

Euroopa Parlamendi ja Nõukogu eelnõu COM(2026) 580 final millega täiendatakse Euroopa Liidu õiguskaitsekoostöö Ameti (EUROPOL) tegevust reguleerivat määrust (EL) 2018/1726 ja määrust (EL) 2024/982 ning millega tunnistatakse kehtetuks määrus (EL) 2016/794 (nn **Europoli uuendatud alusmääruse eelnõu)**

Seletuskirja Lisa 1 - **Kaasamistabel**

nr	Arvamuse esitaja, märkuse sisu	Märkuse arvestamine või mittearvestamine, selgitused
1.	Politsei- ja Piirivalveamet	
1.1	Esmase analüüsi pinnalt toetame üldist Europoli teadus-, innovaatilise tehnoloogia- ja analüüsivõime tugevdamist sh reaajas ühist andmeanalüüsi ja jagatud andmepilvede tüüpi lahendusi (<i>EU Police Shared Data Space</i>). Rakendamisel on oluline arvestada liikmesriikide vajadusi ning tagada tõhus koostöö riigisiseste politseiasutustega, kellele jääb tugiteenuste valikul ja rakendamisel otsustusõigus ja juhtimispädevus.	Arvestatud. Täiendatud seletuskirja (vt punkt 7.7).
1.2	Andmevahetuse ja andmetöötluse tõhustamisel on oluline tagada andmete päritolu ja kasutustingimuste arvestamine ning vastutuse selge jaotus andmete edastamisel, töötlemisel ja edasisel jagamisel. Samuti tuleb tagada asjakohased infoturbemeetmed, andmetöötluse jälgitavus ja tõhus järelevalve.	Arvestatud. Täiendatud seletuskirja (vt punkt 7.4).
1.3	Europoli Haldusnõukogu peab säilitama oma senise pädevuse. Uute tugistruktuuride moodustamine ja nende volituste määratlemine ei tohiks vähendada ega piirata Europoli Haldusnõukogu ja liikmesriikide pädevust. Uute struktuuride ülesanded peaksid toetama Europoli tõhusat toimimist ning olema kooskõlas agentuuri väljakujunenud juhtimis- ja järelevalvekorraldusega.	Arvestatud. Täiendatud seletuskirja (vt punkt 7.9).

1.4	Rakendamisel tuleks arvestada liikmesriikide olemasolevate võimekuste ja eelarveliste võimalustega ning kasutada Euroopa Liidu rahastamis- ja koolitusvõimalusi. Hinnata tuleb ka andmekaitse järelevalveasutuste täiendavat töökoormust ning tagada selleks vajalikud ressursid. Rakendamise kavandamisel tuleb siseriiklikult hinnata vajalikke tehnilisi, organisatsioonilisi ja eelarvelisi muudatusi (sh ka andmekaitse ja järelevalve korralduse osas) ning tagada vajalikud ressursid.	Arvestatud. Täiendatud seletuskirja (vt punkt 7.11).
1.5	Samuti tuleb tagada, et uute lahenduste kasutuselevõtt ei tekitaks liikmesriikidele põhjendamatu dubleerivat aruandlus- või andmesisestuskoormust. SIENA ja teiste turvaliste lahenduste arendamisel tuleb pöörata tähelepanu süsteemide koostalitlusvõimele, kasutusmugavusele ning teabe edastamise ja edasise kasutamise tingimuste selgusele.	Arvestatud. Täiendatud seletuskirja (vt punkt 7.7).
1.6	Europoli operatiiv-, analüüsi- ning tehnoloogia- ja innovatsioonivõimekuse arendamine aitab tõhustada liikmesriikide politseikoostööd ning reageerimist piiriülese raske ja organiseeritud kuritegevuse ning terrorismi ohule.	Arvestatud. Täiendatud seletuskirja (vt punkt 7.1).
1.7	Hübriidse mõõtmega kuritegude käsitlemise puhul oleks oluline tagada mõiste piisav selgus ning selle seos Europoli kehtiva pädevuse ja ülesannetega. See aitab kaasa ühtsele arusaamisele kavandatava sätte eesmärgist ja praktilisest rakendamisest.	Arvestatud. Täiendatud seletuskirja (vt punkt 7.10).
1.8	Liikmesriigi pädevatele asutustele peab jääma otsustusõigus Europoli toe kasutamise ja rakendamise üle ning riigisiseste kriminaalmenetluste ja uurimistoimingute juhtimise pädevus peab jääma liikmesriigile.	Arvestatud. Täiendatud seletuskirja (vt punkt 7.1).

1.9	Europoli operatiivrakkerühmade, ühiste uurimisrühmade ja ekspertreservide kasutamise viis peab jääma liikmesriigi otsustada.	Arvestatud. Täiendatud seletuskirja (vt punkt 7.1).
2.	Siseministeeriumi Infotehnoloogia- ja Arenduskeskus (SMIT)	
2.1	Riiklikud menetlussüsteemid tuleb määruse alusel ühendada Europoli ristkontrolliteenusega. Selleks on vajalikud automaatsed andmelaadurid, päringud, andmete uuendamine ja kustutamine ning andmekvaliteedi kontroll. SMIT peab arvestama turvalise võrguühenduse, lõppseadmete, sertifikaatide, logimise, talitluspidevuse ja võimaliku paralleelkäidu vajadusega. Mõju SMIT-ile seisneb eelkõige volituste, piirangute, nõusolekute ja auditeerimise tehnilises rakendamises. Tegelik töömaht sõltub rakendusaktidest. Seetõttu ei ole eelnõu põhjal veel võimalik prognoosida mõju eelarvele.	Arvestatud. Täiendatud seletuskirja (vt punkt 7.2).
2.2	Tagada määruse alusel koostatavate rakendusaktide eelnõude koostamisel konsulteeritakse liikmesriikide tehniliste ekspertidega enne komiteemenetlust ning näha ette minimaalne üleminekuperiood pärast täieliku tehnilise spetsifikatsiooni vastuvõtmist, et liikmesriigid saaksid arendused eelarvestada, hankida, testida ja sertifitseerida.	Arvestatud. Täiendatud seletuskirja (vt punkt 6.2)
2.3	Vajalik on täpsustada mõistet „ <i>national systems connected to the Europol cloud infrastructure</i> ” – kas nõue puudutab üksnes Europoliga otseliidestatud süsteeme või kõiki süsteeme, millest andmed jõuavad Europoli. Sätestada, et digiidentiteet ei anna iseenesest juurdepääsuõigust ning Eesti süsteemi omanik säilitab lõpliku autoriseerimisõiguse ka kolmanda riigi kasutaja puhul.	Arvestatud osaliselt. Täiendatud kirjalikku tagasisidet töörühmas.
2.4	Sätestada tehnilistes aktides järjekorrahalduse, kordustöötluse, katkestusrežiimi, taaste, teenustaseme ja versioonihalduse miinimumnõuded, et Europoli teenuse rike ei peataks riiklikku menetlust.	Arvestatud. Täiendatud seletuskirja.
2.5	Selgelt tuleb piiritleda isikuandmete töötlemise ulatus, nõuded andmekaitsealaste kontrollide tegemiseks ja vastutuse piirid.	Arvestatud. Täiendatud seletuskirja (vt punkt 7.5).

2.6	Vajalik selge rollijaotus ja vastutused küberintsidentide korral tegutsemiseks, võimalik vajadus täiendavate turvameetmete ja pideva seire järele.	Arvestatud. Täiendatud seletuskirja (vt punkt 6.2).
2.7	Liikmesriikide tehnilised eksperdid tuleb kaasata uute Europoli ja eu-LISA süsteemide planeerimisse piisavalt varakult, et võimaldada siseriiklike arenduste, liidestuste ja hangete õigeaegset ettevalmistamist.	Arvestatud. Täiendatud seletuskirja.
2.8	Uute süsteemide kavandamisel tuleb tagada nende koostalitlusvõime olemasolevate riiklike infosüsteemidega ning arvestada liikmesriikide tehniliste võimekustega.	Arvestatud. Täiendatud seletuskirja (vt punkt 6.2).
3.	Andmekaitse Inspeksioon (AKI)	
3.1	AKI esialgsel hinnangul võib määruse ettepaneku rakendamine kaasa tuua AKI töökoormuse ja ressursivajaduse suurenemise. Ettepaneku kohaselt seisneb AKI roll eelkõige Eesti õiguskaitseasutuste poolt Europolile andmete edastamise ja Europoli teenuste kasutamise õiguspärasuse kontrollimises ning koostöös EDPS-i ja teiste liikmesriikide järelevalveasutustega.	Arvestatud. Täiendatud seletuskirja (vt punkt 6.2).
3.2	Andmekaitse-, infoturbe- ja järelevalvenõuded peavad olema piisavalt selgelt sätestatud nii määruses kui ka selle alusel kehtestatavates rakendusaktides ja -juhistes.	Arvestatud. Täiendatud seletuskirja (vt punktid 6.2 ja 7.8).
3.3	Teadus- ja innovatsioonitegevuses tuleks võimaluse korral eelistada anonümiseeritud, pseudonümiseeritud või sünteetiliste andmete kasutamist.	Arvestatud. Täiendatud seletuskirja (vt punkt 7.8).
3.4	Määruse rakendamisel tuleb hinnata järelevalveasutuste täiendavat töökoormust ning tagada selleks vajalikud ressursid.	Arvestatud. Täiendatud seletuskirja.
3.5	Europoli uute teenuste, infosüsteemide, andmevahetuslahenduste ja innovatsiooniprojektide kasutuselevõtt suurendab vajadust AKI ennetava nõustamise järele. Õiguskaitseasutustele peab olema võimalik pakkuda andmekaitsealast tuge juba arenduste, liidestuste ja uute andmetöötluslahenduste planeerimise etapis.	Arvestatud. Täiendatud seletuskirja (vt punkt 6.2).
4.	Eesti Kohtuekspertiisi Instituut (EKEI)	

4.1	EKEI täiendavat ressursi- ja eelarvevajadust ei ole eelnõu praeguses menetlusetapis võimalik usaldusväärselt hinnata. Võimalikud kulud võivad eelkõige olla seotud infosüsteemide tehnilise kohandamise, DNA-profiilide võrdlemise rakenduse võimaliku kasutuselevõtu ning töötajate väljaõppega.	Arvestatud. Täiendatud seletuskirja (vt punkt 6.2).
5.	Rahapesu andmebüroo (RAB)	
5.1	Eelnõust ei nähtu üheselt, et Europol võiks rahapesu andmebüroodele päringuid teha ainult rahapesu või terrorismi rahastamise kahtluse korral. Eelnõu artikli 9 lõike 4 kohaselt teeb Europol koostööd rahapesu andmebüroodega, et toetada Europoli pädevusse kuuluvaid piiriüleseid uurimisi („ <i>falling within the scope of Europol's competence</i> “). Europoli pädevusse kuuluvad sisuliselt kõik kuriteod, mis tähendab sellisel juhul määruse jõustumisel väga laia mandaati päringute tegemisel . Hetkel jääb selgusetuks see, kas rahapesu andmebüroodelt hakatakse ootama analüüsitoodete koostamist või üksnes olemasolevate analüüsede edastamist. Kui silmas peetakse analüüsitoodete koostamist, tekib küsimus nii ressursivajaduse kui ka koordineerimise kohta.	Arvestatud. Täiendatud seletuskirja
5.2	RAB peab oluliseks, et rahapesu andmebüroodele jääks autonoomsus ning õigus otsustada, millist infot nad saavad Europolile ja Europoli vahendusel teistele liikmesriikidele jagada. Eelnõu menetlemisel vajavad selgust andmete edastamisest keeldumise tingimused.	Arvestatud. Täiendatud seletuskirja (vt punkt 6.2).
5.3	Praeguses etapis on raske hinnata, millises mahus võib Europoli võimestamine mõjutada RAB-i töökorraldust. Määruse jõustumine võib kaasa tuua täiendava ressursikulu arenduste jaoks, kui tekib vajadus luua uusi turvalisi andmevahetuskanaleid ja liidestusi. Lisaks märgime, et RAB-il ei ole praegu SIENA ühendust Europoliga info vahetamiseks. RAB ei ole seni otse Europoli päringutele vastanud.	Arvestatud. Täiendatud seletuskirja
6.	Justiits- ja Digiministeerium (ja Riigiprokuratuur)	
6.1	Leiame, et määruses tuleb sätestada selgemad nõuded Europoli töödeldavate andmete kvaliteedi ja automaatsete vastete	Arvestatud. Täiendatud seletuskirja (vt punktid 6.2 ja 7.6).

	<p>usaldusväärse tagamiseks. Kontrollimata või ebapiisava usaldusväärse andmed ei tohiks üksinda olla operatiivsete meetmete ega isikut mõjutavate otsuste aluseks. Määruses tuleb ette näha, et iga automaatse vastega kaasneb teave andmete allika, usaldusväärse, täpsuse, ajakohasuse ja kasutuspiirangute kohta. Samuti tuleb selgelt määrata Europoli ja andmed esitanud liikmesriigi vastutus andmete kontrollimise, parandamise, kustutamise ning valepositiivsete vastete kõrvaldamise eest.</p> <p>Arvestades ristkontrolliteenuse ulatust ja võimalust tuvastada uurimiste vahelisi seoseid, peab määrus tagama ka läbipaistvuse selles, kas seos on loodud ametniku või analüütiku hinnangu alusel või automaatse andmetöötlemise tulemusena.</p>	
6.2	<p>Leiame, et automaatse tabamus/mitte-tabamus-süsteemi ja Euroopa Prokuratuuriga teabevahetuse regulatsioon vajab täpsustamist eelkõige eesmärgipiirangu, andmete kvaliteedi ning vastutuse jaotuse osas. Selline erand peab olema rangelt piiritletud Euroopa Prokuratuuri pädevusse kuuluvate konkreetsete süütegudega ning sellega peavad kaasnema teabe esitaja teavitamine, edastamise põhjenduse dokumenteerimine ja võimalus kontrollida, kas edastamine oli vajalik ja proportsionaalne.</p> <p>Samuti tuleb täpsustada vastutuse jaotus olukorras, kus Europol edastab Euroopa Prokuratuurile või muule liidu asutusele liikmesriigi esitatud andmeid, mis osutuvad hiljem ebaõigeks, aegunuks või puudulikuks. Andmesubjekti õiguste tõhusaks tagamiseks peab olema arusaadav, millise asutuse poole saab isik pöörduda ning milline asutus teeb lõpliku otsuse andmetega tutvumise, parandamise, kustutamise või töötlemise piiramise kohta.</p>	Arvestatud. Täiendatud seletuskirja (vt punkt 7.6).
6.3	<p>Tuleb täpsustada tingimusi, mille alusel võib Europol edastada isikuandmeid eraõiguslikele isikutele, eelkõige väljaspool Euroopa Liitu asuvatele ettevõtjatele. Lisaks vajab selgemat reguleerimist teabevahetusplatvormi kasutamine. Kui sama platvormi kaudu toimub liikmesriikide, Europoli ja eraõiguslike isikute vaheline</p>	Arvestatud. Täiendatud seletuskirja

	andmevahetus, peab määrukses olema selgelt sätestatud, millal Europol tegutseb vastutava töötlejana ja millal volitatud töötlejana, millistel juhtudel on Europolil platvormi kaudu vahetatavatele andmetele juurdepääs ning kuidas tagatakse andmete eesmärgipärane kasutamine, logimine, juurdepääsupiirangud ja andmesubjekti õiguste teostamine.	
6.4	Leiame, et Europoli teadus- ja innovatsiooniprojektides, sh tehisintellekti süsteemide arendamisel, testimisel ja valideerimisel, ei peaks eriliiki isikuandmete kasutamine olema lubatud <u>üldise alusena</u> , vaid üksnes juhul, kui see on eraldi õiguslikult põhjendatud ja rangelt vajalik või kui tegemist on tahtmatu ja jäägina esineva andmega, mille suhtes kohaldatakse nn <i>Digital Omnibus</i> ’i ettepanekuga võrreldavaid kaitsemeetmeid.	Arvestatud. Täiendatud seletuskirja (vt punkt 7.8).
6.5	Teeme ettepaneku lisada määruksesse mõiste „ <i>operational personal data</i> “. Mõiste täpsustamine on vajalik, kuna sellest sõltub, millistele andmetele ja millises ulatuses kohalduvad määrukses ette nähtud töötlemisreeglid ja kaitsemeetmed. Ebaselge mõiste võib kaasa tuua erineva tõlgendamise ning Europoli andmetöötlushädevuse ebamäärase ulatuse.	Arvestatud osaliselt. (vt punkt 7.2).
6.6	Soovitame näha lisa II kategooriatest väljapoole jäävate isikute andmete töötlemisel ette täiendavad kaitsemeetmed (dokumenteeritud vajalikkuse hinnang, lühem kontrolliperiood, tehniline eraldamine ja aruandlus). Eesti seisukohtades seda teemat eraldi ei kajastata. Täiendavad kaitsemeetmed on vajalikud, sest selliste isikute seos kuritegevusega võib olla nõrk või üldse puududa ning nende andmete ulatuslik töötlemine suurendab põhjendamatu seostamise ja põhiõiguste riive riski.	Arvestatud. Täiendatud seletuskirja (vt punkt 7.3).
6.7	Peame vajalikuks täpsustada osalejate rolle isikuandmete töötlemisel, sealhulgas vastutust andmete õigsuse, andmesubjekti õiguste	Arvestatud. Täiendatud seletuskirja (vt punkt 7.3)

	<p>tagamise ning andmeruumis tehtud analüütiliste järelduste kasutamise eest. See ei ole Eesti seisukohtades otseselt kajastatud. Kuna ühises andmeruumis töötlevad andmeid mitu osalist ning andmeid võidakse omavahel seostada ja analüüsida, peab määrusest selgelt nähtuma, kes vastutab konkreetsete töötlemistoimingute ja nende tagajärgede eest.</p>	
6.8	<p>Teeme ettepaneku sätestada isikuandmete säilitamise absoluutne ülempiir ning diferentseeritud säilitamistähtajad. Üksnes perioodilise ülevaatamise kohustus ei pruugi tagada, et andmeid ei säilitata põhjendamatult kaua, eriti nende isikute puhul, kelle seos kuritegevusega on kaudne või kõrvaline.</p>	Arvestatud. Täiendatud seletuskirja (vt punkt 7.5).
6.9	<p>Juhime tähelepanu vajadusele täpsustada artiklis 102 liikmesriigi nõusoleku õiguslikku tähendust ning selgitada, milline pädev asutus sellise hinnangu annab ja milliste kriteeriumide alusel. Tuleks selgitada, kas nõusolekut on võimalik piirata või tagasi võtta ning kuidas mõjutab see juba alanud projekti ja selle käigus loodud tulemuste kasutamist. Küsimus vajab Eesti seisukohtades sisulisemat kajastamist, sest vastasel juhul võib liikmesriigi kontroll tema edastatud andmete kasutamise üle jääda üksnes formaalseks.</p>	Arvestatud. Täiendatud seletuskirja (vt punkt 7.8).