hindamiseks ja vajaduse korral välistamiseks. Praktikas sõltub riskide kaalutlemisest suuresti konkreetse hankija kompetentsist, riskitaluvusest ning olemasolevate õigusnormide tõlgendamisest.

Probleemi paremaks mõistmiseks on Justiits- ja Digiministeerium kaardistanud⁸ olemasolevad võimalused riskiriikidega seotud tehnoloogiariskide maandamiseks riigihangetes. Kaardistuse tulemusena tuvastati kuus peamist õiguslikku ja korralduslikku meetet, sealhulgas tehnilise kirjelduse kujundamine, tootjapõhiste riskianalüüside koostamine, julgeolekuasutuste kaasamine, olemasolevate juhendmaterjalide kasutamine ning riigihangete seaduses sätestatud julgeolekuuerandi kohaldamine. Analüüs näitas siiski, et ükski olemasolev meede ei paku hankijatele piisavalt ühtset ja õiguslikult kindlat alust riskiriikidega seotud tehnoloogiate välistamiseks kõikides olukordades.

Nimetatud järeldustest lähtudes on Justiits- ja Digiministeerium algatanud analüüsi „Riskiriikide tehnoloogiate kasutamise piiramine ja välistamine“, mille eesmärk on hinnata olemasolevate õiguslike ja korralduslike meetmete piisavust, töötada välja praktilised soovitusel riskiriikidega seotud tehnoloogiate tuvastamiseks, hindamiseks ja välistamiseks ning vajaduse korral teha ettepanekud õigusraamistiku täiendamiseks.

VTK ettevalmistamisel on tehtud koostööd riigiasutustega ning arvestatud RaM RHS muutmise ettevalmistustega ning Euroopa Komisjoni tehtud riigihankedirektiivide ettepanekutega. VTK avalikustamise järgsel kaasatakse täiendavalt ministeeriumid, riigiasutused, ettevõtjad, ettevõtlusorganisatsioonid ning teised asjaomased huvirühmad, et hinnata kavandatavate lahenduste rakendatavust ja mõju ning koguda sisendit eelnõu koostamiseks.

5. Mõju

Mõjuvaldkond - majanduslikud mõjud (mõju ettevõtlusele)

Muudatus mõjutab eelkõige kriitilise IKT-taristu riigihangetes osalevaid ettevõtjaid. Positiivse mõjuna suureneb riigihangete läbipaistvus ja õigusselgus, kuna hankijatele tekivad ühtsemad alused julgeolekuriskide hindamiseks. See vähendab olukordi, kui erinevad hankijad käsitlevad samalaadseid riske erinevalt või kehtestavad erinevaid nõudeid. Selgemad reeglid muudavad hanketingimused ettevõtjatele prognoositavamaks ja vähendavad õigusvaidluste võimalust.

Mõju võib avalduda ettevõtjatele, kelle tooted või teenused on seotud kõrgendatud julgeolekuriskiga või kelle tarneahelad sõltuvad riskiriikidest. Sellistel ettevõtjatel võib tekkida vajadus tõendada oma tarneahela turvalisust, omandistruktuuri või esitada tõendeid riskimaandamismeetmete kohta. Samas ei ole kavandatava regulatsiooni eesmärk piirata konkurentsi ega välistada ettevõtteid nende päritolu tõttu, vaid võimaldada julgeolekuriskide objektiivset ja riskipõhist hindamist.

Kuna muudatus puudutab peamiselt riigihankeid kriitiliste taristu ja elutähtsate teenuste valdkonnas ning muudatus puudutab väljaspool Eestit tehtud tooteid, tehnoloogiad või teenuseid, ei ole mõju enamikele Eesti ettevõtjatele ulatuslik.

Mõjuvaldkond - riigivalitsemine (mõju keskvalitsuse korraldusele)

Kavandatav muudatus avaldab positiivset mõju keksvalitsuse töökorraldusele, kuna loob ühtsemad alused julgeolekuriskide arvestamiseks riigihangetes.

⁸ Lisa 1 _tarneahela arvestamine IKT riigihangetes

Selgem õiguslik raamistik vähendab vajadust, et iga riigiasutus töötaks iseseisvalt välja riskihindamise meetodikaid või telliks eraldiseisvaid õiguslikke analüüse. See aitab vähendada dubleerivat tööd ning suurendab riigiasutuste vahelist ühtset praktikat.

Rakendamise algfaasis võib suureneda töökoormus ministeeriumitel ja pädevatel asutustel, kes peavad välja töötama juhendmaterjalid, koolitused ja rakenduspraktika. Pikemas perspektiivis aitab muudatus teha otsustusprotsessid ühtlasemaks, läbipaistvamaks ja õiguslikult kindlamaks. Samuti väheneb ka võimalus, et IKT kaudu saab väline isik mõjutada avaliku sektori toimimist, avalikku korda ning üldist turvatunnet.

Mõjuvaldkond – infotehnoloogia ja infoühiskond (mõju e-riigile)

Kavandatav muudatus toetab Eesti e-riigi usaldusväarsust ja toimepidevust, vähendades riski, et riigi võrgu- ja infosüsteemides või kriitilise taristu teenuste pakkumisel kasutatakse tehnoloogiaid, mille kasutamisega võivad kaasnedä kõrgendatud julgeoleku- või tarneahelariskid.

Muudatus ei eelda uute riiklike infosüsteemide loomist ega ulatuslikke IT-arendusi. Vajaduse korral tuleb täiendada olemasolevaid juhendmaterjale ja hankemenetluse dokumentatsiooni ning töötada välja praktilised juhised riskihinnangu tulemuste kasutamiseks hankemenetluses. Samuti on oluline tõsta hankijate, tooteomanike, infoturbe eest vastutavate isikute ja teiste protsessi kaasatud osapoolte teadlikkust ning tagada neile vajalikud teadmised ja oskused juhendmaterjalide ühetaoliseks rakendamiseks. See aitab vältida olukorda, kus loodud võimalust rakendatakse asutustes erinevalt või jäetakse see vajalike teadmiste puudumise tõttu kasutamata.

Pikaajaliselt aitab muudatus suurendada riigi infosüsteemide hukukindlust ja küberturvalisust ja toetab Eesti e-riigi usaldusväarsust nii siseriiklikult kui ka rahvusvaheliselt.

Mõjuvaldkond – infotehnoloogia ja infoühiskond (mõju küberkeskkonnale ja küberhügieen)

Kavandataval muudatusel on positiivne mõju Eesti küberkeskkonna turvalisusele.

Selgemad alused võimaldavad hankijatel senisest süsteemsemalt hinnata tehnoloogiate, teenusepakkujate ja tarneahelaga seotud küberturvalisuse riske juba hankemenetluse käigus. See vähendab tõenäosust, et kriitilise taristu või elutähtsate teenuste osutamisel võetakse kasutusele tehnoloogiaid, mille puhul esineb kõrgendatud oht andmete konfidentsiaalsusele, süsteemide terviklusele, teabe autentsusele või teenuse käideldavusele.

Lisaks soodustab muudatus organisatsioonides riskihindamise, infoturbe ja tarneahela turvalisuse alase pädevuse kasvu ja toetab küberturvalisuse 2. direktiivis sätestatud riskipõhise küberturvalisuse põhimõtete rakendamist. Pikaajaliselt aitab see tugevdada Eesti kübervastupanuvõimet ja vähendada strateegilisi sõltuvusi kõrgendatud riskiga tehnoloogiatest ning riikidest.

Eelistatud lahendusena toetab Justiits- ja Digiministeerium välja pakutud võimalikku lahendust nr 3, kuna see võimaldab siduda riigihanke protsessi olemasoleva infoturbe riskijuhtimisega, loomata hankijatele eraldiseisvat ja dubleerivat riskihindamise kohustust. Lahendus annab hankijale selge õigusliku aluse juba tehtud riskihinnangu kasutamiseks hankemenetluses (nt pakkumise koostamisel) ning vajaduse korral riskiga seotud IKT-toote, -teenuse mittevastavaks

tunnistamiseks või pakkuja kõrvaldamiseks. Võrreldes loetelupõhiste lahendustega võimaldab see arvestada konkreetse kasutusjuhtumi, süsteemi kriitilisuse ja tegeliku riskiga ning hinnata ka riski maandamise võimalusi.

6. Edasine väljatöötamine

VTK avalikustamise käigus saavad huvitatud osapooled esitada seisukohti ja ettepanekuid kavandatavate lahenduste kohta. Laekunud tagasiside põhjal hinnatakse lahendusvariantide sobivust ja rakendatavust ning vajaduse korral täpsustatakse kavandatava seadusemuudatuse lähtekohti.

Saadud tagasiside põhjal koostatakse vajadusel seaduseelnõu ning korraldatakse lahendile täiendavate hinnangute tegemine. Selle käigus hinnatakse kavandatavate muudatuste kooskõla Euroopa Liidu õigusega, sealhulgas riigihangete, siseturu ja konkurentsi käsitlevate õigusnormide ja Euroopa kohtu praktikaga.

Eelneva alusel koostatakse seaduseelnõu, mis on kavandatud esitada kooskõlastamiseks ja avalikuks konsultatsiooniks veel 2026. aastal.

Kavandatava muudatuse jõustumine on eelduslikult 1. juuli 2027. Selline ajakava võimaldab riigiasutustel, kriitiliste taristu ettevõtjatel ja teistel osapooltel valmistuda uute nõuete rakendamiseks ning töötada välja vajalikud juhendmaterjalid ja rakendusmeetmed.

Avaliku konsultatsiooni käigus oodatakse tagasisidet eelkõige järgmiste küsimuste kohta:

- kas VTK-s kirjeldatud probleemipüstitus ja eesmärgid on asjakohased;
- kas kavandatavad lahendused võimaldavad saavutada soovitud eesmärki ning kas esineb alternatiivseid lahendusvõimalusi;
- millised võivad olla kavandatavate muudatuste mõjud riigihangete korraldajatele, pakkujatele ja teistele asjaomastele osapooltele;
- kas kavandatav regulatsioon on Euroopa Liidu õigusega kooskõlas ning kas selle rakendamisel võib tekkida täiendavaid õiguslikke või praktilisi probleeme.

Vastutav ministeerium

Justiits- ja Digiministeerium

Vastutavate ametnike nimed ja kontaktandmed

Guido Pääsuke - digitaristu ja küberturvalisuse osakonna riikliku küberturvalisuse talituse küberturvalisuse õigusnõunik (riiklikkyber@justdigi.ee);

Kristina Kivisild - digitaristu ja küberturvalisuse osakonna riikliku küberturvalisuse talituse küberturvalisuse tehnoloogia nõunik (riiklikkyber@justdigi.ee);

Lisa: Tarneahela arvestamine IKT riigihangetes