JUSTIITS- JA DIGIMINISTEERIUM

Rahandusministeerium
Majandus- ja Kommunikatsiooniministeerium
Siseministeerium
Kultuuriministeerium
Haridus- ja Teadusministeerium
Välisministeerium

Teie 30.07.2025 nr 2-5/25-01425-1, 6.1.1/25-0429/-2T
Meie 17.09.2025 nr 7-1/6463

Seisukohad MFF 2028-2034 perioodiks

Esitame Justiits- ja Digiministeeriumi seisukohad Euroopa Komisjoni ettepanekutele Euroopa Liidu 2028.-2034. aasta pikaajalise eelarve kohta:

1. Peame oluliseks, et mitmeaastane finantsraamistik ja väljapakutud fondid **toetaksid Euroopa Liidu peamiste digivaldkonna strateegiate** – sealhulgas Euroopa digikümnendi, EL küberturvalisuse strateegia, kvantstrateegia ja EL tehisintellekti strateegia – **elluviimist**. Nende strateegiate läbiv rakendamine aitab tagada, et Euroopa Liit suudab kiirendada digitaalset üleminekut, tugevdada konkurentsivõimet ja innovatsioonivõimekust, kaitsta oma kodanikke ja taristut küberturvalisuse ohtude eest ning rakendada usaldusväärseid ja turvalisi tehisintellekti lahendusi. Digivaldkonna sihipärane rahastamine toetab samal ajal rohepöörde eesmärkide saavutamist ning aitab väiksematel liikmesriikidel, nagu Eesti, kasutada oma piiratud ressursse maksimaalselt tõhusalt. Samas tuleb rõhutada, et nende eesmärkide elluviimine ning välissõltuvuste vähendamine – alates turvalise taristu arendamisest ja küberturvalisuse tugevdamisest kuni tehisintellekti rakendusteni – eeldab püsivat rahastust ja märkimisväärseid investeeringuid.
2. Prioritiseerime uue perioodi Euroopa Liidu mitmeaastases finantsraamistikus (MFF 2028-2034) erinevaid digiühiskonna vajadusi, millel on suur Euroopa Liidu lisandväärtus, tuginedes EL ja Eesti strateegiatele, arengusuundadele ja kokkulepetele õiguskaitse valdkonnas ning prioriteetidele. Need on järgmised:

    2.1. **Euroopa ja Eesti pilve- ja andmeruumide arendamine.** Ühtsed ja turvalised andmeruumid vähendavad killustatust, toetavad teadust, innovatsiooni ja ettevõtlust ning suurendavad Euroopa strateegilist autonoomiat. Eestis on tugev alus X-tee ja e-riigi lahendustega, kuid vaja on arendada piiriüleseid ühendusi, arendada pilve- ja kvanttehnoloogiaid jne.

    2.2. **Turvaliste sidevõrkude arendamine.** Turvalised ja töökindlad sidevõrgud on alus küberjulgeolekule, digiteenustele ja innovatsioonile, eriti geopoliitiliste pingete taustal. Eestis on vaja panustada järgmise põlvkonna (5G/6G) võrkude turvalisusse ning tagada kriitilise taristu kaitse, et vältida riske ja hoida usaldust nii riigi kui ettevõtete teenuste vastu.

Suur-Ameerika 1 / 10122 Tallinn / +372 620 8100 / info@justdigi.ee/ www.justdigi.ee
Registrikood 70000898

2.3. **Protsessorite ja kiipide tootmine.** Euroopa sõltumatus väljastpoolt tulenevatest tarneahelatest on hädavajalik. Eestisse tuleb luua tootmisvõimekus või vähemalt panustada targa spetsialiseerumise kaudu – näiteks kiipide testimise, disaini ja arenduse tugiteenuste pakkumise ning osalemise rahvusvahelistes tarneahelates. See roll haakub laiemalt Euroopa ja Eesti digitehnoloogia arendamise prioriteetidega (vt järgmist punkti).

2.4. **Euroopa ja Eesti digitehnoloogia ja tööriistade arendamine, sh tehisaru mudelid ja tehisaru gigatehased.** Euroopa vajab tipptasemel digitaristut ja tööriistu, mis lähtuvad Euroopa väärtustest ja regulatsioonidest ning vähendavad sõltuvust kolmandatest riikidest. Selle saavutamiseks tuleb rajada nn tehisaru gigatehased – ulatuslikud ja energiatõhusad arvutustaristu keskused, mis ühendavad andmekeskused, tippriistvara ja spetsialiseeritud platvormid alusmudelite treenimiseks. Eesti peab selles protsessis võtma proaktiivse rolli, pakkudes oma digiriigi kogemust potentsiaalseks Euroopa tehisaru taristu sõlmpunktiks. Samal ajal tuleb panustada väiksemate keeleressursside ja kohalike andmemudelite arendamisse, et tagada eesti keele ja kultuuri nähtavus digitaalses ökosüsteemis ning pakkuda lahendusi, mis võivad saada eeskujuks kogu Euroopa Liidule.

2.5. **Tehisaru laialdane kasutuselevõtt ja ökosüsteemi arendamine (platvormid, standardid, koolitus).** Eesti peab panustama mitte ainult tehisaru lahenduste kasutuselevõttu, vaid ka nende rakendamise standardite, platvormide ja koolitusmudelite kujundamisse Euroopa Liidu tasandil. Juhtiva positsiooni saavutamine tähendab, et Eesti edendab tehisaru kasutust avalike teenuste pakkumisel, sh justiitssüsteemis, et need lahendused võiksid saada eeskujuks teistele liikmesriikidele. Samal ajal tuleb toetada ettevõtteid tehisaru lahenduste praktilisel rakendamisel, et Eesti toimiks innovatsioonilaborina, kus uued lahendused seotakse Euroopa digitaalse ökosüsteemiga ja kus arendatav taristu – sealhulgas gigatehased – pakuvad tuge kogu kontinendile.

2.6. **Õiguskaare digitaliseerimine.** Justiitssüsteem peab olema inimestele digitaalselt kättesaadav ja arusaadav, tagatud peab olema läbipaistev ja kaasav õigusloome protsess ning kiired ja õiglased kohtumenetlused, sh digitaalne õigusemõistmine. Oluline on tagada ettevõtluskeskkonna efektiivsus ja usaldusväärsus, tagada tugev konkurentsiõiguse rikkumise vastane võitlus ja madalat halduskoormust tagavad digitaalsed teenused. Ettevõtja peab saama oma kohustusi riigi ees täita riigile ühekordselt andmeid edastades. Tõhus justiitssüsteem kasutab ja pakub masintöödeldavaid andmeid, kasutab tehisintellekti abilisena ja suurendab partnerite vahel (piiriüleselt) andmete vahetamist.

2.7. **Idufirmade ja ülikoolide koostöö.** Teaduse ja ettevõtluse sidumine kiirendab innovatsiooni ja uute lahenduste turule jõudmist. Eesti huvi on rohkem toetada ülikoolide ja idufirmade ühiseid projekte, luua katsekeskkondi ning arendada mehhanisme, mis aitavad teadusest sündinud ideedel jõuda rahvusvahelistele turgudele.

2.8. **Digiharidus ja digiekspertsuse kasvatamine.** Digihariduse ja spetsiifilisemate pädevuste kasvatamine on strateegiliselt keskne prioriteet, sest ilma vajalike oskusteta ei ole võimalik arendada ega rakendada uusi tehnoloogiaid ega maandada nendega kaasnevaid riske. Haridussüsteem peab tagama nii tippspetsialistide ettevalmistamise – näiteks tehisintellekti insenerid, küberkaitse eksperdid ja pooljuhtide arendajad – kui ka ühiskonna üldiste digipädevuste tõusu, et inimesed oskaksid uusi lahendusi kasutada ja neid usaldada. Eesti ja Euroopa tugevus sõltub sellest, kui hästi suudetakse ühendada kõrgharidus, teadus- ja arendustegevus ning ettevõtlus, et luua tipptasemel teadmisi ja oskusi, mis toetavad digipöörde eesmärke. Samal ajal peab digipädevuste

arendamine olema läbiv kõigis haridustasemetel ja ka täiskasvanute õppes, et kogu ühiskond oleks valmis kasutama ja arendama lahendusi, millele tugineb Euroopa konkurentsivõime ja turvalisus.

2.9. **Küberspetsialistide defitsiidi vähendamine ning järelkasvu tagamine.** ENISA andmetel on Euroopas küberturvalisuse spetsialistide defitsiit umbes 300 000 töökoha võrra, mida hetkel ei suudeta täita olemasolevate lõpetajatega. Sama kinnitas ka ISC 2023.aasta uuring, mille järgi ISC2 2023. aasta tööjõu-uuringu hinnangul on küberturvalisuse spetsialistide tööjõupuudus ELis 274 000 ja selle puudujäägi kaotamiseks on vaja oskuste baasi laiendada 29%. Üle kahe kolmandiku ELi vastanutest väidab, et nende organisatsioonides on küberturvalisuse töötajate puudus, kes suudaksid ennetada ja tõrkeotsingut teha. Sellest tulenevalt toetame küberspetsialistide järelkasvu aktiivset rahastamist hariduse kõigil tasanditel: nii üldhariduskoolides, kui kutse- ja ülikoolides, sh doktori- ja magistriõppes.

2.10. **Roheline digipööre.** Digilahendused on olulised kliimaeesmärkide saavutamisel, kuid samas tuleb tagada, et ka digitaristu ise oleks võimalikult keskkonnasäästlik. Eestis on potentsiaal siduda digiriigi kogemus rohetehnoloogia arendamisega, näiteks energiatõhususe suurendamisel, nutikate energiavõrkude arendamisel või ringmajanduse põhimõtteid toetavate digiplatvormide loomisel.

2.11. **Eesti kui digivaldkonna innovatsioonilabor ja katsepolügoon.** Eestil on oma digiriigi kogemuse, paindliku regulatiivse keskkonna ja avatud innovatsioonikultuuri tõttu unikaalne potentsiaal toimida Euroopa digivaldkonna innovatsioonilabori ja katsepolügoonina. Väikese, aga digitaalselt arenenud ühiskonnana on võimalik kiiresti katsetada uusi lahendusi reaalses keskkonnas, koguda usaldusväärset tagasisidet ja skaleerida õnnestunud mudeleid laiemalt. Selline roll aitab kiirendada Euroopa Liidu strateegiliste digieesmärkide elluviimist, vähendada tehnoloogia kasutuselevõtuga seotud riske ja toetada ühtse innovatsiooniruumi kujunemist Euroopas. Seda positsiooni saab veelgi tugevdada läbi Põhja-Euroopa partnerluste – sarnase digiarengu tasemega riikidega koostöös on võimalik katsetada lahendusi mitmes riigis korraga, luues usaldusväärseid ja laiemalt rakendatavaid mudeleid, mida saab kiiresti kogu Euroopa Liidus skaleerida.

2.12. **Digivõimestamine ja lahenduste skaleerimine väljaspool avalikku sektorit.** Edukalt digitaliseeritud riik ei saa toimida ilma ettevõtete laiapõhjalise digivõimekuseta. Ettevõtlussektori digitaliseerimine on sama oluline kui avaliku sektori areng, kuna just ettevõtted loovad tootlikkust, konkurentsivõimet ja uusi töökohti. Eestis tuleb toetada väikeste ja keskmise suurusega ettevõtete suutlikkust võtta kasutusele uuenduslikke digilahendusi, arendada uusi ärimudeleid ja kasvatada oma rahvusvahelist konkurentsivõimet. Samuti on vaja kujundada keskkond, kus Eesti ettevõtete innovatiivsed lahendused saavad kasvada Euroopa edulugudeks. Fookus peab olema juba toimivate ja tõestatud lahenduste skaleerimisel – nii ettevõtluses kui ka avalikus sektoris –, mis aitab vältida killustatust, kiirendab EL digieesmärkide saavutamist ja vähendab sõltuvust kolmandatest riikidest pärit tehnoloogiatest. Eesti saab oma digiriigi kogemuse ja paindliku innovatsioonikeskkonna kaudu toimida platvormina, kus lahendusi on võimalik kiiresti katsetada ja seejärel laiemalt turule tuua. Avaliku ja erasektori koostöö võimaldab kasvatada innovatsiooni ja lisandväärtust kogu ühiskonnale.

2.13. **Koostöö Ukraina, Põhjala-Balti riikide ja Ühendkuningriigiga digi- ja kübervaldkonnas.** Rahvusvaheline partnerlus tugevdab nii Euroopa Liidu kui Eesti vastupanuvõimet, võimendades teadmisi ja oskusi, samuti suurendab see Eesti positsiooni ja hoiab tugeva digiriigi mainet.

2.14. **Andmete kättesaadavuse ja kvaliteedi suurendamine.** Digiühiskonna järgmise arengu eelduseks on see, et avalikus sektoris loodavad andmed oleksid kättesaadavad, kvaliteetsed ja usaldusväärsed. Eesti senine tugevus – laialdane e-teenuste kasutus – vajab järgmisel perioodil uut sammu, kus andmetest kujuneb majanduse ja ühiskonna järgmise arenguhüppe alus. Selleks tuleb oluliselt parandada andmete kättesaadavust ja kvaliteeti. Süsteemne andmekorraldus täna avaliku sektori organisatsioonides puudub, mistõttu andmete halb kvaliteet ja leitavus takistavad nii personaalsemaid teenuseid, andmepõhist juhtimist kui ka tärkavate tehnoloogiate kasutuselevõttu, sh. tehisaru arendamist ja rakendamist. Teisalt tuleb soodustada andmevahetust erinevate osapoolte vahel, luues selleks täiendavaid võimalusi andmete turvaliseks jagamiseks ja kasutamiseks ning riigisiseselt kui ka piiriüleselt (näiteks valdkondlike andmeruumide loomine, turvalised liivakastid, privaatsuskaitse tehnoloogiate arendamine ja rakendamine).

2.15. **Küberjulgeoleku tugevdamine.** Eesti ja kogu läänemaailma jaoks on küberohtu märkimisväärselt suurendanud Venemaa agressioonisõda Ukrainas. Küberründeid kasutatakse hübriidsõja osana, kogutakse luureinfot ning „karistatakse ebasõbralikke riike“ nende poliitiliste otsuste eest. Seetõttu on äärmiselt oluline ajakohase ohupildi tagamine, tugeva küberkilbi loomine ning elutähtsate teenuste kriisikindluse suurendamine. Eesti küberjulgeolekut mõjutavad ka üldised tehnoloogilised suundumused: 5G-tehnoloogia järjest laiem kasutuselevõtt, tehisintellekti ulatuslikum rakendamine, kvantarvutite ja postkvantkrüptograafia, digitaalsete teenuste ühilduvus uue põlvkonna internetiprotokolliga IPv6 jne. Uute kübertrendide- ja ohtudega arvestamine on küberjulgeoleku suurendamise lahutamatu osa. Eesti kübervaldkonna oluliseks prioriteediks on ka küberspetsialistide järelkasvu parandamine, mille suur puudus on üle Euroopa[1]. Oluline on rahvusvahelise küberkoostöö tugevdamine nii ühise olukorrapildi tekitamiseks, kui ka ühisõppuste läbiviimiseks.

2.16. **Jätkusuutliku digitaristu tagamine.** Jätkuvalt on oluline digitaalsete ühenduste arendamine, millele uuel perioodil ei ole eraldi tähelepanu pööratud. Fookus on nihkunud CEF Transpordile ja CEF Energiale Rõhutame vajadust ja jätkuvat tööd Euroopa Komisjoni suunal, et suurtesse piiriülestesse transpordi- ja energeetika (CEF Transport ja CEF Energy) projektides oleks abikõlblik kulu elektrooniline sidetaristu. Euroopa Liidu suurem eesmärk peab olema, et Euroopa Liit tervikuna on ühenduva transpordivõrgustikuga kaetud, mis suurendab ka kõikehõlmavat side toimepidevust ja ühendab kõiki digiteenuseid. Sidetaristu teenib julgeolekut ja siseturvalisust, millele Eesti peab Euroopa suunal rõhuma. Suuremate digitaalsete ühenduste kasutuselevõtt eeldab suuremat tähelepanu küberturvalisusele ja andmekaitsele. Tähelepanu tuleb pöörata vastupanuvõime (kerksuse) ja hukukindluse suurendamisele, tehnoloogilisele suveräänsusele ja juhtpositsioonile.

2.17. **Tagada siseturvalisus ja tõhustada võitlust organiseeritud kuritegevusega.** Organiseeritud kuritegevuse puhul on oluline riikide vaheline koostöö, kriminaaluurimise materjalide edastamine digitaalsete kanalite kaudu ning õigusemõistmise digivõimekuse kasv. Tõhustama peab võitlust organiseeritud kuritegevuse vastu (majanduskuriteod, sh rahapesu, kelmused, terrorismi rahastamine korruptsioon, küberkuritegevus), tugevdades õiguskaitsealast koostööd ja andmevahetust, töötades koostöös teiste liikmesriikidega välja rahapesu ja finantskuritegevuse vastased meetmed ning tõhustades kriminaaltulu tuvastamist, arestimist ja konfiskeerimist. Europoli ja Eurojusti rolli peab tugevdama, et hõlbustada liikmesriikide politsei- ja

[1] ENISA[8] andmetel on Euroopas küberturvalisuse spetsialistide defitsiit umbes 300 000 töökoha võrra, mida hetkel ei suudeta täita olemasolevate lõpetajatega.[9] Sama kinnitas ka ISC 2023.aasta uuring[10], mille järgi ISC2 2023. aasta tööjõu-uuringu hinnangul on küberturvalisuse spetsialistide tööjõupuudus ELis 274 000 ja selle puudujäägi kaotamiseks on vaja oskuste baasi laiendada 29%.

kohtuasutuste vahelist koostööd. Samuti on oluline Euroopa Prokuratuuri tugevdamine. Euroopa Liidus peab edendama kiiret ja turvalist andmevahetust organiseeritud kuritegevuse võrgustike jälgimiseks ja neutraliseerimiseks. Oluline on Schengeni ala julgeoleku tugevdamine, sh vajadusel suurendades piirikontrolli efektiivsust, et takistada kuritegelike rühmituste liikumist. Kriisiolukordade süvenemisel (näiteks rändekriis) on vaja täiendavaid ressursse nendega toimetulemiseks (näiteks riigi õigusabi osutamise ja kohtumenetluse toimepidevuse tagamine). Jätkuvalt vajavad tähelepanu laste ja teiste haavatavate sihtrühmade vastu suunatud kuriteod ja nende ennetamine ning õigusrikkujate taasühiskonnastamine, mis teenib siseturvalisuse ja julgeoleku eesmärke.

2.18. Uurimisvõimekuse tõhustamine. Arvestades, et masskuritegude (nt küberrünnakud) toimepanemisel kasutatakse aina sagedamini erinevaid arvutisüsteeme ning tehisaru arenemine ja laialdasem kasutusele võtmine loob suurema riski võltsitud (*fake*) tõendite loomiseks, tuleb luua paremad digikriminalistika võimekused. Kohtueelse ja kohtuliku uurimise tõhustamiseks on vaja tõhustada õiguskaitseametnike justiitskoostööd ja suurendada teadmisi kuritegude, küberrünnete ja riigi infrastruktuuri kahjustamise uurimisel, sh parandades andmeanalüüsi kvaliteeti (sh AI analüüs, massandmete analüüs, mõjutustegevuse aluseks oleva sotsiaalmeedia, sh kampaaniate analüüs, süvavõltsingute leidmine jm) ja teabe tõendiks vormistamist. Eraldi tähelepanu väärib hübriidohtude temaatika, nt merekaablitega seotud ekspertiisid, laevades olevate tehniliste vahendite ekspertiisid, GPS *spoofing*, selle modelleerimine.

2.19. Kokkuvõtvalt peame oluliseks, et mitmeaastase finantsraamistiku tulemusraamistik ja rakendusmehhanismid arvestaksid digivaldkonna strateegilisi eesmärke kõikides poliitikavaldkondades. Digilahenduste süsteemne kasutamine aitab vähendada halduskoormust, lihtsustada aruandlust ja kiirendada fondide rakendamist. Digitaalsed tehnoloogiad peavad kaitsma isikute põhiõigus ja vabadusi, toetama demokraatia ja õigusriigi põhimõtet ning tagama ühenduste turvalisuse ning võimaluse kuritarvitajad tuvastada ja vastutusele võtta.

Oluline on tagada, et väiksemad liikmesriigid ei kaotaks oma positsiooni ning et aruandlus ja tulemusraamistik oleksid proportsionaalsed, toetaksid haldusvõimekust ja võimaldaksid maksimaalselt kasutada ühtseid vorme ja digitööriistu.

Järgnevalt esitame täpsemad seisukohad Rahandusministeeriumi (RaM) ettepanekutele Euroopa Liidu pikaajalise eelarve aastateks 2028-2034 (edaspidi eelarve määrus)[2], Euroopa Liidu Euroopa Fondi ning riiklike ja piirkondlike partnerluskavade raamistiku (edaspidi riigiplaani määrus)[3], Euroopa Liidu programmide rakendamise ja tulemusraamistiku (edaspidi tulemusraamistiku määrus)[4] kohta, milles peame vajalikuks täiendavalt midagi lisada (vajadusel Vabariigi Valitsusele esitamiseks) ja millel on puutumuses ka Konkurentsivõime Fondi määruse ettepaneku,[5] teadusuuringute ja innovatsiooni

[2] komisjoni teatis Euroopa Parlamendile, Euroopa Ülemkogule, nõukogule, Majandus- ja Sotsiaalkomiteele ning Regioonide komiteele ELi dünaaminline eelarve tuleviku prioriteetide elluviimiseks – Mitmeaastane fianantsraamistik 2028-2034, COM(2025) 570; ettepanek: nõukogu määrus, millega määratakse kindlaks mitmeaastane finantsraamistik aastateks 2028-2034, COM(2025) 571; ettepanek: institutsioonidevaheline kokkulepe Euroopa Parlamendi, Euroopa Liidu Nõukogu ja Euroopa Komisjoni vahel eelarvedistsipliini, eelarvealase koostöö ning usaldusväärse finantsjuhtimise kohta, COM(2025) 572.

[3] Euroopa Parlamendi ja nõukogu määrus (EL) 2025/0240, millega luuakse Euroopa Fond majandusliku, sotsiaalse ja territoriaalse ühtekuuluvuse, põllumajanduse ja maaelu, kalanduse ja merenduse, heaolu ja julgeoleku perioodiks 2028–2034 ja muudetakse määrust (EL) 2023/955 ning määrust (EL, Euratom) 2024/2509 (COM(2025) 565); Euroopa Parlamendi ja nõukogu määrus (EL) 2025/0239, millega luuakse Euroopa Sotsiaalfond osana riiklikust ja regionaalsest partnerluskavast… (COM(2025) 558); Euroopa Parlamendi ja nõukogu määrus (EL) 2025/0238, millega luuakse Euroopa Fond Regionaalarenguks sealhulgas Euroopa territoriaalse koostöö (Interreg) ja Ühtekuuluvusfond… (COM(2025) 552)

[4] Euroopa Parlamendi ja nõukogu määrus 025/0545 (COD), millega luuakse Eelarvekulude jälgimise ja tulemuslikkuse raamistik ning muud horisontaalsed reeglid liidu programmide ja tegevuste jaoks ja selle lisad

[5] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing the European Competitiveness Fund ('ECF'), including the specific programme for defence research and innovation

raamprogramm „Euroopa Horisont[6]“ (edaspidi Euroopa Horisont) ja Globaalse Euroopa Instrumendi ettepanekuga:[7]

1. **Peame oluliseks ja toetame RaM ettepanekut, et kõik liikmesriigid ja Euroopa Liit järgivad õigusriigi põhimõtet, mis on Euroopa Liidu põhiväärtus (seotud ka RaM eelarve määruse ettepanekuga 5.2.3), kuid rõhutame vajadust arvestada, et õigusriigi protsessis on oluline ka liikmesriigile prioriseerimise ja otsustusõiguse jätmine, kuidas oma eelarve ja poliitika kujundamise valikuid teha.** Uuel rahastusperioodil peavad liikmesriigid riigiplaanide koostamisel järgima õigusriigi põhimõtet. Nad peavad selgitama komisjonile**,** kuidas kava ja selle kavandatud rakendamine tagavad õigusriigi põhimõtete järgimise vastavalt riigiplaani määruse artiklile 9 (õigusriigi horisontaalsed tingimused), koos selgitustega selle kohta, milliseid järelmeetmeid on rakendatud viimase õigusriigi aruande ja Euroopa poolaasta raames esitatud riigipõhiste soovituste osas, samuti meetmetest nende tuvastatud riigipõhiste probleemide lahendamiseks. Õigusriigi põhimõtetest mittekinnipidamisel on Euroopa Komisjonil õigus peatada maksed liikmesriigile. Toetame ühtlasi ka seda, et õigusriigi riigiraportis väljatoodud soovitusi saab adresseerida riigiplaanis reformide ja investeeringute planeerimisel ning nende elluviimist rahastada Euroopa Liidu vahenditest.

2. **Toetame RaM ettepanekut, et Euroopa Liidu idapiiri riikidele ja piirkondadele, kes on kannatanud Venemaa Ukraina vastu suunatud agressioonisõja tõttu, eraldatakse pikaajalises eelarves täiendavad vahendid.**
   Lisaks RaM seisukohtadele peame vajalikuks rõhutada, et lisaks majanduslikele raskustele on nimetatud riigid silmitsi ka elanike igapäevaelu mõjutavate väljakutsetega, mis nõuavad täiendavaid investeeringuid. Näiteks on agressorriigist tingituna mõjutatud piiriäärne mobiilsideteenuste toimimine, sagenenud GPS-signaalide häired ja märkimisväärselt suurenenud küberründed, sh elutähtsale taristule. Nende probleemide lahendamine, näiteks uute tugijaamade ja häireid tõrjuvate süsteemide paigaldamine, suurendab omakorda kulutusi, aga on vajalikud elanike igapäeva elu toimimiseks (ohutu lennuliiklus ja andmeside kättesaadavus). Küberrünnetega kogutakse luureinfot ning “karistatakse ebasõbralikke riike” nende poliitiliste otsuste eest.

3. **Toetame RaM ettepanekut, et Eesti prioriteediks on ettepanekus esitatud kaitsevalmiduse ja piiriüleste taristuühenduste ning Ukraina toetamise eelarvemahtude kaitsmine läbirääkimistel.**
   Lisaks Rahandusministeeriumi seisukohtadele peame rõhutama, et vähendada ei tohi ka piiriülestele taristuühendustele, sh sidetaristule olemasolevaid summasid ja Euroopa Liidu prioriteetideks peab endiselt jääma Euroopa katmine omavahel ühenduva taristuvõrgustikuga (vt ülevalt punkti 15).

4. **Toetame RaM ettepanekut rõhutada vajadust tagada EL eelarve kasutusega seotud näitajate süsteemi sihipärasus, tasakaal ja paindlik rakendamine.**
   Tulemuspõhisuse rakendamisel on võrreldes käimasoleva rahastusperioodiga 2021-2027 oluline muudatus, sest väljund- ja tulemusnäitajate loend on ette nähtud tulemusraamistiku määruse lisas. See võib tekitada olukorra, et riigiplaanis olevale valdkonnale vastavat (eelkõige) tulemusnäitajat ei ole (nt rida 428 sekkumise “Capacity building of justice actors, judicial training, transparency and accountability” puudub väljundnäitajat “Number of participants in training activities (including exchange programmes and study visits) või olemasolevad ei sobi (näiteks

activities, repealing Regulations (EU) 2021/522, (EU) 2021/694, (EU) 2021/697, (EU) 2021/783, repealing provisions of Regulations (EU) 2021/696, (EU) 2023/588, and amending Regulation (EU) [EDIP]

[6] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing Horizon Europe, the Framework Programme for Research and Innovation, for the period 2028-2034 laying down its rules for participation and dissemination, and repealing Regulation (EU) 2021/695

[7] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing Global Europe, COM(2025)551.

rida 429 sekkumise “Digitalisation of justice system” väjundnäitaja “Number of EU-level ICT systems set up/adapted/maintained” ei näita siseriikliku digitaliseerimise taset, kuna näitaja täitmine sõltub Euroopa Liidu enda arendustest, mis võib aega võtta aastaid. Digitaliseerituse taset näitab see, kui paljud ELi poolt kättesaadavaks tehtud lahendused on riigi poolt kasutusele võetud). Tuleb arvestada, et mõnedes poliitikavaldkondades ei ole tavapärane kvantitatiivne mõõtmine asjakohane, näiteks õiguskaitse valdkonnas kuritegude ennetamisel, samuti õigussüsteemi digitaliseerimise valdkonnannas. Toetame Taaste- ja vastupidavusrahastu senise praktika jätkamist, mil reformide ja sekkumiste näitajad (*milesto ja target)* lepib liikmesriik Euroopa Komisjoniga eraldi kokku, arvestades liikmesriigispetsiifiliste reformide ja sekkumiste sisu.
Tulemusraamistiku lisas on küberturvalisuse valdkond sisustatud kahe näitajaga (intervention field): poliitika valdkonnas “*Research and innovation*” #347 “*Cybersecurity”* ja poliitika valdkonnas “*Digital capacities and advanced technologies*” #100 “*Cybersecurity - deployment and scale-up".* Katmata on indikaatorite nimekirjas kaks väga olulist valdkonda “Conflict, peace and security” ning “EU internal security”, millele palume küberturvalisuse indikaatorid samuti juurde lisada. Tabeli täiendus on all toodud.

Policy area (level 1)	Policy area (level 2)	Intervention field	Output indicator	Result indicator
Peace, conflict and humanitarian aid	Conflict, peace and security	Cybersecurity	Number of projects	• Increase of preparedness for dealing with cyber crises; • Number of resolved high-impact incidents
Resilience, defence industry and space	EU internal security	Cybersecurity	Number of projects	• The crisis resilience of vital services has improved

Tulemusraamistiku lisas olevas väljund- ja tulemusnäitajate loendist tulenevalt ei näidata poliitikavaldkondade “Ühendatavus” ja “Digivõimekus ja innovatsioonitehnoloogiad” osakaalu Euroopa Komisjoni poolt ettenähtud osakaaludega valdkondades (kliima, keskkond ja sotsiaal). Seetõttu näeme vajadust riigi pikaajaliste strateegiliste eesmärkide seadmisel arvestada digilahenduste (sh digitaristu ja küberturvalisuse) olulisuse ja panustamisega kohustuslikult jaotatud valdkondade (temaatiliste eesmärkide) rakendamisel. See tagab näiteks, et iga uue tehnoloogia arendamisel oleks tagatud ka küberturvalisus.
Lisaks tuleb analüüsida, kas nõutud andmete küsimine osalejatelt vastab andmekaitseõiguse põhimõtetele või tuleb ette näha erisusi, näiteks õigusametnike koolitusel osalejatelt on tulemusraamistiku lisa kohaselt vaja küsida andmeid soo kohta (mees, naine, mitte-binaarne), jätmata aruandluskohustuse raames vastajale võimalust mitte vastata.

5. **Toetame Euroopa Konkurentsivõime Fondi (KVF) eelarve jaotust valdkondade vahel**, kus kogusummast 234 300 000 000 eurost moodustab digitaalne juhtpositsioon 51 493 000 000 eurot, kuhu alla kuulub ka sidetaristu, arvestades nende valdkondade investeeringute suurenenud vajadusi ning muutunud geopoliitilist olukorda. Samas toetame RaM seisukohta, et vajadusel – nt kaitse eesmärgil, välis- ja majanduskeskkonna olulisel muutumisel, ettenägematus suunas läbimurdeliste ja suure mõjuga tehnoloogiliste lahenduste väljatöötamisel oleks võimalik seda valdkondade vahelist jaotust uuendada. Tänases julgeoleku olukorras ei piisa elutähtsate teenuste osutamisel enam tavapärasest toimepidevuse tagamisest, vaid peame olema valmis ka riigikaitselisteks stsenaariumiteks vastavalt Riigikaitse arengukavale. Riigi Infosüsteemi andmeil toimus Eestis 2024. aastal 6515 mõjuga küberintsidenti ehk umbes kaks korda rohkem kui 2023. aastal ning umbes kolm korda rohkem

kui 2021. aastal. Venemaa agressioonisõda Ukrainas on näidanud, et lisaks kineetilise sõjategevuse toetamisele küberrünnetega elutähtsa taristu pihta kasutatakse küberründeid hübriidsõja osana ka laiemalt. Kuna ründeid on tehtud ka elutähtsate teenuste ja elutähtsa taristu vastu, on küberrünnete ennetamine ja nendega toimetulemine seotud ka riigi üldise julgeolekuga ja täiendavate valdkondade vahelise rahalise jaotuse ümbervaatamisega. Peame oluliseks, et konkurentsivõime fondi poliitikavaldkonna “Kerksus ja julgeolek ning kaitsetööstus ja kosmos" eelarvejaotuse eesmärkides oleks konkreetselt väljatoodud kahe otstarbelised (*dual-infrast*) infrastruktuuri tüübid, mida poliitikaeesmärk rahastab ja kaetud oleks ka sidetaristu ehitus ja küberturvalisus. Seda võimaldab ka nimetatud poliitikasuuna eelarvevahendid.

6. **Toetame RaM seisukohta, et riigiplaanis peab paremini arvestama liikmesriikide ja nende piirkondade eripärade ning pikaajaliste strateegiliste arenguvajadustega ja suurendada elluviimise/rakendamise paindlikkust, vähendades riigiplaani struktuuri jäikust ja detailsust ning lihtsustada riigiplaanile seatud eritasandilisi reegleid ja nõudeid.** Digivaldkonna rahastusel on oluline prioriteet ka riigiplaani koostamisel, sest turvalise ja kestliku digitehnoloogia, -keskkonna ja -taristu arendamine ja rakendamine on hädavajalik, et tagada Euroopa Liidu konkurentsivõime, innovatsioonivõimekus ja elutähtsate teenuste toimepidevus. Digivaldkonna sihipärane rahastamine loob eeldused küberturvalisuse tugevdamiseks, rohepöörde edukaks elluviimiseks ja väiksemate liikmesriikide võrdsete võimaluste tagamiseks. Ilma eraldi tähelepanu ja rahastuseta on oht, et digitaalne üleminek jääb killustatuks ning Euroopa ei saavuta seatud strateegilisi eesmärke, kus arvestatakse ka liikmesriikide enda pikaajaliste strateegiliste arenguvajadustega.

7. **Toetame RaM ettepanekut suurendada paindlikkust riigiplaani muutmisel, et liikmesriigil oleks võimalik vajadusel paindlikult plaane ümber teha, et kiiresti kohaneda ettenägematute ja ootamatute asjaolude ja kriisidega.**
Lisaks RaM seisukohtadele, tuleb arvestada käesoleva perioodi kogemustega (näiteks ReArm) ja võimalike tulevaste kriisidega (nt rändekriis), mis vajab kiirete lisaressursside leidmist (näiteks riigi õigusabi osutamiseks, kohtumenetluste pidamiseks) riigiplaani või fondide sisestest jaotustest.

8. **Toetame nn EL eelistuse (EU *preference*) põhimõtet, mis toetab** ELi strateegilist autonoomiat – Euroopa Liidu enda ettevõtteid ning tehnoloogiaarendust (näiteks osalevad üksused peavad olema asutatud liikmesriikides, tegevuste läbiviimiseks tuleb kasutada ainult nendes riikides asuvaid rajatisi või tegevusi jne).

9. **Toetame Euroopa Horisondi raamprogrammi ligipääsetavust Euroopa Liidu välistele assotsieerunud liikmetele uuel MFFi programmiperioodil.** Uuel programmiperioodil peame oluliseks ja toetame aktiivselt Ukraina riigi assotsiatsioonilepingu sõlmimist Euroopa Horisondi raames. Selline samm aitaks tugevdada teaduskoostööd, sealhulgas keelemudelite ja AI lahenduste arendamise vallas, edendada innovatsiooni ning toetada Ukraina integreerumist Euroopa teadus- ja majandusruumi.

10. **Peame oluliseks täiendavate meetmete rakendamist, mis võimaldaksid Ukraina riigi finantsilist toetamist Euroopa Horisondi raamprogrammis.** See aitaks tugevdada Ukraina teadus- ja innovatsioonivõimekust ning toetaks riigi sügavamat integreerumist Euroopa teadus- ja majandusruumi. Ukrainal on ülisuur potentsiaal pakkuda Euroopale kogemusi ja teadmisi kaitsevaldkonnas (kübertehnoloogiad, droonide testimiskeskkond jne*).* Laiapõhisem toetamine võimaldab Ukrainal aktiivsemalt arendada enda majandust ja ettevõtluskeskkonda, mis tagab ka Ukraina majandusliku ja institutsionaalse valmisoleku Euroopa Liiduga liitumiseks.

11. **Peame tähtsaks arvestada asjaoluga, et Eesti riik ei kuulu lähiaastatel laienemisriikide (*widening countries*) kategooriasse, vaid on määratletud kui üleminekuriik (*transition country*).** Antud klassifikatsioonil on oluline mõju MFFi programmidest rahastuse taotlemisel ja saamisel. Üleminekurühma kuuluvad Eesti, Kreeka, Küpros, Malta, Portugal ja Sloveenia. Kuue üleminekuriigi edasiminek innovatsiooninäitajates (*European Innovation Scoreboard*) näitab, et nende teadus- ja innovatsioonisüsteemid vajavad senisest vähem välist tuge — see on positiivne areng. Külla aga tähendab see meie jaoks osaluse laienemise meetme (*widening-meede*) lõppu, mis avaldab negatiivset mõju Eesti ettevõtetele ja geopoliitilise asetuse tõttu on investeeringud juba niigi Eestisse vähenenud.

12. **Näeme murekohana, et Euroopa Horisonti raames ei ole MFF 2028–2034 perioodil ette nähtud piisavaid täiendavaid toetusmeetmeid üleminekuriikidele, mis aitaksid neil tõsta oma digivaldkonna innovatsioonivõimekust võrreldavale tasemele ELi mittelaienemisriikidega (*arenenud riikidega*).** Soovitame eraldi innovatsioonikiirendite loomist, mis soodustaks innovatsioonilõhe vähendamist mittelaienemisriikidega või et kehtiks eelmise perioodi laienemisriikide võimalused ka mittelaienemisriikidele. Üleminekuriikidelt ei saa oodata valmisolekut konkureerida sarnastel alusetel mittelaienemisriikidega.

13. **Euroopa Horisondi projektirahastuse puhul me ei toeta toetuse üldmäära langetamist üleminekuriikidele, mille puhul senine 80%-i määr vähendatakse 60%-i peale.** Antud muudatusega tõuseb mh. digivaldkonna ettevõtetele omaosaluse nõue. Selline muudatus ohustab üleminekuriikides võimekust osaleda teadus- ja arendustegevuses ning pärsib innovatsiooni ja konkurentsivõime kasvu üleminekuriikides, kes ei ole veel konkureerivad mittelaienemisriikidega. See vähendab niigi vähest osalemist rahastusprogrammides ning tõkestab kohalike ettevõtete kasvu. Muudatustel on oluline kaal üleminekuriikidele ning Eesti majandusele.

14. **Teeme ettepaneku lisada Euroopa Horisondi ja Konkurentsivõime Fondi eesmärkidesse küberturvalisus kui eesmärk**, mitte ainult jääda üldise "*security*" alla nagu seni. Tänapäeval on kõik juba digi, seega kõik alates põllumajandusest kuni loomemajanduseni, kaitsest kuni terviseni peab olema digitaalne ja seega kõige puhul peaks küberturvalisus olema võtmetähtsusega.

15. **Euroopa Horisondi ja Konkurentsivõime Fondi digitaalse juhtpositsiooni fookusvaldkondadena peame oluliseks tehisaru, andmepõhiste lahenduste ja küberjulgeoleku suurendamise süstemaatilist rahastamist. Sealhulgas järgmistes valdkondades:**
    a) tehisaru gigatehased ja kõrgjõudlusega andmetöötlus kui strateegiline taristu, et tagada Euroopa oma keele- ja multimodaalsete mudelite arendamise võimekus;
    b) andmete kättesaadavus, arusaadavus ja kvaliteet – avaandmete, andmeruumide arendamine ja liidestumine, privaatsuskaitse tehnoloogiate rakendamine, et tagada andmete kasutatavus innovatsiooniks ning teenuste osutamiseks nii era- kui ka avalikus sektoris;
    c) tehisaru põhiste lahenduste arendamine ja kasutuselevõtu toetamine avalikus sektoris, sh justiitssüsteemi tõhustamine ning selleks vajalike protsesside muutmine, oskuste ja teadmiste arendamine;
    d) AI-põhiste rünnete kaitsesüsteemid (o*ffensive/defensive AI*), kvantarvutite ja post-kvant krüptograafia, täisusaldamatuse turbeprintsiibi rakendamine *(zero-trust architecture)*, tarneahelate turvalisus, lõimturbe põhimõtete, mittefunktsionaalsete nõuete rakendamine teenuse arenduses ja IoT turvalisus, AI mudelite ja andmete ründevektorid ja kaitsemeetmed (*modal hacking, data poisoning*), digitaalsete teenuste ühilduvus uue põlvkonna internetiprotokolliga IPv6 jne, et arvestada uute tehnoloogiate ja küberturbe trendidega küberjulgeoleku suurendamisel.

16. **Tunnustame Komisjoni ettepanekut võimaldada uues Euroopa Horisondis kaitseotstarbelise ja kahese kasutusega tehnoloogia rahastamist, mis puudutab II samba 4. teemavaldkonda („digivaldkond, tööstus ja kosmos"), kuhu lisandub kaitsetööstus eraldi fookusena.** Samuti toetame Euroopa Liidu soovi tugevdada oma strateegilist autonoomiat ja kaitsevõimekust ka teadus- ja innovatsioonipoliitika kaudu.

17. **Peame vajalikuks vähendada Euroopa Horisondi erinevate meetmete ja teemaplokkide vahelist dubleerimist, näiteks soodustada kahese kasutusega teadus-arendustegevust ning tehnoloogiasiiret tsiviil- ja kaitsesektorite vahel.** Selle tagamiseks tuleb rakendada kahese kasutuse ja tehnoloogiasiiret toetava teadus- ja arendustegevuse soodustamiseks vastavaid meetmeid ja hindamiskriteeriume. On vajalik luua regulatsioonid teadus- ja arendusprogrammide üleselt valdkondades, mis võivad puudutada kahest kasutust, nt tundliku ja salastatud teabe käitlemine, teadusjulgeolek, küberkaitse, standardiseerimine, avatud teadus jm.

18. **On oluline soodustada lõppkasutajate (eriti riigiasutused) süsteemset kaasamist Euroopa Horisondi projektide elluviimisse,** mis aitab tagada sidususe teadusuuringute, innovatsiooni ja teaduspõhise poliitikakujundamise vahel ning suurendada projektide tulemite rakendamist ja mõju ühiskonnale.

19. **Toetame Euroopa Liidu investeeringuid teadusarendusse uute tehnoloogiate ja küberturbe trendidega arvestamiseks küberjulgeoleku suurendamisel,** sh teaduslike kompetentsikeskuste loomist uute tehnoloogiliste lahenduste rakendamiseks (nt pilvetehnoloogiad, tehisaru ja krüptograafia).

20. **Teeme ettepaneku lisada Euroopa Horisondi samba "Euroopa teadusruum" alla teemana digiareng ja küberturvalisus, tagamaks Eesti ja Euroopa vastavate ülikoolide-teadusasutuste globaalselt tipptasemel püsimiseks ning jõudmaks maailma parimate hulka ka kvant-, postkvant, AI jm temaatikates.** Küberturvalisuse tähtsus maailmas tõuseb ja selle tõttu tuleks selle tippteaduse jaoks teha täiesti eraldiseisvaid pingutusi.

21. **Toetame RaM ettepanekut ja nõustume Euroopa ühendamise rahastu eelarvemahu ettepaneku kohase tasemega. Leiame, et üleeuroopalise transpordivõrgu ja energiavõrgu arendamise ning nende vastupidavuse ja kerksuse parandamise eesmärkide saavutamise katteks on vaja investeeringuid piiriüleste ühenduste arendamiseks oluliselt suurendada.** Peame oluliseks, et Euroopa ja riiklike eesmärkide saavutamiseks on kriitilise tähtsusega integreerida sidetaristu väljaarendamine abikõlbliku kuluna suurtesse piiriülestesse transpordi- ja energeetika projektidesse (vt ülevalt punkti 1.2). See strateegiline lähenemine teenib mitmekordset Euroopa Liidu poliitika eesmärki ja aitab optimeerida ressursside kasutamist.
    Tänapäevane transporditaristu sõltub üha enam kõrgtehnoloogilistest süsteemidest, mis vajavad stabiilset ja kiiret sideühendust. Näiteks raudteede puhul on toimiva sidevõrgu olemasolu hädavajalik rongi juhtimissüsteemide (nt FRMCS), signalisatsiooni, ohutussüsteemide ja operatiivkommunikatsiooni toimimiseks. Lisaks on side oluline energiajuhtimiseks, võimaldades reaalajas andmete vahetust, energiatarbimise optimeerimist ja katkestuste kiiret avastamist, mis on energiavõrkude puhul ülioluline.

22. **Toetame AgoraEU ettepanekut laste ja teiste riskis olevate sihtrühmade vägivallavastase võitluse suuna jätkumist,** kuid rõhutame vajadust pöörata suuremat tähelepanu ennetussüsteemi tugevdamisele EL tasemel ja siseriiklikult ning Euroopa Kuriteoennetuse Võrgustiku (EUCPN) võimestamisele. Lastevastase vägivalla all tuleks eraldi välja tuua ka

kübervägivalla vastaste meetmete väljatöötamist, piloteerimist, kasutusele võtmist ja süsteemset juurutamist. Täna näeme, et lastega seotud vägivallakuriteod saavad alguse või jätkuvad küberruumis ja seega on oluline mh ennetus ja teavitus laste ja noorte hulgas, et valitsevate ohtudega olla kursis, kuid ka vajadusel reageerida kiiresti juhtumitele.
Media+ raames näeme vajadust lapse õiguste teematika kajastamist avalikus ruumis, kus tõsta teadlikkust laste ja noorte endi seas nende õigustest, kohustustest ja nende kaasatusest ühiskondlike otsuste tegemisel.
Kriisiolukordades võib oodata mõjutustegevuse ja noorte radikaliseerumise suurenemist, millele õiguskaitseorganid peavad kiiresti ja adekvaatselt reageerima. Mõjutustegevuse ja noorte radikaliseerumise ennetamiseks on Euroopa Liidu tasandil oluline tugevdada strateegilist kommunikatsiooni ja meediakirjaoskust, et suurendada noorte vastupanuvõimet valeinfole ja propagandale. Samuti on vaja tihendada koostööd tehnoloogiaettevõtetega, et piirata äärmusliku sisu levikut veebikeskkondades, ning arendada ühiseid varajase hoiatamise süsteeme trendide kiireks tuvastamiseks.
Määruse ettepanek ei sisalda CERV+ (kodanike, võrdõiguslikkuse, õiguste ja väärtuste programm) suundade lõikes eelarvelist jaotust, mistõttu vahendite piisavuse või ebapiisavuse osas ühele või teisele suunale ei saa hinnangut anda.

23. **Toetame pettusevastase võitluse struktuuri parendamist.** Euroopa Liidu rahaliste vahendite tõhus kaitse pettuste, korruptsiooni ja muu ebaseadusliku tegevuse eest nõuab mitmetasandilist lähenemist, mis hõlmab ennetusmeetmeid, järelevalvet ja õiguskaitset. Tagada tuleb ajakohane, ent mitte piiravalt bürokraatlik õigusraamistik ning Euroopa Liidu institutsioonide, nt OLAF, EPPO, Euroopa Kontrollikoda ja Euroopa Kohus tõhus ja läbipaistev töö. Liikmesriigid ja Euroopa Liidu institutsioonid peavad rakendama tõhusaid auditeerimis- ja seiresüsteeme, et väärkasutust ennetada. Korruptsiooni vältimiseks tuleb tugevdada avalike hangete järelevalvet ja tagada kõigi osalejate võrdne kohtlemine. Euroopa Liidu toetuste saajatel peab olema mugav ja lihtne aruandluskohustusi täita ning rikkumisest teavitajatele peavad Euroopa Liidu ja liikmesriikide tasandil olema mehhanismid pettustest teavitamiseks ning kaitseks.

Lugupidamisega
(allkirjastatud digitaalselt)

Liisa-Ly Pakosta
justiits- ja digiminister

Kristel Järve
kristel.jarve@justdigi.ee
Sandra Kaljumäe
sandra.kaljumae@justdigi.ee
Monika Karu
monika.karu@justdigi.ee
Kaidi Ristal
kaidi.ristal@justdigi.ee
Raigo Iling
raigo.iling@justdigi.ee
Natalja Zinovjeva
natalja.zinovjeva@justdigi.ee
Annika Leevand 6208174
annika.leevand@justdigi.ee