

Kriminaalmenetluse seadustiku, kriminaalmenetluse seadustiku rakendamise seaduse ning politsei ja piirivalve seaduse muutmise seaduse (teabevahetus Euroopa Liidu liikmesriikide vahel ja Europoliga) eelnõu seletuskiri

Sisukord

1. Sissejuhatus	3
1.1. Sisukokkuvõte	4
1.2. Eelnõu ettevalmistaja.....	5
1.3. Märkused	5
2. Seaduse eesmärk.....	7
2.1. Hetkeolukord ja kehtiv õigus.....	7
2.2. Eelnõu eesmärk ja kavandatud lahendus	10
2.3. Eelnõu põhiseaduspärasus	12
3. Eelnõu sisu ja võrdlev analüüs	18
1. alljaotis	19
Teabevahetuse üldreeglid	19
§ 508 ⁸⁵ . Teabevahetuse korraldus.....	19
§ 508 ⁸⁶ . Ühtne kontaktpunkt.....	26
§ 508 ⁸⁷ . Teabevahetuskanal.....	29
§ 508 ⁸⁸ . Edastatav teave.....	33
§ 508 ⁸⁹ . Teabekasutuse tingimused	37
2. alljaotis	38
Teabetaotlusele vastamine.....	38
§ 508 ⁹⁰ . Teabetaotlusele vastamine	38
§ 508 ⁹¹ . Teabeedastusest keeldumine.....	40
§ 508 ⁹² . Teabetaotlusele vastamise tähtaeg.....	45
§ 508 ⁹³ . Teabetaotluse vastuse koopia edastamine.....	47
3. alljaotis	49
Teabetaotluse esitamine.....	49
§ 508 ⁹⁴ . Teabetaotluse esitamine	49
§ 508 ⁹⁵ . Nõuded teabetaotlusele	50
4. alljaotis	51
Omaalgatuslik teabeedastus.....	51
§ 508 ⁹⁶ . Omaalgatuslik teabeedastus	51
5. alljaotis	54
Teabeedastus Europolile.....	54

§ 508 ⁹⁷ . Teabeedastus Europolile	54
Eelnõu § 2. KrMSRS-i täiendamine	56
Eelnõu § 3. PPVS-i muudatused.....	56
§ 25 ⁸ . Ühtse kontaktpunkti ülesanded	57
§ 25 ⁹ . Töövoosüsteem	57
§ 25 ¹⁰ . Töövoosüsteemi andmed	61
§ 25 ¹¹ . Töövoosüsteemi andmete säilitamine	63
4. Eelnõu terminoloogia	65
5. Eelnõu vastavus Euroopa Liidu õigusele.....	65
6. Seaduse mõjud.....	65
7. Seaduse rakendamisega seotud riigi ja kohaliku omavalitsuse tegevused, eeldatavad kulud ja tulud.....	77
7.1. Ühtne kontaktpunkt	77
7.2. IT-arendused.....	78
7.3. Koolituskulud	79
8. Rakendusaktid	80
9. Seaduse jõustumine	81
10. Eelnõu koostööstamine, huvirühmade kaasamine ja avalik konsultatsioon	81

Kriminaalmenetluse seadustiku, kriminaalmenetluse seadustiku rakendamise seaduse ning politsei ja piirivalve seaduse muutmise seaduse (teabevahetus Euroopa Liidu liikmesriikide vahel ja Europoliga) eelnõu seletuskiri

1. Sissejuhatus

1.1. Sisukokkuvõte

Kavandatava eelnõuga võetakse üle kaks direktiivi:

1. Euroopa Parlamendi ja nõukogu direktiiv 2023/977, mis käsitleb liikmesriikide õiguskaitseasutuste vahelist teabevahetust ja millega tunnistatakse kehtetuks nõukogu raamotsus 2006/960/JSK (edaspidi *Rootsi direktiiv*)¹;
2. Euroopa Parlamendi ja nõukogu direktiiv 2023/2123, millega muudetakse nõukogu otsust 2005/671/JSK, et viia see vastavusse isikuandmete kaitset käsitlevate liidu õigusnormidega (edaspidi *direktiiv 2023/2123*).

Selleks et Rootsi direktiivi nõuded Eesti õigusesse üle võtta, muudetakse [kriminaalmenetluse seadustikku](#) (edaspidi *KrMS*), [kriminaalmenetluse seadustiku rakendamise seadust](#) (edaspidi *KrMSRS*) ning [politsei ja piirivalve seadust](#) (edaspidi *PPVS*).

Rootsi direktiivi kohaselt peavad kõik Euroopa Liidu (edaspidi *EL*) liikmesriikide õiguskaitseasutused vahetama teavet, mis on vajalik süütegude tõkestamiseks, avastamiseks või uurimiseks (edaspidi ka *kriminaalteave*²). Teabevahetus toimub üldjuhul ööpäev läbi töötavate ühtsete kontaktpunktide kaudu.³ Kõigi EL-i liikmesriikide ühtsetele kontaktpunktidele nähakse ette ühesugused reeglid, ülesanded ja tähtajad, mille jooksul tuleb teise liikmesriigi teabetaotlejale vastata. Samuti peavad liikmesriigid tagama teabevahetuse toimumise reeglina selleks ette nähtud Euroopa Liidu Õiguskaitsekoostöö Ameti⁴ (edaspidi *Europol*) hallatava turvalise teabevahetusvõrgu⁵ (edaspidi *SIENA*) kaudu. Uudsenä nähakse ette, et SIENA kaudu vahetatav rasket kuritegevust puudutav teave peab jõudma lisaks EL-i liikmesriikidele ka Europolini, kes saab seda kasutada oma analüüside koostamisel.

Eelnõuga kavandatud muudatused omavad positiivset mõju siseturvalisusele. Eesmärkide täitmisel tiheneb koostöö naaberriikide õiguskaitseasutustega, avanevad uued koostöövõimalused ning täienevad meetmed võitluses kuritegevusega. Kui politseiametnikele

¹ Euroopa Parlamendi ja nõukogu direktiiv 2023/977, mis käsitleb liikmesriikide õiguskaitseasutuste vahelist teabevahetust ja millega tunnistatakse kehtetuks nõukogu raamotsus 2006/960/JSK ([ELT L 134, 22.5.2023, lk 1–24](#)).

² Clarke, V., Eck, J. Probleemikeskseks kriminaalanalüütikuks 55 lihtsa sammuga. Tallinn 2006, lk 26. Kättesaadav: <https://popcenter.asu.edu/sites/default/files/kasiraamat.pdf>.

³ Selgitus: ühtne kontaktpunkt on riiklik teabekeskus, mis tegeleb teabe vastuvõtmise, töötlemise ja teistele riikidele saatmisega. See koondab samasse haldusstruktuuri kõik peamised rahvusvahelised ja liidu õiguskaitsealase teabe vahetamise kanalid (Interpol, Europol ja SIRENE).

⁴ Europoli tegevustest saab ülevaate Europoli veebilehel: <https://www.europol.europa.eu/about-europol:et>.

⁵ Euroopa Parlamendi ja nõukogu 11. mai 2016. aasta määrus (EL) 2016/794, mis käsitleb Euroopa Liidu Õiguskaitsekoostöö Ametit (Europol) ning millega asendatakse ja tunnistatakse kehtetuks nõukogu otsused 2009/371/JSK, 2009/934/JSK, 2009/935/JSK, 2009/936/JSK ja 2009/968/JSK ([ELT L 135, 24.5.2016, lk 53–114](#)).

antakse juurde digivahendeid, mis toovad otsest ja vahetut kasu operatiivtasandile, suureneb siseturvalisuse pakkumine EL-i kodanikele.

KrMSRS-i täiendatakse sättega, kus nähakse uurimisasutustele ette erisus SIENA kasutamises kuni 2027. aasta 12. juunini. Kõik uurimisasutused ei ole praegu SIENA-ga ühendatud, mistõttu võib olla vaja teha nii tehnilisi ettevalmistusi kui ka vajadusel sõlmida andmetöötluslepingud. Selleks tuleb ette näha pikem tähtaeg võrreldes KRMS-is sätestatava SIENA kasutamisega alates 2024. aasta 12. detsembrist.

Ülevõetava direktiiviga 2023/2123 muudeti nõukogu otsust 2005/671/JSK⁶ (edaspidi *otsus*), et viia see kooskõlla tänapäevaste EL-i isikuandmete kaitse reeglitega ning tagada terrorismiga seotud teabevahetuse õiguspärasus ja proportsionaalsus.

Direktiivi 2023/2123 ülevõtmisel on tegemist tehnilise muudatusega, millega täpsustatakse Europolile edastatavate isikuandmete ja andmesubjektide kategooriad, tagades, et andmevahetus piirdub üksnes Europoli eesmärkide saavutamiseks vajaliku teabega.

Vabariigi Valitsuse 22. detsembri 2011. aasta määruses nr 180 „Hea õigusloome ja normitehnika eeskiri“ on sätestatud, et kui eelnõuga kavandatavate nõuete tõttu kasvab ettevõtjate, inimeste või vabaühenduste halduskoormus, nähakse ette muudatused ka halduskoormuse vähendamiseks. Käesoleva eelnõuga ettevõtjate, inimeste ega vabaühenduste halduskoormus ei kasva.

Eelnõu seadusena jõustumine nähakse ette üldises korras.

1.2. Eelnõu ettevalmistaja

Eelnõu ja seletuskirja on koostanud Siseministeeriumi nõunik Ott Aarma (ott.aarma@siseministeerium.ee) ja õigusnõunik Marju Aibast (marju.aibast@siseministeerium.ee) koostöös Politsei- ja Piirivalveameti (edaspidi *PPA*) esindajatega. Eelnõu ja seletuskirja juriidilist kvaliteeti on kontrollinud Marju Aibast.

Direktiiviga 2023/2123 seonduva osa on ette valmistanud Justiits- ja Digiministeeriumi kriminaalkoostöö ja õigusloome talituse nõunik Mari Keskküla (mari.keskkyla@justdigi.ee, tel 5877 9915).

Eelnõu ja seletuskirja on keeleliselt toimetanud Luisa Keelelahenduste eesti keele vanemtoimetaja Tiina Alekõrs (tiina@luisa.ee).

1.3. Märkused

Eelnõuga võetakse üle Rootsi direktiiv ja direktiiv 2023/2123. Rootsi direktiivi artikli 22 lõike 1 kohaselt pidid EL-i liikmesriigid jõustama direktiivi järgimiseks vajalikud õigus- ja haldusnormid hiljemalt **12. detsembriks 2024. aastal**. SIENA kasutuselevõttu puudutavad õigus- ja haldusnormid peavad EL-i liikmesriigid jõustama hiljemalt **12. juuniks 2027. aastal**. Direktiiv 2023/2123, millega tagatakse vastavus direktiiviga (EL) 2016/680 (edaspidi

⁶ Euroopa Liidu Nõukogu 20. septembri 2005. aasta otsus 2005/671/JSK terroriaktidega seotud teabevahetuse ja koostöö kohta ([ELT L 253/22, 29.9.2005](https://eur-lex.europa.eu/eli/dec/2005/671/oj)).

õiguskaitse direktiiv)⁷ ning Europoli õigusraamistikku reguleeriva määrusega (EL) 2016/794⁸ (edaspidi *Europoli määrus*), sätestades kohustuse vahetada Europoliga isikuandmeid terrorismi ja muude Europoli pädevusse kuuluvate kuritegude ennetamise, uurimise, avastamise ja vastutusele võtmise eesmärgil kooskõlas EL-i andmekaitse nõuetega, tuli liikmesriikidel riigisisesse õigusesse üle võtta hiljemalt 1. novembriks 2025. aastal. Eelnõu ei ole seotud Vabariigi Valitsuse tegevusprogrammiga ega muu menetluses oleva eelnõuga.

Eelnõu on kooskõlas „Siseturvalisuse arengukava 2020–2030“⁹ meetme „Kindel sisejulgeolek“ eesmärkidega, mille kohaselt on Eesti sisejulgeolekut ohustavad tegurid hästi teadvustatud ja maandatud mitmesuguste riigisiseste tegevuste ning rahvusvahelise koostöö kaudu.

Eelnõuga kavandatud muudatused aitavad saavutada dokumendis „Kriminaalpoliitika põhialused aastani 2030“¹⁰ kirjeldatud eesmärki, keskenduda ühiskonnale kõige enam kahju tekitavate õigusrikkumiste ärahoidmisele, eelkõige küber-, majandus-, korruptsiooni-, narko-, inimkaubanduse ja vägivalda ennetamisele ning organiseeritud kuritegevuse tõkestamisele. Samuti toetavad need samas dokumendis kirjeldatud eesmärki teha rahvusvahelist koostööd ning kasutada tehnoloogiat õigusrikkumiste prognoosimisel, ärahoidmisel ja avastamisel ning ekspertiiside läbiviimisel. Eelnõu koostamisel on peetud silmas ka nõukogu järeldusi, millega on määratud kindlaks EL-i prioriteedid võitluseks raske ja organiseeritud kuritegevusega Euroopa multidistsiplinaarse kuritegelike ohtude vastu võitlemise platvormi (edaspidi *EMPACT*)¹¹ raames aastateks 2022–2025.¹²

Ühtlasi toetavad kavandatavad muudatused 2021. aastal valminud Justiits- ja Digiministeeriumi ning Siseministeeriumi valitsemisalas süüteomenetluse digitaliseerimise ühise tegevuskava elluviimist. Ka selles on piiriülene andmevahetus toodud välja ühe koostöö kitsaskohana.¹³ Samuti on eelnõuga kavandatavad muudatused kooskõlas raamdokumendiga „Eesti Euroopa Liidu poliitika prioriteedid 2022–2023“¹⁴, mille järgi peab EL-i politseikoostöö seadustik lihtsustama piiriülest politseikoostööd.

Eelnõu ettevalmistamiseks moodustas Siseministeerium töörühma, kuhu lisaks Siseministeeriumi valitsemisala asutuste esindajatele kuulusid esindajad Justiits- ja Digiministeeriumi, Kaitseministeeriumi, Kliimaministeeriumi ja Rahandusministeeriumi valitsemisala asutustest (uurimisasutustest). Eelnõu esitati töörühma liikmetele tutvumiseks ja tagasiside andmiseks 2024. aasta juunis. Esitatud tagasiside on võetud arvesse eelnõu lõpliku versiooni koostamisel.

⁷ Vt. lähemalt Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK ([ELT L 119, 4.5.2016, lk 89](#)).

⁸ Euroopa Parlamendi ja Nõukogu 11. mail 2016. aasta määrus (EL) 2016/794, mis käsitleb Euroopa Liidu Õiguskaitsekoostöö Ametit (Europol) ning millega asendatakse ja tunnistatakse kehtetuks nõukogu otsused 2009/371/JSK, 2009/934/JSK, 2009/935/JSK, 2009/936/JSK ja 2009/968/JSK ([ELT L 135, 24.5.2016, lk 53–114](#)).

⁹ Vt lähemalt: <https://www.siseministeerium.ee/stak2030>.

¹⁰ Vt lähemalt: <https://www.just.ee/kuritegevus-ja-selle-ennetus/kriminaalpoliitika-pohialused>.

¹¹ Vt EMPACT-i tegevuste kohta lähemalt: <https://www.europol.europa.eu/crime-areas-and-statistics/empact>.

¹² Vt lähemalt: <https://data.consilium.europa.eu/doc/document/ST-8665-2021-INIT/et/pdf>

¹³ Vt lähemalt: <https://www.just.ee/uudised/suuteomenetlus-muutub-digitaalseks-ning-asjatut-burokraatiat-valtivaks>.

¹⁴ Vt lähemalt: <https://riigikantselei.ee/el-poliitika-julgeolek-ja-riigikaitse/eesti-euroopa-liidu-poliitika/el-poliitika>.

Eelnõu kohaselt muudetakse:

- KrMS-i 6. juulil 2025. aastal jõustunud redaktsiooni avaldamismärkega RT I, 05.07.2025, 14;
- KrMSRS-i 27. aprillil 2025. aastal jõustunud redaktsiooni avaldamismärkega RT I, 17.04.2025, 8;
- PPVS-i 6. juulil 2025. aastal jõustunud redaktsiooni avaldamismärkega RT I, 26.06.2025, 12.

Enne eelnõu koostamist väljatöötamiskavatsust ei koostatud, sest eelnõus käsitletakse EL-i õiguse rakendamist ja eelnõu aluseks oleva EL-i õigusakti eelnõu¹⁵ menetlemisel on sisuliselt lähtutud Vabariigi Valitsuse 22. detsembri 2011. aasta määruse nr 180 „[Hea õigusloome ja normitehnika eeskiri](#)“¹⁶ (edaspidi *HÕNTE*) § 1 lõikes 1 sätestatud nõuetest ning arvestatud *HÕNTE* § 1 lõike 2 punktis 2 toodud võimalust loobuda eelnõu väljatöötamiskavatsuse koostamisest, sest eelnõus käsitletakse EL-i õiguse rakendamist ja eelnõu aluseks oleva EL-i õigusakti eelnõu menetlemisel on sisuliselt lähtutud *HÕNTE* § 1 lõikes 1 sätestatud nõuetest. [Vabariigi Valitsuse seisukohad](#) Rootsi direktiivi suhtes kinnitati 13. aprillil 2022. aastal.

Kuna Rootsi direktiivis sätestatakse miinimumnõuded, mis on vajalikud õiguskaitseasutuste vahelise tõhusa ja kiire teabevahetuse tagamiseks, puudub EL-i liikmesriikidel kaalutlusruum leebemate nõuete kehtestamiseks. Ehkki EL-i liikmesriikidele on jäetud võimalus miinimumnõudeid¹⁷ vastavalt oma õiguskaitseüsteemide eripäradele kohandada või veelgi tõhustada, on Rootsi direktiivi ning direktiivi 2023/2123 ülevõtmisel lähtutud eelnõus seaduse sisulise kohaldamisala sätestamisel direktiivi miinimumreeglitest.¹⁸

Eelnõu vastuvõtmiseks on vaja [Eesti Vabariigi põhiseaduse](#) (edaspidi *PS*) § 104 lõike 2 punkti 14 kohaselt **Riigikogu koosseisu häälteenamust**, sest muudetakse KrMS-i.

2. Seaduse eesmärk

2.1. Hetkeolukord ja kehtiv õigus

EL-i sisepiirikontrollita ala (edaspidi *Schengeni ala*¹⁹) on suurim vaba reisimise piirkond kogu maailmas. See võimaldab enam kui 420 miljoni inimese vaba liikumist ning takistuseta kauba- ja teenusevoogusid. Samuti toob see kaasa turvalisusega seotud probleeme, kuna vaba liikumise õigust kasutavad oskuslikult ära ka kurjategijad, et oma kuritegevust piiriüleselt laiendada.

¹⁵ Euroopa Komisjoni ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb liikmesriikide õiguskaitseasutuste vahelist teabevahetust ja millega tunnistatakse kehtetuks nõukogu raamotsus 2006/960/JSK. Kättesaadav: <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52021PC0782>.

¹⁶ Vabariigi Valitsuse 22. detsembri 2011. aasta määrus nr 180 „[Hea õigusloome ja normitehnika eeskiri](#)“ – [RT I, 22.05.2025, 8](#).

¹⁷ Selgitus: näiteks on EL-i liikmesriikidele jäetud kaalutlusruum kehtestada täiendavad andmekaitsemeetmed, mis on kooskõlas EL-i üldiste andmekaitsenormidega; sätestada riigisisest või kahe- ja mitmepoolsete lepingute abil vastamiseks veelgi lühemaid tähtaegu või laiemat süütegude ringi (näiteks väärted), mille puhul teavet vahetatakse.

¹⁸ Euroopa Komisjoni mõjuanalüüs Euroopa Parlamendi ja nõukogu direktiivi kohta, mis käsitleb liikmesriikide õiguskaitseasutuste vahelist teabevahetust ja millega tunnistatakse kehtetuks nõukogu raamotsus 2006/960/JSK. Kättesaadav: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021SC0374>.

¹⁹ Selgitus: Schengeni ala koosneb 26 Euroopa riigist: Austria, Belgia, Eesti, Hispaania, Island, Itaalia, Kreeka, Leedu, Liechtenstein, Luksemburg, Läti, Madalmaad, Malta, Norra, Poola, Portugal, Prantsusmaa, Rootsi, Saksamaa, Slovakkia, Sloveenia, Soome, Šveits, Taani, Tšehhi Vabariik ja Ungari.

EL-i ja Schengeni viisaruumi laienemise, eeskätt isikute vaba liikumise ala suurenemise ja riikidevaheliste piirikontrollide kaotamise tõttu on kuritegevus muutunud aina rohkem piiriüleseks. Selleks et EL suudaks enda kodanikele tagada [EL-i toimimise lepingu](#) V jaotises nimetatud vabadusel, turvalisusel ja õigusel põhineva ala, on oluline liikmesriikide õiguskaitseasutuste²⁰ vaheline tihe koostöö. Teabevahetus on selle koostöö üks olulisemaid aspekte, kuna võimaldab ohtusid kiiresti tuvastada ja neile reageerida. Senine praktika näitab, et riiklikud ja piirkondlikud meetmed, nagu kahe- ja mitmepoolsed kokkulepped, ei taga piisavat teabevahetust. Samuti on ühtsete kontaktpunktide (kehtivas KrMS-is rahvusvahelise koostöö keskasutus) korralduses märkimisväärsed erinevusi, mis takistavad tõhusat koostööd. Ühtsete reeglite ja juhisteta ei suuda EL-i liikmesriigid tagada ühtset teadlikkust ega suutlikkust kasutada vajalikke andmebaase ning sidekanaleid. Teabevahetust käsitlevad ühiseeskirjad loodi selleks, et parandada õiguskaitseasutuste koostööd ja tõhusust.

EL-i julgeolekuliidu strateegias²¹ on sedastatud, et EL-il tuleb vastakuti seista pidevalt muutuvate ja üha keerukamate julgeolekuohtudega. EL-i raske ja organiseeritud kuritegevuse põhjustatud ohtude 2021. aasta hinnangu²² (edaspidi *SOCTA*) kohaselt iseloomustab organiseeritud kuritegevust võrgustike keskkond, kus kurjategijatevaheline koostöö on kiiresti muutuv, süstemaatiline ja tulu saamisele orienteeritud. Peaaegu 70% kuritegelikest võrgustikest tegutseb enam kui kolmes EL-i liikmesriigis ning ligikaudu 65% EL-i liikmesriikides tegutsevatest kuritegelikest võrgustikest koosneb mitme riigi kodanikest. Üle 80% kuritegelikest võrgustikest on seotud peamiste piiriüleste kuritegudega, nagu uimastikaubandus, varavastased kuriteod, inimkaubandus ja sisserändajate ebaseaduslik üle piiri toimetamine.²³ Kuritegevusmaastiku kiire muutumise ja inimeste liikuvuse tõttu on õiguskaitseasutuste piiriülene koostöö EL-is ja Schengeni alal ülioluline, et võidelda kuritegevuse vastu ning võimaldada EL-i kodanikel ja seaduslikult EL-is viibivatel kolmandate riikide kodanikel kasutada turvaliselt oma vaba liikumise õigust. Selleks tuleb jätkuvalt edendada õiguskaitseasutuste suutlikkust vahetada tõhusalt ja tulemuslikult teavet teiste liikmesriikide õiguskaitseasutustega. Rootsi direktiivi eesmärk ongi tagada piisav ja kiire teabevahetus pädevate õiguskaitseasutuste vahel ning Europoliga, toetades seeläbi liikmesriike võitluses raske ja organiseeritud kuritegevuse vastu.

Õiguskaitsealase koostöö kaks põhiharu on teabevahetus ja piiriülene operatiivkoostöö. EL-i liikmesriikide vahelist teabevahetust, mille eesmärk on tõkestada ja avastada süütegusid, reguleeritakse 19. juunil 1990. aastal vastu võetud konventsiooniga, millega rakendatakse 14. juuni 1985. aasta Schengeni lepingut²⁴, eelkõige selle artikleid 39 ja 46. Nõukogu raamotsusega 2006/960/JSK²⁵ (edaspidi *Rootsi raamotsus*) asendati need sätted osaliselt ning kehtestati uued normid teabe ja jälitusteabe vahetamiseks pädevate õiguskaitseasutuste vahel. Need EL-i õigusaktidest tulenevad regulatsioonid võeti Eesti õigusesse esimest korda üle 1. juulil 2014. aastal jõustunud kriminaalmenetluse seadustiku ja sellega seonduvalt teiste

²⁰ Selgitus: terminit „õiguskaitseasutus“ kasutatakse eelnõu järgi KrMS-is, viidates teise EL-i liikmesriigi vastavale asutusele. Üksnes Eesti vastava asutuse puhul kasutatakse läbivalt terminit „uurimisasutus“.

²¹ Vt lähemalt <https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52020DC0605&from=ET>.

²² Vt lähemalt: <https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021>.

²³ Europol (2021), European Union serious and organised crime threat assessment, a corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, Euroopa Liidu Väljaannete Talitus, Luksemburg.

²⁴ Konventsioon, millega rakendatakse 14. juuni 1985. aasta Schengeni lepingut Beneluxi Majandusliidu riikide, Saksamaa Liitvabariigi ja Prantsuse Vabariigi valitsuste vahel nende ühispiiridel kontrolli järkjärgulise kaotamise kohta ([EÜT L 239, 22.9.2000, lk 19](#)).

²⁵ Nõukogu 18. detsembri 2006. aasta raamotsus 2006/960/JSK Euroopa Liidu liikmesriikide õiguskaitseasutuste vahelise teabe ja jälitusteabe vahetamise lihtsustamise kohta ([ELT L 386, 29.12.2006, lk 89](#)).

seaduste muutmise seadusega²⁶. Teabe ja jälitustoiminguga kogutud teabe vahetamine EL-i liikmesriikide vahel on sätestatud kehtiva KrMS-i 19. peatüki 8. jao 9. jaotises. See põhineb Rootsi raamotsusel, mis näeb EL-i liikmesriikidele ette kohustuse sellist teavet vahetada. Ühtlasi põhineb see KrMS-i peatükk [nõukogu soovitusel 2022/915 õiguskaitsealase operatiivkoostöö kohta](#) (edaspidi *operatiivkoostöö soovitus*)²⁷, millega sätestatakse õiguslikult mittesiduv juhised, kuidas teabevahetus peaks praktikas toimuma.

Rootsi direktiiv on osa politseikoostöö seadustiku paketist²⁸, kuhu lisaks Rootsi direktiivile kuuluvad 2022. aastal vastu võetud politsei operatiivkoostöö soovitus²⁹ ja määrus³⁰, millega täiendatakse politseikoostöös kasutatava automatiseeritud andmevahetusmehhanismi (edaspidi *Prüm II*) kasutusvõimalusi ning mille eesmärk on tugevdada nõukogu otsuse 2008/615/JSK (piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega (edaspidi *Prümi otsus*)³¹) kohase teabevahetuse tehnilist ülesehitust, hõlmata sellega rohkem andmekategooriaid ning ühtlustada ja kiirendada päringutabamuse järgset teabevahetust. Rootsi direktiivi eesmärk on siduda Rootsi raamotsuses ja operatiivkoostöö soovitusel sisaldunud põhimõtted ning muuta nende järgimine liikmesriikidele kohustuslikuks. Rootsi direktiivis ei nähta ette uudseid põhimõtteid võrreldes Rootsi raamotsuses või operatiivkoostöö soovitusel tooduga.

Kuna Rootsi direktiiv puudutab kuritegude kohtueelset menetlemist kõikide uurimisasutuste poolt, on kavas direktiivist tulenevad reeglid sätestada ka edaspidi KrMS-is selleks, et kõikidele KrMS § 31 lõikes 1 nimetatud uurimisasutustele (edaspidi *uurimisasutus*) oleks direktiivist tulenevad kohustused üheselt selged ja lihtsalt leitavad.

Kuigi direktiivikohane teabevahetus puudutab ka kriminaalmenetluse eelset teabevahetust, mis ei peaks olema ilmtingimata sätestatud KrMS-is, räägib viimase kasuks asjaolu, et vahetatav on lahutamatu seotud Eestis või teises EL-i liikmesriigis läbiviidava või algatatava kriminaalmenetlusega. Teabevahetuse aluseks peab olema kas toimepandud, kavandatav või eesseisev kuritegu, mistõttu on teabevahetuse käigus saadav või edastatav teave suure tõenäosusega kas KrMS § 194 lõikes 1 sätestatud kriminaalmenetluse alustamise ajend või puudutab juba käimasolevat kriminaalmenetlust. Seetõttu on ka kehtiva KrMS § 1 lõike 1 kohaselt kuritegude kohtueelse menetluse kord reguleeritud KrMS-is. Samuti on KrMS § 508⁷⁸ lõikes 1 sätestatud EL-i liikmesriikide õiguskaitseasutuste vaheline teabevahetus süütegude avastamise ja tõkestamise faasis ehk kohtueelse menetluse etapis. Selline regulatsioon on vajalik selleks, et tagada kohtus hinnatavate tõendite kujunemise protsessi läbipaistvus ning õiguspärasuse ja usaldusväärsuse kontrollitavus.

Asjaolu, et Rootsi direktiivi kohase teabevahetuse alusel saadud teavet ei ole vaikumisi lubatud kasutada menetluses tõendina, ei tähenda, et reguleeritava teabevahetuse raames vahetataks kriminaalmenetlusega mitteseotud teavet. Põhimõtet tuleb mõista selliselt, et ehkki tegemist ei ole tõendusteabe vahetamise põhiinstrumendiga – vastav teave tuleb endiselt taotleda Euroopa

²⁶ [Kriminaalmenetluse seadustiku ja sellega seonduvalt teiste seaduste muutmise seadus](#) (RT I, 21.06.2014, 11).

²⁷ Nõukogu 9. juuni 2022. aasta soovitus (EL) 2022/915 õiguskaitsealase operatiivkoostöö kohta ([ELT L 158, 13.6.2022, lk 53](#)).

²⁸ Vt lähemalt https://ec.europa.eu/commission/presscorner/detail/et/ip_21_6645.

²⁹ Nõukogu 9. juuni 2022. aasta soovitus (EL) 2022/915 õiguskaitsealase operatiivkoostöö kohta ([ELT L 158, 13.6.2022, lk 53](#)).

³⁰ Euroopa Parlamendi ja nõukogu määrus (EL) 2024/982, milles käsitletakse politseikoostöö raames toimuvat automatiseeritud andmete otsingut ja vahetust ning millega muudetakse nõukogu otsuseid 2008/615/JSK ja 2008/616/JSK ning Euroopa Parlamendi ja nõukogu määruseid (EL) 2018/1726, (EL) 2019/817 ja (EL) 2019/818 (*Prüm II* määrus) ([ELT L, 2024/982, 5.4.2024](#)).

³¹ Nõukogu 23. juuni 2008. aasta otsus 2008/615/JSK piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega ([ELT L 210, 6.8.2008, lk 1–11](#)).

uurimismääruse (edaspidi *EIO*) abil –, on Rootsi direktiivi kohane teabetaotlus sihistatud EIO alus. Samuti võib Rootsi direktiivi kohases vastuses ette näha, et vahetatavat teavet võib kasutada kohtumenetluses tõendina. See vähendab oluliselt asutuste töökoormust, võimaldades saada EIO-ga samalaadse tulemuse vähem bürokraatlikult, ent seejuures põhiõigusi austavalt ja kiiremini.

Direktiiviga 2023/2123 rakendatakse Rootsi direktiivi põhimõtteid terrorismi puudutava teabe vahetamisele. Eriregulatsiooni vajadus tuleneb terrorismialase teabe eripärast – selline teave ei piirdu üksnes kriminaalteabega, vaid hõlmab ka andmeid, mida vahetatakse ohutõrjelisel eesmärgil.

Terrorismialase teabe vahetus toimub sageli ohutõrje faasis, mil terrorismikuriteo toimepanemise oht on olemas, kuid kriminaalmenetluse lävend ei ole veel ületatud. Näiteks võib vahetatav teave käsitleda radikaliseerumisiilminguid või isikuid, kelle käitumisest saab objektiivselt järeldada tõsist ohtu, kuigi nad ei ole veel toime pannud kuritegu. Selline varajane teabevahetus on vajalik, et ennetada võimalikke kahjusid ning reageerida ohule enne selle realiseerumist, enne kriminaalmenetluse alustamiseks aluse esinemist.

Terrorismialase teabe vahetamisel tuleb selgelt eristada, kas tegemist on ohutõrjelise või kriminaalmenetlusliku teabega, et tagada teabele asjakohane õigusraamistik, mis võtab arvesse teabes kajastatud isikute isikuandmete ja põhiõiguste kaitse nõudeid. Selleks tuleb tagada, et Europolile edastatav teave vastaks Europoli määruse (EL) 2016/794 II lisas sätestatud kriteeriumidele, mis määratlevad andmekategooriad ja andmesubjektide liigid, ning et oleks selgelt eristatav, millisel õiguslikul alusel teavet vahetatakse. Nii tagatakse, et teabevahetus on proportsionaalne ja kooskõlas isikute põhiõigustega, sealhulgas mõtte-, sõna- ja eneseteostusvabadusega.

Eriregulatsiooni vajadus tuleneb ka asjaolust, et terrorismialase teabe vahetamises võivad osaleda lisaks uurimisasutustele ka julgeolekuasutused. Kui kriminaalteabe vahetus piirdub tavapäraselt uurimisasutustega, siis terrorismialase teabe vahetamine hõlmab laiemat asutuste ringi. Eestis on Kaitsepolitseiametil (edaspidi *KAPO*) seadusest tulenevalt kaksikroll – asutus võib osaleda teabevahetuses vastavalt ohu realiseerumise tõenäosusele nii julgeoleku- kui ka uurimisasutusena. Seetõttu on vajalik reguleerida terrorismialase teabe vahetuse põhimõtted selliselt, et need hõlmaks mõlemad olukorrad ning tagaksid ühtse, õiguspärase ja andmekaitsealastele vastava praktika.

2.2. Eelnõu eesmärk ja kavandatud lahendus

Seaduseelnõu eesmärk on võtta Eesti õigusesse üle Rootsi direktiiv ja täpsustada KrMS-i regulatsiooni, et see vastaks Rootsi direktiivis sätestatud nõuetele ning Eesti õiguses oleks õiguskaitsealast koostööd, teabevahetust ja piiriülest operatiivkoostööd tõhustavad reeglid asjakohaselt sätestatud.

KrMS-i muudatustega:

- sätestatakse ühtsele kontaktpunktile ja uurimisasutusele kohustus vahetada kriminaalteavet, sealhulgas rasket kuritegevust puudutavat kriminaalteavet omal algatusel, teiste EL-i liikmesriikide õiguskaitseasutuste ja Europoliga selleks, et tagada EL-i liikmesriikidel olemasoleva teabe jõudmine osapoolteni, keda see teave puudutab või kellel võib sellest kuritegude ennetamisel, avastamisel, tõkestamisel või uurimisel kasu olla;
- koondatakse kogu uurimisasutuste ja EL-i liikmesriikide vaheline teabevahetus SIENA-sse;

- tugevdatakse ühtse kontaktpunkti rolli rahvusvahelise teabevahetuse koordineerijana selleks, et tagada teabevahetuse nõuetekohasus, sujuvus, kiirus ja korralduse selgus. Sellega seoses sätestatakse uurimisasutusele kohustus edastada teabevahetuse koopia alati ka ühtsele kontaktpunktile;
- seatakse selged ja proportsionaalsed tähtajad liikmesriikidevahelisele teabevahetusele, mis võtavad arvesse taotluse kiireloomulisust ja uurimisasutuse juurdepääsu teabele.

PPVS-i muudatustega tagatakse KrMS-i regulatsiooni rakendamisel kasutatava elektroonilise töövoosüsteemi ja statistika kogumist puudutav regulatsioon.

PPVS-i muudatustega:

- nähakse ette teabe vahetamise ühtse kontaktpunkti ülesanded;
- sätestatakse ühtsele kontaktpunktile kohustus koguda teabevahetuse kohta üksikasjalikku statistikat ja edastada see kord aastas Euroopa Komisjonile, et oleks võimalik järgida Rootsi direktiivist tulenevate nõuete järgimist, aga ka tõhustada protsesse ning likvideerida praktikas tõusetuda võivaid probleemkohti;
- nähakse ette teabevahetuse ja selle kohta kogutavate andmete automatiseerimine ning juhtumite haldamine töövoosüsteemis.

Eeltoodu on vajalik riigisisest kohustuste tekkimiseks, aga ka avalikkuse teadlikkuse suurendamiseks sellest, milliseid meetodeid ja vahendeid uurimisasutused EL-is vabadusel, turvalisusel ja õigusel rajaneva ala tagamiseks kasutavad ning millised isikuõiguste riivid sellega kaasnevad. Eeltoodu peaks heidutama ka kuritegelikke ühendusi ehk täitma üldpreventiivset funktsiooni.

Rootsi direktiivi üks alameesmärk on käsitleda EL-i õiguskaitseasutuste vahelise teabevahetuse korralduslikke ja menetluslikke aspekte, et tagada tõhus ja tulemuslik teabevahetus, millega kaitsakse täielikult toimivat ja vastupidavat Schengeni ala. Selleks kehtestatakse pädevate õiguskaitseasutuste vahelise piisava ja kiire teabevahetuse ühtlustatud normid kuritegude tõkestamiseks, avastamiseks või menetlemiseks.

Rootsi direktiivi teine alameesmärk on tagada mis tahes EL-i liikmesriigi õiguskaitseasutuste samaväärne juurdepääs teistes EL-i liikmesriikides kättesaadavale teabele, et avastada kuritegusid, viia läbi kriminaalmenetlusi või kuritegevuse vastaseid operatsioone, järgides põhiõigusi, sealhulgas andmekaitseõigusi. Praegu takistavad riikide tasandil kehtestatud eeskirjad tõhusat ja tulemuslikku teabevahetust.

Rootsi direktiiviga muudetakse kohustuslikuks EL-i liikmesriikide õiguskaitseasutuste vahelise teabe ja jälitusteabe operatiivset vahetamist siiani reguleerinud Rootsi raamotsuse sätted ning nende rakendamist puudutavad operatiivkoostöö soovituselised sätted.

Rootsi direktiivi kohaselt peavad EL-i liikmesriikide infovahetuse ühtsed kontaktpunktid töötama ööpäev läbi.³² Ühtsele kontaktpunktile nähakse ette ühtsed reeglid, ülesanded ja aeg, mille jooksul tuleb teise liikmesriigi teabetaotlusele vastata. Samuti peavad liikmesriigid kindlustama, et infovahetus toimub reeglina SIENA kaudu ning et vahetatav teave, mis puudutab rasket kuritegevust, jõuab ka Europolini, kes saab seda kasutada oma analüüsitoodete koostamisel. Varem on EL-i liikmesriikidel olnud suurem võimalus valida ise infovahetuseks sobivaimad kanalid ja neist tulenevalt teabetaotlusele vastamise aeg. Liikmesriigid kasutavad

³² Selgitus: ühtne kontaktpunkt on riiklik teabekeskus, mis tegeleb teabe vastuvõtmise, töötlemise ja teistele riikidele saatmisega. See koondab samasse haldusstruktuuri kõik peamised rahvusvahelised ja liidu õiguskaitsealase teabe vahetamise kanalid (Interpol, Europol ja SIRENE).

teabe taotlemiseks, saatmiseks ja vastuvõtmiseks eri kanaleid erineval määral, sageli ilma eelnevalt kindlaks määratud selge põhjendusega,³³ ning see takistab tõhusat ja tulemuslikku teabevahetust, toob kaasa taotluste dubleerimise, viivitused andmeedastuses ja võimaliku teabekao. Samuti jäävad riikide ametiasutused niiviisi ilma Europol toest, ehkki liikmesriigid ootavad, et Europol oleks EL-i kuritegevust käsitleva teabe keskus, mis on võimeline pakkuma kvaliteetseid teabepõhiseid tooteid.

Meetmed, millega EL reageerib kindlakstehtud probleemidele, peaksid tooma lisaväärtust kogu EL-ile ja seega ka EL-i kodanikele, kuna need muudavad Schengeni ala vastupidavamaks ning kindlamaks, mis omakorda avaldab mõju Schengeni lepinguga ühinenud riikidele. Ühised EL-i tasandi eeskirjad, standardid ja nõuded, mis hõlbustavad õiguskaitseasutuste vahelist piiriülese kuritegevusega seotud teabevahetust, loovad märkimisväärse mastaabisäästu, tagades samal ajal kõrgetasemelised andmeturbe- ja andmekaitsestandardid.

Lisaks täiendatakse KrMS-i normitehnilist viidet, lisades viite direktiivile 2023/2123. Kuna Eesti õiguses on direktiivist 2023/2123 tulenevad kohustused juba kehtivate normide kaudu tagatud, ei ole vaja kehtestada uusi sisulisi sätteid. Seetõttu piirdub ülevõtmine KrMS-i normitehnilise viite täiendamisega, millega tagatakse õiguslik selgus ja läbipaistvus direktiivist 2023/2123 tulenevate kohustuste täitmisel.

2.3. Eelnõu põhiseaduspärasus

Eelnõuga kavandatud muudatused ei muuda oluliselt senist KrMS-i regulatsiooni. Kehtiva KrMS 19. peatüki 8. jao 9. jaotis põhineb Rootsi raamotsusel ja operatiivkoostöö soovitusel, mille põhimõtted kattuvad Rootsi direktiivis sätestatuga. Rootsi direktiiv ei sisalda võrreldes Rootsi raamotsuse või operatiivkoostöö soovitusel uudseid põhimõtteid, vaid seab liikmesriikidele kohustuse neid põhimõtteid järgida ja täpsustab neid. Ehkki kehtiva KrMS-i regulatsioon sisaldab kõiki Rootsi direktiivi ja operatiivkoostöö soovitusel põhimõttelisi aspekte, on need kehtivas KrMS-is, eeskätt rakendaja jaoks, liiga abstraktsed. Rootsi direktiivist juhinduvad eelnõukohased muudatused tagavad õiguskaitsealase koostöö sätetest parema arusaadavuse ehk õigusselguse ning tõhusama põhiõiguste kaitse isikutele, kelle andmeid teisele EL-i liikmesriigile või Europolile edastatakse.

PS §-ga 3 sätestatakse, et riigivõimu teostatakse üksnes PS-i ja sellega kooskõlas olevate seaduste alusel. Kuna eelnõu kohaselt vahetavad uurimisasutused ja õiguskaitseasutused teavet kuritegude avastamiseks, tõkestamiseks ja menetlemiseks teiste EL-i liikmesriikide ning Europoliga selleks, et tõhustada kuritegevuse vastast võitlust nii riigisisesele kui ka riikideülelele, liidu tasandil, keskendume eelnõu põhiseaduspärasuse analüüsimisel peamiselt privaatsuse kaitsele, aga ka menetluse kiirele ja tõhusale läbiviimisele.

Peamised PS-is sätestatud põhiõigused, mida eelnõuga kavandatud muudatused riivata võivad, on järgmised.

1) Õigus eraelu puutumatusele (PS § 26): PS § 26 kohaselt on igaühel õigus perekonna- ja eraelu puutumatusele.

³³ Selgitus: mitu riiklikku ühtset kontaktpunkti kasutab sisesuuniseid, milles soovitatakse või nõutakse konkreetse sidekanali kasutamist konkreetsel otstarbel, millega tagatakse järjepidevus ja välditakse taotluste dubleerimist. Teistes kontaktpunktides on samal ajal määravaks ametnike harjumused ja eelistused. Paraku põhjustab selline tegutsemisvabadus piiriüleste uurimiste korraldamisel ebatõhusust.

Kui andmed, mida teise EL-i liikmesriigi ühtne kontaktpunkt või õiguskaitseasutus küsib, on isikuandmed, ja need talle väljastatakse, riivab Eesti riik selle füüsilise isiku õigust perekonna- ja eraelu puutumatusel, kelle andmeid vahetatakse.

Nimetatud põhiõiguste intensiivne riive riigi poolt leiab aset isikuga läbiviidavate süüteomenetluse tõendamistoimingute raames: kriminaalmenetlusele allutatud isikult proovide võtmisel; ülekuulamistel eraelu faktide kohta; läbiotsimistel ning nende raames leitud ja ära võetud esemete vaatlusel, eeskätt teabekandjate sisuga tutvumisel; jälitustoimingutega andmete kogumisel. Olukorras, kus süüteomenetluse käigus kogutud andmeid vahetatakse teise EL-i liikmesriigi ühtse kontaktpunkti või õiguskaitseasutusega, on võimalik, et isiku eraelu puutumatus riivatakse eelkirjeldatud toimingutega ka selle teise EL-i liikmesriigi õiguskaitseasutuse poolt, kui isik sinna riiki satub, või selle EL-i liikmesriigi algatusel Eestis, kui taotletakse EIO alusel menetlustoimingute läbiviimist. See tuleneb asjaolust, et teave, mida kõnesoleva regulatsiooni alusel vahetatakse, on lahutamatu seotud Eesti või teise EL-i liikmesriigi läbiviidava kriminaalmenetlusega. Teabevahetuse aluseks peab olema kavandatud, eesseisev või aset leidnud kuritegu ehk teabevahetuse eesmärk saab olla selle avastamine, tõkestamine või menetlemine. Nimetatud eesmärki ei ole võimalik saavutada ilma, et riivataks PS §-s 26 sätestatud põhiõiguseid.

PS §-s 26 sätestatu puhul ei ole aga tegemist absoluutse keeluga, vaid kvalifitseeritud seadusereservatsiooniga põhiõigusega, mis tähendab, et teatud juhtudel on riigil siiski õigus isiku perekonna- ja eraellu sekkuda. Perekonna- ja eraelu puutumatus kui põhiõiguse riive lubatavus on sätestatud PS §-s 26 endas, mille kohaselt võivad riigiasutused sekkuda isiku perekonna- ja eraellu tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks. Kuna kõnesolev teabevahetus toimub kuritegude ennetamise, tõkestamise ja menetlemise eesmärgil, on teabevahetusega kaasneva põhiõiguste riive eesmärk legitiimne.

Seejuures sätestatakse PS §-ga 26 lisakriteerium, mille kohaselt peavad lubatava sekkumise juhud ja kord olema täpsemalt reguleeritud seaduses. Selline kord on ette nähtud kehtivas KrMS-is, mille kohaselt peab teabevahetus toimuma süütegude avastamise, tõkestamise ja kriminaalmenetluse läbiviimise eesmärgil (KrMS § 508⁷⁸ lõige 1); teabetaotlusest peab nähtuma seos taotluse esitamise aluseks oleva põhjuse ja isiku vahel, kelle kohta teavet soovitakse (KrMS § 508⁷⁹ lõike 1 punkt 3); ning teabetaotluse täitmisel tuleb veenduda, et taotlus on proportsionaalne ehk vajalik ja soovitud eesmärgiga võrreldes mõistlik ning isikutele kõige vähem koormav (KrMS § 508⁸⁰ lõike 1 punktid 2 ja 3). Samad põhimõtted säilivad ka eelnõukohastes muudatustes, ent täpsustavad neid oluliselt, sätestades konkreetsed keeldumisalused (eelnõukohase KrMS § 508⁹¹ lõike 1 punktid 1–12) ja üksikasjalikud nõuded teabetaotlusele (eelnõukohase KrMS § 508⁹⁵ punktid 1–7) ning piiritledes teabe, mis nõuetekohase taotluse puhul vahetamisele kuulub (eelnõukohase KrMS § 508⁸⁵ lõige 2 ja § 508⁸⁸ lõige 1).

Arvestades, et rahvusvaheliste kuritegude tõkestamine nõuab üleeuroopalist koostööd, on õigustatud, et kriminaalmenetluses kogutud teavet jagatakse õiguskaitseorganite vahel. PS ei keela rahvusvahelist koostööd, kuid see peab toimuma kooskõlas õigusriigi põhimõtetega ja tagama isiku põhiõiguste kaitse. PPA kui ühtne kontaktpunkt ja uurimisasutused oma pädevuse piires vastutavad koostöö läbiviimise eest, mis tagab asutuste pädevuse kontrolli ja vähendab õiguste ülemäärase riive riski. Koosmõjus eelnõukohase KrMS § 508⁸⁷ lõikes 1 sätestatud kohustusega vahetada teavet vaid SIENA kaudu ja lõikest 4 tuleneva kohustusega SIENA kasutamise võimatuse korral teabevahetus esimesel võimalusel seal fikseerida tõhustub kontroll põhjendamatu päringute üle oluliselt. See peaks märkimisväärselt maandama võimalike õigustamata päringute esinemise riski.

Eelnõukohased KrMS 19. peatüki 8. jao 10. jaotise sätted on kooskõlas PS-i nõuetega, kuna need aitavad kaasa kuritegevuse tõkestamisele ja rahvusvahelisele koostööle, järgides samas isikute põhiõigusi. Isikuandmete edastamine teisele EL-i liikmesriigile võib riivata mitmeid PS-is sätestatud põhiõigusi, eriti eraelu puutumatuse, isikuandmete kaitse, tõhusa õiguskaitse ja õiglase kohtumenetluse, turvalisuse ja vabaduse ning isikupuutumatuse õigusi. Sellise andmete edastamise korral peavad olema tagatud seaduslikud alused, proportsionaalsus ja piisavad kaitsemeetmed isikute põhiõiguste kaitseks. Jaotises sätestatud piirangud, teabetaotlusele vastamisest keeldumise alused ja tingimused on mõeldud selleks, et tagada proportsionaalsus ning vältida liigset riivet. Seega võib eelnõu pidada põhiseaduspäraseks tingimuseks, et rakendamisel järgitakse kõiki sätestatud menetlusnorme, mis omakorda aitavad tagada isikute põhiõiguste kaitset.

Kavandatava muudatuse tulemusena isiku perekonna- ja eraelu puutumatuse riive tõenäoliselt suureneb, kuna raskete kuritegude puhul muutub andmevahetus asjassepuutuva liikmesriigi ja Europoliga kohustuslikuks, mis tähendab, et kasvab nii edastatavate andmete hulk kui ka nende adressaatide ring. Põhiõiguste riive ulatust tasakaalustab aga see, et muudatused kehtestavad senisest üksikasjalikumad, täpsemad ja kitsamad õigusraamid. Seega võib öelda, et kuigi kvantitatiivselt võib riive suureneeda, on see edaspidi kvalitatiivselt täpsemates ja kitsamates raamides, et vähendada meelevaldsuse või ülemäärasuse riski. See tähendab, et riive ei suurene põhiseadusvastaselt, vaid liigub õigusriiklikult paremini hallatava ja läbipaistvama teostuse suunas. Eeltoodust tulenevalt võib väita, et tegemist on olemasoleva riive parema reguleerimise ja piiramisega, mitte lihtsalt riive suurenemisega. Kuna riive eesmärk on raskete kuritegude avastamine, tõkestamine ja menetlemine, võib muudatuse tulemusena tekkivat põhiõiguste riivet pidada põhjendatuks, proportsionaalseks ja lubatavaks, sest see toimub kvalifitseeritud seadusereservatsiooni alusel, on seotud legitiimsel eesmärgil saavutamise ja piisavalt täpselt reguleeritud, vältimaks meelevaldset sekkumist isikute eraellu.

2) Õigus isikuandmete kaitsele (PS § 44): PS §-st 44 tuleneb igaühe õigus tutvuda enda kohta riigi arhiivides hoitavate andmetega ja saada teavet selle kohta, mida riik nende andmetega teeb. PS §-ga 44 sätestatakse seega isiku õigus kontrollida ja jälgida oma andmete kasutamist, veendumaks, et tema isikuandmete kaitse ning perekonna ja eraelu puutumus on tagatud.

Kehtivates seaduse sätetes arvestatakse andmekaitseõiguste ja proportsionaalsuse põhimõtet, ent need on sõnastatud liigabstraktselt, eeldades sisustamisel PS-i ja [isikuandmete kaitse seaduse](#) (edaspidi *IKS*) poole pöördumist. Eelnõus kavandatavate muudatustega täpsustatakse põhiõigusesse sekkumise lubatavaid juhtumeid ja korda senisest enam, nähes muu hulgas ette sõnaselge üksikasjaliku tegevusjuhise enne teise EL-i liikmesriigi teabetaotlusele vastamist selle nõutelevastavuse kontrolliks ning vajadusel õigusasutuselt (s.o Eesti kontekstis kohus või prokuratuur) teabevahetuse loa taotlemiseks. Ehkki muudatustega tekib inimestel eelduslikult parem arusaam sellest, mida riik nende kohta kogutud andmetega teeb ning kellel on nende kohta kogutud andmete juurdepääs, ei teki isikutele juurdepääsu teabe sisule ehk PS §-s 44 sätestatud õiguste piiramine jätkub vähemalt samas ulatuses kui praegu.

Kuna PS §-s 44 sätestatud õigus tutvuda enda kohta riigi arhiivides hoitavate andmetega ning saada teavet selle kohta, mida riik nende andmetega teeb, ei ole absoluutne, on riigil teatud juhtudel lubatud seda õigust piirata. Sellised juhud on eeskätt olukorrad, kus juurdepääsu piiramine on vajalik teiste isikute õiguste ja kriminaalmenetluse oluliste huvide kaitseks. Niisugustes olukordades ei ole juurdepääsupiirangu seadmisel tegemist mitte ametniku kaalutlusega, kas piirangut teabe suhtes kohaldada või mitte, vaid hinnanguga, millisel konkreetsel alusel seda teha tuleb, sest teiste isikute ja üldsuse huvid prevaleerivad üksikisiku huvide ees.

Õigus piirata isiku juurdepääsu tema kohta riigi arhiivides hoitavatele andmetele ning teabele selle kohta, mida riik nende andmetega teeb, tuleneb eeskätt KrMS § 15¹ lõikest 4, mis lubab piirata andmesubjekti isikuandmete kaitse seadusest tulenevaid õigusi siis, kui see on vajalik süüteo tõkestamiseks, avastamiseks, menetlemiseks või karistuse täideviimiseks, teise isiku või andmesubjekti õiguste ja vabaduste kahjustamise takistamiseks, riigi julgeoleku ohustamise takistamiseks või avaliku korra kaitse tagamiseks. Veel enam, sisuliselt kogu direktiivikohase teabevahetuse puhul on riigil AvTS-i kohaselt kohustus andmesubjekti õigusi piirata. AvTS § 35 lõike 1 punkti 1 kohaselt tuleb piirata juurdepääsu kriminaalmenetluses kogutud teabele, mida ei ole avaldatud (AvTS § 35 lõike 1 punkt 1); mille avalikuks tulek kahjustaks riigi välissuhtlust (AvTS § 35 lõike 1 punkt 3); mis sisaldab uurimisasutuse tegevuse meetodeid ja taktikat, kui selle avalikuks tulek võiks raskendada süütegude avastamist või soodustada nende toimepanemist (AvTS § 35 lõike 1 punkt 5¹); süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist (AvTS § 35 lõike 1 punkt 11) ning isikuandmeid sisaldavale teabele, kui sellele juurdepääsu võimaldamine kahjustaks oluliselt andmesubjekti eraelu puutumatust (AvTS § 35 lõike 1 punkt 12).

Eeltoodu tähendab, et isik saab seda teada tema kohta kogutud andmetest ja nende jagamise kaudu alles siis, kui ta on menetlusosaline ning algavad avalikud menetlustoimingud. Kuna PS §-s 44 sätestatu puhul on tegemist kvalifitseeritud seadusereservatsiooniga põhiõigusega ning AvTS ja KrMS näevad ette õigustuse andmete töötlemise ja vahetamise piiramiseks eesmärgiga kaitsta riigi ja üksikisikute õigusi ja huve, on isikuõiguse piiramine õiguspärane, sest see teenib õiguskaitse huve ning on vajalik selleks, et tagada menetluse sujuvus ja õiguskaitseorganite töö efektiivsus. Samuti tagavad need piirangud, et isikuandmete kaitse ja eraelu puutumatuse riive on proportsionaalne ning põhjendatud riigi ja ühiskonna huvidega.

3) Õigus sõnumisaladusele (PS § 43): PS §-ga 43 sätestatakse sõnumisaladuse kaitse, mis tähendab, et igal isikul on eraelu puutumatusega seoses õigus tema poolt või temale üldkasutataval teel edastatavate sõnumite saladusele. Sõnumisaladust riivab riik peaaesjalikult KrMS §-s 126³ loetletud jälitustoiminguid tehes. Kuna eelnõukohases KrMS 19. peatüki 8. jao 10. jaotises kirjeldatud teabe vahetamise süsteem võimaldab teiste liikmesriikide asutustega jagada näiteks KrMS § 126³ lõike 2 punktis 2 nimetatud jälitustoiminguga ehk salaja pealtkuulamise või varjatud jälgimisega kogutud teavet, paljastatakse tõenäoliselt seejuures delikaatseid isikuandmeid ja riivatakse nende isikute privaatsusõigust, kelle kohta need andmed käivad. Samuti riivatakse privaatsusõigust olukordades, kus teabevahetuse raames saadud teabele tugineva õigusasutuse loa alusel asutakse Eestis või teises EL-i liikmesriigis isiku suhtes eelkirjeldatud toiminguid tegema.

Kuna ka PS §-s 43 sätestatud õiguse puhul on tegemist kvalifitseeritud seadusereservatsiooniga põhiõigusega, ei ole sõnumite saladuse kaitse absoluutne. Riive on PS § 43 teise lause kohaselt lubatav kohtu loal kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks seadusega sätestatud juhtudel ja korras. Arvestades, et vahetatav teave on lahutamatu seotud Eesti või teise EL-i liikmesriigi läbiviidava või ees seisva kriminaalmenetlusega ning sellise teabe kogumine on toimunud riigisisese kriminaalmenetlusõiguse sätete kohaselt, on riive nõuetekohase teabevahetuse korral eelduslikult põhiseaduspärane ja lubatav. Ehkki reeglina ei otsusta kohus teistele riikidele teabe jagamise üle (v.a kinniseks kuulutatud istungi või lahendi puhul), on ta esmalt hinnanud jälitustoimingu lubatavust riigisiselt, tagades, et kõik vajalikud kaitsemehhanismid ja õiguslik alus on täidetud.

Ehkki ka kehtiva KrMS § 508⁷⁸ kohaselt vahetatakse teiste liikmesriikidega jälitusteavet, toob uus regulatsioon kaasa senisest ulatuslikuma ja regulaarsema teabevahetuse. See omakorda

tähendab suuremat sekkumist PS-is tagatud eraelu puutumatuse ja sõnumisaladuse kaitsesse. Kui seni on jälitustoimingutega kogutud teabe edastamine piirdunud enamasti üksikjuhtumite ja rahvusvaheliste menetlustega, siis nüüd, kui teabevahetus muutub regulaarsemaks ja laiemaks – tulenevalt kohustusest vahetada rasket kuritegevust puudutavat teavet asjassepuutuva liikmesriigi ja Europoliga –, suureneb ka mõju isiku õigusele privaatsusele ja sõnumisaladusele. Riive suurenemine seisneb seega peamiselt selles, et edaspidi jagatakse juba kogutud teavet laiemalt teiste liikmesriikide õiguskaitseasutustega. Kuigi teabevahetus liikmesriikide vahel ja sellega kaasnev riive isiku privaatsusele suureneb, tuleb märkida, et PS § 43 riive kontekstis vahetatakse vaid teavet, mis on juba salajase pealtkuulamise abil kogutud, ehk selleks hetkeks on põhiline riive – salajane pealtkuulamine – kohtu loal juba aset leidnud. See tähendab, et vahetatava teabe kogumine on läbinud *ultima ratio* ehk viimase abinõu kontrolli. Kohus on pidanud jälitustoimingut põhjendatuks ja vajalikuks kriminaalmenetluse eesmärkide täitmiseks, muu hulgas kuriteo tõendamiseks ja süüdlase vastutusele võtmiseks. Et vältida ohtu, kus suurenev andmevahetus võiks viia isikuandmete ülemäärase ja ebaõiglase kasutamiseni, on eelnõus ette nähtud mehhanismid, mis aitavad tagada andmekaitse põhimõtete järgimist ning tasakaalustada põhiõigustesse sekkumist. Kuigi andmete vahetamise ulatus suureneb, sätestatakse eelnõuga selged protseduurireeglid ja järelevalvemehhanismid, mis aitavad hoida isiku õiguste riivet mõistlikkuse piirides ning tagada, et sõnumisaladus ja eraelu puutumatus jääksid kaitstuks.

Esmalt nähakse ette selged kriteeriumid, mille alusel teabevahetus saab toimuda – teave peab olema seotud konkreetse kuriteoga, mille eest on ette nähtud vähemalt ühe aasta pikkune vangistus, ning teabe vahetamise aluseks peab olema põhjendatud alus arvata, et see aitab objektiivselt kaasa kuriteo avastamisele, tõkestamisele või menetlemisele (KrMS § 508⁹¹). Samuti nõutakse vahetatava teabe proportsionaalsuse hindamist, mis tähendab, et pelgalt võimalus teavet saada ei anna õigust selle vahetamiseks (KrMS § 508⁹¹). Eelnõus on määratletud täpsed nõuded teabetaotluse sisule ja vormistusele. Taotlus peab olema piisavalt konkreetne, sisaldama selgelt määratletud taotletavat teavet ja selle kasutamise eesmärki, samuti sisaldama põhjendust, miks on alust eeldada, et teavet omav riik seda konkreetset teavet valdab (KrMS § 508⁹⁵). Sellised nõuded aitavad vältida põhjendamatu andmevahetust ning takistada olukordi, kus teavet küsitakse laialdaselt ilma konkreetse eesmärgita.

Oluline kaitsemehhanism on kogu teabevahetuse koondamine turvalisse ja ühtsesse kanalisse SIENA, mis väldib teabe killustumist eri sidekanalite vahel ning muudab järelevalve teostamise tõhusamaks ja läbipaistvamaks. Kuigi erandkorras on lubatud teavet edastada ka muude sidevahendite kaudu, peab see teabevahetuse fakt ja vahetatud teave esimesel võimalusel SIENA-s kajastuma (KrMS § 508⁸⁷). Kuna kogu teabevahetuse kohta kogutakse üksikasjalikku statistikat (eelnõukohase PPVS § 25¹⁰), mis kuulub regulaarsele ülevaatamisele ka EL-i tasandil (Rootsi direktiivi artikkel 19), siis tõhustab see järelevalvet veelgi ning aitab kaasa rikkumiste avastamisele ja menetlemisele.

Jälitusteabe vahetamise näeb ette ka kehtiva KrMS 19. peatüki 9. jaotis „Teabe ja jälitustoiminguga kogutud teabe vahetamine EL-i liikmesriikide vahel“, mis lubab teavet vahetada siis, kui seejuures järgitakse Eesti õiguse üldpõhimõtteid (KrMS § 508⁸⁰ lõike 1 punkt 1 ja § 436 lõike 1 punkt 2). Eelnõukohaste muudatustega sellise teabe vahetamise nõudeid täpsustatakse, sätestades, et enne teabevahetust tuleb riive lubatavuse hindamisel arvestada, kas riive eesmärk (kuritegude avastamine, tõkestamine ja kriminaalmenetluse läbiviimine) on legitiimne ning kas see riive vastab proportsionaalsuse põhimõttele (eelnõukohase KrMS § 508⁹⁰ lõike 6, § 508⁹¹ lõike 1 punktid 1–12, seejuures sõnaselgelt eraldi välja toodud punktis 9). Eelnõu kohaselt tuleb teabetaotlusele vastamisel järgida kehtivaid menetlusnorme ja nõudeid, samuti on ette nähtud teabetaotlusele vastamisest keeldumise alused, mis annavad võimaluse jätta teabetaotlusele vastamata, kui see on ebaproportsionaalne

või ebaoluline. Need sätted aitavad tagada, et isiku privaatsusõigust ei riivataks ülemääraselt ja et riive oleks õigustatud. Eeltoodust tulenevalt võib asuda seisukohale, et eelnõuga kavandatavad muudatused ei ole paradigmaatilised, vaid pelgalt olemasolevaid nõudeid täpsustavad. Kuigi kvantitatiivselt riive tõenäoliselt suureneb, on see kvalitatiivselt edaspidi täpsemalt ja kitsamalt reguleeritud, vähendades seeläbi meelevaldse või ülemäärase riivamise riski.

4) Õigus tõhusale õiguskaitsele (PS § 15): PS § 15 lõigetega 1 ja 2 sätestatakse õigus PS-i kohaldamisele, mis tähendab, et isikule peab olema tagatud mitte üksnes juurdepääs kohtule, vaid ka tulemuslik õiguskaitse ja aus menetlus. Samuti hõlmab PS § 15 lõike 1 esimene lause ausa ja tõhusa kohtumenetluse nõuet. Eelnõu kohaselt sätestatakse KrMS § 508⁹⁶ lõikega 2 uurimisasutuse kohustus edastada omaalgatuslikult asjassepuutuvatele EL-i liikmesriikidele ja Europolile rasket kuritegevust käsitlevat kriminaalteavet. Sama kohustus kehtib ka vastupidiselt teistele EL-i liikmesriikidele. See tagab, et riigil, kus süütegu menetletakse, on juurdepääs kogu EL-is olemasolevale asjakohasele teabele.

PS §-s 15 sätestatud õiguste riive väljendub võimalikus läbipaistvuse puudumises ja isiku piiratud võimaluses kontrollida või vaidlustada tema kohta edastatud teavet enne, kui see mõjutab teda puudutavaid menetlusotsuseid. Samas tuleb riivet hinnata koostoides teabevahetuse eesmärgiga. Nagu eelnõus märgitud, aitab vastastikune andmeedastus tagada, et kuritegusid menetlevatel EL-i liikmesriikidel oleks ligipääs kogu asjakohasele teabele, suurendades seeläbi tõenäosust, et kuriteod tuvastatakse ja kurjategijad võetakse vastutusele. Seeläbi on võimalik tugevdada ka kannatanute õigust tõhusale õiguskaitsele. Lisaks võib andmevahetus toimida kahtlustatava kaitsemeetmena – võimaldades koguda objektiivset lisateavet, mis võib viia kahtluse kõrvaldamiseni või anda aluse menetluse lõpetamiseks. Selliselt toetab regulatsioon ka õiglasema ja tõenditel põhineva menetluse läbiviimist. Kokkuvõtvalt on teabevahetusega kaasnev põhiõiguste riive legitiimne ja proportsionaalne, kuna see teenib olulist avalikku huvi – tõhusa õiguskaitse ja menetluse eesmärki –, suurendades nii kannatanute kui ka kahtlustatavate õiguste kaitset ning tagades kooskõla PS §-s 15 sätestatud õigustega.

5) Õigus au ja hea nime, elu ning tervise kaitsele (PS §-d 16, 17 ja 28): igaühel on õigus oma au ja hea nime, elu ning tervise kaitsele. Isiku põhiõiguste riive võib suurenedagi siis, kui kurjategijatele saab teatavaks fakt, et isik on osutanud uurimisasutusele kaasabi. See võib viia tõendite, sealhulgas isikuliste, mõjutamise ja hävitamiseni, mis omakorda võib ohustada isiku turvalisust, au, head nime või tervist.

Loogiliselt ei ole kurjategijad huvitatud toime pandud tegude eest vastutamisest ja võivad seepärast asuda tõendeid, sealhulgas isikulisi, kõrvaldama. Kriminaalmenetluse huvid ei prevaleeri inimõiguste ees, mistõttu on nii objektiivses õiguses (KrMS § 508⁸⁰ lõike 1 punktis 2) kui ka eelnõukohase KrMS § 508⁹¹ lõike 1 punktis 10 ette nähtud kohustus teabevahetusest keelduda juhul, kui teabetaotluse täitmine kahjustaks isiku turvalisust. Eelnõuga seda põhimõtet ei muudeta, sama keeldumisasutus jääb kehtima ka edaspidi.

6) Õigus isikupuutumatusse ja vabadusele (PS § 20): igaühe õigus vabadusele ja isikupuutumatusse kaitseb üksikisikut meelevaldse vabadusekaotuse eest ning tagab, et tema kehalisse puutumatusse ei sekkutaks õigusliku aluseta. Vabaduse piiramine on lubatud üksnes seaduses sätestatud juhtudel ja korras, eelkõige kuritegude ärahoidmiseks, isiku toimetamiseks pädeva riigigorgani ette või tema põgenemise vältimiseks.

Kriminaalmenetlusala teabevahetus EL-i liikmesriikide vahel võib kujutada endast sekkumist nimetatud põhiõiguse kaitsealasse. Isiku suhtes võidakse algselt

kriminaalmenetlus, rakendada menetlustoiminguid – sealhulgas jälitustoiminguid, sundtoomist või isegi kinnipidamist –, tuginedes teisele liikmesriigile edastatud või sealt saadud isikuandmetele. Selline olukord tähendab, et isiku suhtes võidakse kohaldada tema õigusi piiravaid meetmeid, ilma et need põhineksid Eesti uurimisasutuste kogutud teabel. Lisaks võib isiku õigusi riivata juhul, kui ta ei ole kahtlustatav, vaid omab kriminaalasja seisukohalt olulist teavet. Tunnistaja ehk füüsilise isiku, kes võib teada tõendamiseseme asjaolusid, võib allutada menetlustoimingule tema soovist hoolimata, põhjustades seeläbi vähemalt ebamugavusi. Vajadusel võib seejuures riivata kriminaalmenetluse huvides ka tema põhiõigusi, eeskätt füüsilist vabadust, sest KrMS § 138 lõike 3 kohaselt võib tunnistaja suhtes kohaldada ka sundtoomist. Seejuures tuleb aga eelnimetatud näidete puhul rõhutada, et keeldumisaluste loetelu on võrreldes objektiivse õigusega oluliselt täiendatud (eelnõukohase KrMS § 508⁹¹ lõike 1 punktid 1–12), mistõttu saab vabaduste piiramine toimuda senisest kaalukamatel juhtudel. Näiteks nähakse muudatusega ette, et teabevahetus teiste EL-i liikmesriikidega saab toimuda ainult kuritegude osas, seejuures selliste kuritegude osas, mis on karistatavad vähemalt üheaastase vangistusega (eelnõukohase KrMS § 508⁹¹ lõike 1 punkt 1). Samuti tagab lisakaitse asjaolu, et vahetada tohib ainult teavet, mis on õige, täielik ja ajakohane (eelnõukohase KrMS § 508⁹¹ lõike 1 punkt 3).

Kuigi tegemist on sekkumisega põhiõigusesse, on see riive õiguspärane. Esiteks teenib see legitiimset eesmärki – kuritegude tõhusamat uurimist ja õigusemõistmise tagamist EL-i üleses koostöös. Teiseks on see ette nähtud seaduses, PS § 20 lõikes 3 ning ka KrMS-i rahvusvahelise koostöö ja teabevahetuse sätetes. Kuigi kvantitatiivselt riive tõenäoliselt suureneb, on see kvalitatiivselt edaspidi täpsemalt ja kitsamalt reguleeritud. Kehtiva KrMS § 508⁷⁸ kohaselt on EL-i liikmesriikidel lubatud vahetada teavet, sealhulgas jälitustoiminguga kogutud teavet, sõltumata teabevahetuse aluseks oleva süüteo liigist. Eelnõukohase KrMS § 508⁹¹ lõike 1 punkti 1 kohaselt tuleb teavet vahetada aga üksnes selliste kuritegude puhul, mille eest on seadusega ette nähtud vähemalt ühe aasta pikkune vangistus. Sellest tulenevalt kitseneb teabevahetuse kohaldamisala võrreldes senise regulatsiooniga. Lisaks piiravad võimalikku sekkumist täiendatud keeldumisalused, mis võimaldavad isiku põhiõigusi kaitsta juhtudel, kus andmete edastamine või selle alusel toimimine ei ole põhjendatud või proportsionaalne. Seetõttu on põhjendatud järeldada, et tegemist on põhiseadusliku õiguse riivega, kuid see riive on õiguspärane. See on kooskõlas seaduslikkuse, vajalikkuse ja proportsionaalsuse põhimõtetega, arvestades kehtestatud materiaalõiguslikke ja menetluslikke kaitsemeetmeid.

3. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb kolmest paragrahvist, millega muudetakse KrMS-i, KrMSRS-i ja PPVS-i.

Eelnõu § 1. KrMS-i muudatused

Eelnõu § 1 punkti 1 kohaselt tunnistatakse KrMS 19. peatüki 8. jao 9. jaotis kehtetuks.

Eelnõu § 1 punkti 2 kohaselt täiendatakse KrMS 19. peatüki 8. jagu uue 10. jaotisega. Sisult on lisanduv 10. jaotis seni KrMS 19. peatüki 8. jao 9. jaotises sätestatud teabevahetuse regulatsioon, kuid kuna Rootsi direktiivist tulenevalt on vaja senist regulatsiooni täpsustada ning osa sätete järjekorda parema jälgitavuse huvides muuta ja lisada alljaotisi, siis on otstarbekas esitada kavandatav regulatsioon uues 10. jaotises.

Selleks et tagada seadusest parem arusaadavus, luuakse KrMS 19. peatüki 8. jao 10. jaotises „Teabevahetus Euroopa Liidu liikmesriikide vahel ja Europoliga“ järgmised alljaotised:

1. alljaotis – teabevahetuse üldnõuded (§-d 508⁸⁵–508⁸⁹);

2. alljaotis – teabetaotlusele vastamine (§-d 508⁹⁰–508⁹³);
3. alljaotis – teabetaotluse esitamine (§-d 508⁹⁴–508⁹⁵);
4. alljaotis – omaalgatuslik teabeedastus (§ 508⁹⁶);
5. alljaotis – teabeedastus Europolile (§ 508⁹⁷).

KrMS 19. peatüki 8. jao 10. jaotises sätestatakse õiguslikud alused ja põhimõtted teiste EL-i liikmesriikide pädevate asutuste ja Europoliga teabe vahetamiseks.

Võrreldes kehtiva KrMS 19. peatüki 8. jao 9. jaotisega ei tooda uue 10. jaotise pealkirjas eraldi välja jälitustoiminguga kogutud teavet. Viide terminile „jälitustoiminguga kogutud teave“ ei ole vajalik, kuna eelnõus läbivalt kasutatav termin „teave“ hõlmab lisaks avalike menetlustoimingute abil saadud teabele ka jälitusteavet ehk KrMS 3¹. peatükis nimetatud jälitustoiminguga või PPVS 2². peatüki alusel salajase koostöö abil kogutud teavet, aga ka seaduses sätestatud ülesande täitmiseks tehtud isikuandmete töötlust muul viisil, kui see on tehtud eesmärgiga varjata andmete töötlemise fakti ja sisu andmesubjekti eest (nt luureteave avalikest allikatest ehk *open source intelligence* ehk OSINT).

Samuti ei ole KrMS 19. peatüki 8. jao 9. jaotises mainitud Europoli, kellega aga juba praegu teavet vahetatakse. Uue 10. jaotise pealkirjas tuuakse ka Europol õigusselguse huvides sõnaselgelt välja, sest Europol toetab nii Eesti uurimisasutusi kui ka teiste EL-i liikmesriikide õiguskaitseasutusi EL-i kriminaalteabe keskusena.

1. alljaotis **Teabevahetuse üldreeglid**

§ 508⁸⁵. Teabevahetuse korraldus

Kõnesoleva paragrahviga sätestatakse teabevahetuse üldpõhimõtted.

Lõikega 1 nähakse ette, et kuritegude avastamiseks, tõkestamiseks ja menetlemiseks vahetavad KrMS § 508⁸⁶ lõikes 1 nimetatud ühtne kontaktpunkt ja uurimisasutus (PPA, KAPO, Maksu- ja Tolliamet (edaspidi *MTA*), Konkurentsiamet, Sõjaväepolitsei, Keskkonnaamet ning Justiits- ja Digiministeeriumi vanglate osakond ja vangla) teavet:

- 1) teise EL-i liikmesriigi ühtse kontaktpunktiga;
- 2) teise EL-i liikmesriigi õiguskaitseasutusega ehk politsei-, tolli- või muu asutusega, kes on liikmesriigisisese õiguse kohaselt volitatud ja pädev kasutama riiklikku sundi³⁴ kuritegude avastamiseks, tõkestamiseks või menetlemiseks;
- 3) Europoliga.

Kuritegelik tegevus ei tunne riigipiire ning selle väljundiks on kuritegelikud võrgustikud, kes panevad toime väga erinevaid ning järjest dünaamilisemaid ja keerulisemaid kuritegusid, enamjaolt piirideüleselt. SOCTA kohaselt tegutseb 70% organiseeritud kuritegelikest ühendustest enam kui kolmes riigis, pannes toime erinevat liiki kuritegusid.³⁵ Arvestades Eesti geograafilist asukohta, on olulisemad kuritegevuse marsruudid laevaühendused üle Läänemere

³⁴ Selgitus: riiklik sund on avaliku võimu teostamise element, millega isikut seadusest tulenevalt piiratakse või kohustatakse tegutsema selliselt, et reegli täitmise tagamiseks võib haldusorgan seadusest tulenevalt kasutada sunnimeetmeid, nagu menetlustoimingutel osalemise kohustus, läbiotsimine, kinnipidamine, karistus jne.

³⁵ Europol, European Union Serious and Organised Crime Threat Assessment: A Corrupting Influence, Publications Office of the European Union, Luksemburg, 2021, 19. Kättesaadav: <https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021>.

ning maismaaliinid Lätist ja Venemaalt. Eestit mõjutavad kuritegevuse valdkonnad, mis omavad rahvusvahelist mõõdet, on:

- küberkuritegevus – väljastpoolt EL-i pärit ja Eestile suunatud küberkuritegevust on omistatud muu hulgas Nigeeriale, Rumeeniale ja Venemaale. Eelkõige on selliseks kuriteovormiks laste seksuaalne ärakasutamine internetis;
- narkokaubandus – täpsemalt kanepi, kokaiini ja sünteetiliste narkootiliste ainete piiriülene käitlemine, mille puhul narkokaubitsejate marsruudid kulgevad tavaliselt Leedu ja Läti kaudu Eestisse;
- pettused – täpsemalt käibemaksupettuste valdkonnas;
- rahapesu – Financial Action Task Force³⁶ on välja toonud, et suur osa Venemaal teenitud kuritegelikust tulust on pestud Kesk-Euroopa riikidesse või nende kaudu, sealhulgas Eesti kaudu;
- inimkaubandus – Eesti on inimkaubanduse ohvrite jaoks peamiselt transiitriik.

Kuritegelikud võrgustikud on proovikiviks võitluses raske ja organiseeritud kuritegevuse vastu, kuna nad õnnestavad õigusriigi põhimõtet, kasutades korruptsiooni ja võrgupettusi, sooritades vägivallategusid, kasutades tulirelvi oma kuritegelike eesmärkide saavutamiseks ning pestes kriminaaltulu põrandaaluse finantssüsteemi kaudu. Selleks et Eesti uurimisasutused saaksid kuritegusid tõhusamalt tõkestada, avastada ja menetleda, on oluline teha koostööd teiste EL-i liikmesriikide ja Europoliga. Sellise koostöö põhielement on kiire teabevahetus, mis lähtub põhimõttest, et Eesti uurimisasutustel on samaväärne juurdepääs teiste EL-i liikmesriikide õiguskaitseasutuste teabele. Kriminaalteabe vahetamise üldine eesmärk on kaitsta füüsiliste isikute julgeolekut ja juriidiliste isikute seadusega kaitstud olulisi huve.

Selleks et EL saaks tagada enda kodanikele [EL-i toimimise lepingu](#) V. jaotises nimetatud vabadusel, turvalisusel ja õigusel rajaneva ala, nähakse Rootsi direktiiviga kriminaalteabe vahetamine EL-i liikmesriikidele ette kohustusena. Vastav muudatus tuleb selgelt sätestada ka KrMS-is, sest kehtiv KrMS § 508⁷⁸ lõike 1 sõnastus näeb kriminaalteabe vahetamise ette vaid võimalusena, mille kasutamine sõltub uurimisasutuse initsiatiivist. See on osutunud probleemiks EL-i-üleselt, sest hindamised on näidanud, et praegu teabevahetust reguleerivate mittekohustusliku iseloomuga operatiivkoostöö soovitusel ning kohustusliku iseloomuga, aga põhimõttelisi, abstraktseid sätteid sisaldava Rootsi raamotsuse võimalusi ei kasutata tõhusalt, need ei ole piisavalt selged ega taga piisavat ja kiiret teabevahetust.³⁷ Seevastu Rootsi direktiiviga seatav kohustus teavet kiirelt edastada ja juhis, kuidas seda teha – kas teabetaotluse saamisel või omal algatusel siis, kui olemasoleva teabe puhul võib eeldada, et sellest on kasu teisele EL-i liikmesriigile kuritegude avastamiseks, tõkestamiseks või uurimiseks (KrMS-i mõistes menetluseks) –, võimaldab õiguskaitseasutustel palju tõhusamalt võidelda piiriülese kuritegevuse, sealhulgas kuritegevusturismi vastu.

Kuritegevuse vastast võitlust EL-is aitab tõhustada seegi, et Rootsi direktiiviga nähakse EL-i liikmesriikide õiguskaitseasutustele ette kohustus vahetada teavet ka Europoli kui EL-i kriminaalteabe keskusega. Seeläbi tekib Europolil kõikehõlmav ülevaade EL-i territooriumil asetleidvast kriminaalsest tegevusest. Eelnõuga nähakse vastav kohustus ette ka Eesti õiguses selleks, et tagada selle järgimine seaduse rakendajate, s.o uurimisasutuse töötajate (eeskätt

³⁶ Financial Action Task Force (FATF). Kättesaadav: <https://www.fatf-gafi.org/en/home.html>.

³⁷ Politseikoostöö: nõukogu eesistujariik ja Euroopa Parlament leppisid kokku direktiivis, millega parandatakse õiguskaitseasutuste vahelist teabevahetust. Euroopa Liidu Nõukogu, 29.11.2022. Kättesaadav: <https://www.consilium.europa.eu/et/press/press-releases/2022/11/29/police-cooperation-council-presidency-and-european-parliament-agree-on-a-directive-to-improve-information-exchange-between-law-enforcement-authorities/>.

eesliiniametnike) poolt. Ehkki juba praegu on kohustus edastada Europolile tema eesmärkide täitmiseks vajalikku teavet, peamiselt teavet EL-i poolt prioriteetsena käsitatavate kuriteoliikide tõkestamise ja nende vastu võitlemise kohta³⁸, ei nähtu see KrMS-ist, sest KrMS-is ei ole Europoli mainitud. Veel enam, sellise teabe vahetamine on kehtiva õigusega pandud täies ulatuses ühtse kontaktpunkti ülesandeks. See ei ole aga mõistlik, sest eeldab ühtselt kontaktpunktilt kõikide riigisiseste infoteadetega tutvumist ja nende analüüsi.

Lõikega 2 nähakse ette, et „teave“ on KrMS 19. peatüki 8. jao 10. jaotise tähenduses igasugused andmed, mis puudutavad vähemalt üht füüsilist või juriidilist isikut, fakte või asjaolusid ning mis on uurimis- ja õiguskaitseasutusele vajalikud kuritegude tõkestamiseks, avastamiseks või menetlemiseks, sealhulgas jälitustoiminguga ja salajase koostöö abil kogutud andmed.

Kehtiva KrMS § 508⁷⁸ lõikega 1 sätestatakse pelgalt, et EL-i liikmesriigiga võib vahetada teavet ja jälitustoiminguga kogutud teavet, jättes seejuures teabe mõiste määratlemata. Kuna sättest nähtub, et teabeks on vähemalt jälitustoiminguga kogutu ehk KrMS § 126¹ lõike 1 kohaselt isikuandmed, mida on töödeldud andmesubjekti eest varjatult, võib loogiliselt järeldada, et kehtiva õiguse kohaselt on teabeks ka kõik avalikult kogutud isikuandmed. Eelkirjeldatu ei pruugi aga selgelt ja kõikehõlmavalt määratleda andmeid, mida direktiivikohase teabevahetuse raames teiste EL-i liikmesriikidega vahetada tuleb. Seetõttu määratletakse võrreldes kehtiva KrMS § 508⁷⁸ lõikega 1 eelnõukohase KrMS § 508⁸⁵ lõikega 1 andmesubjektile ja teabevahetuse teostajale arusaadavamalt see, milliseid andmeid vahetatakse.

Lisaks laiendatakse oluliselt vahetatava teabe ulatust, juhindudes Rootsi direktiivi mõttest ja eesmärgist. Ehkki Eesti õiguses puudub jälitustegevuse legaalse definitsioon, saab jälitustegevusena tõlgendada KrMS §-s 126³ loetletud jälitustoimingu tegemist jälitustoimiku raames ja salajast koostööd PPVS 2². peatüki alusel, s.o väljaspool jälitustoimiku pidamist. Näiteks võib politsei koguda varjatult teavet PPVS § 7⁵¹ lõike 1 alusel salajasele koostööle kaasatud isikut või PPVS § 7⁵⁶ kohaselt variisikut kasutades. Rootsi direktiivi mõtte ja eesmärgiga on kooskõlas teabe määratlemine eelnõus toodud viisil, sest direktiivis reguleeritud teabevahetuse üks eesmärke võib olla mittetõendusliku tähendusega teabe saamine, et otsustada jälitustoimingu (s.o KrMS-i jälitustoimiku raames tehtava) tegemise vajaduse üle või taotleda selle teostamiseks prokuratuurilt või kohtult luba.

Lõike 3 kohaselt vahetatakse teavet ööpäev läbi ühtse kontaktpunkti kaudu.

Esmalt tuleb selgitada, et kehtiva KrMS § 508⁷⁸ lõikes 3 nimetati ühtset kontaktpunkti keskasutuseks. Kuna rahvusvahelises suhtluses kasutatakse rohkem terminit „ühtne kontaktpunkt“ (ingl *single point of contact* ehk SPOC), siis on otstarbekas ka KrMS-is seda terminit kasutada.

Rootsi direktiivi kohane teabevahetus on mõeldud toimuma ööpäev läbi ja reeglina EL-i liikmesriikide ühtsete kontaktpunktide kaudu. Uurimisasutuste struktuuriüksustele ööpäevaringse päringutele vastamise võimekust ette nähtud ei ole. Eeltoodu tähendab, et ehkki näiteks PPA korruptsioonivastase võitlusega tegelev üksus tagab küll ööpäev läbi teenuse toimimise, ei ole selle üksuse isikkoosseis alaliselt tööruumides reageerimisvalmis, sest selleks puudub vajadus. Pelgalt teabevahetuse tagamiseks ei ole sellise valmisoleku loomine iga uurimisasutuse ja iga valdkonnapõhise struktuuriüksuse tasandil kindlasti otstarbekas ega teabevahetuse mahtude mõttes põhjendatud.

³⁸ Europoli määruse ([ELT L 135, 24.5.2016, lk 53–114](#)) artikkel 7.

Seevastu riiklikul tasandil operatiivse teabevahetuse ööpäevaringne tagamine on hädavajalik selleks, et õiguskaitseasutused suudaksid reageerida kuritegevusele võimalikult varajases staadiumis, jõudes parimal juhul kuriteo ära hoida. Samuti on teabevahetuse kiirus väga tähtis esialgsete kriminaalmenetluslike tõkendite kohaldamise otsustamisel. Tõkendid on kriminaalmenetlust tagavad sunnivahendid, mis piiravad intensiivselt isiku põhiõigusi, kõige sagedamini õigust isiku- ja liikumisvabadusele. Samuti on tõkendite puhul tegemist süütuse presumptsiooni riivega. Eelkõige on tõkendite eesmärk kindlustada kriminaalmenetluse toimimine ja kohtuotsuste täitmine. Tõkendid on KrMS-i järgi elukohast lahkumise keeld (KrMS § 128), vahistamine (KrMS § 130), võimalus asendada vahistamine kaitsjoniga (KrMS § 135), vahistamise asendamine elektroonilise valvuga (KrMS § 137¹) ja kaitsevälase järelevalve (KrMS § 129). Sellise teabevahetusvõimekuse tagamiseks on ette nähtud, et igas EL-i liikmesriigis peab olema **üks keskne kontaktpunkt**:

- 1) kellel on juurdepääs kogu teabele, mis on tema riiklikel õiguskaitseasutustel;
- 2) kes on võimeline seda teavet teiste EL-i liikmesriikide õiguskaitseasutuste või ühtsete kontaktpunktidega ööpäev läbi vahetama.

Eesti kontekstis tähendab see, et ühtsel kontaktpunktil on juurdepääs Eesti uurimisasutuste teabele, mis on olemas riiklikus andmekogus, või võimalus saada sellist teavet direktiivis sätestatud tähtaegade raames uurimisasutustelt nende kontaktametnike kaudu.³⁹ Kui kuritegu aset leiab, võimaldab kiire reageerimine tõendeid koguda ajal, mil need ei ole veel kadunud. Kiire reageerimise tagab ühtne kontaktpunkt, kes olemata ise menetlev üksus, korraldab vajadusel teabe või teabetaotluse laekumisel selle kiire jõudmise pädeva uurimisasutuse struktuuriüksuseni. Kokkuvõtvalt tähendab eeltoodu, et kui mõne EL-i liikmesriigi õiguskaitseasutus peaks saatma kiireloomulist vastamist nõudva teabetaotluse töövälisel ajal otse uurimisasutusele, ei saa tal olla õigustatud ootust tähtaegsele vastusele. Küll aga tekib õigustatud ootus siis, kui teabetaotlus on adresseeritud ühtsele kontaktpunktile või kui viimane on teabetaotluse koopias.

Samuti on oluline märkida, et kuna vahetatav teave hõlmab paljudel juhtudel isikuandmeid, rõhutatakse Rootsi direktiivi põhjenduses nr 23, et kogu direktiivikohase teabevahetuse korral tuleb tagada isikuandmete kaitse vastavalt EL-i õigusele. Selleks peaks direktiivi alusel toimuv isikuandmete töötlemine ühtse kontaktpunkti või uurimisasutuse poolt toimuma täielikus kooskõlas Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2016/680⁴⁰, mis on Eesti õigusesse üle võetud peamiselt IKS 4. peatükis ja osaliselt ka KrMS-is. Samuti peavad teabevahetuses osalevad ühtne kontaktpunkt ja uurimisasutus käsitlema direktiivikohaseid taotlusi võimalikult kiiresti, et tagada isikuandmete õigsus ja usaldusväärsus, vältida tarbetut andmete dubleerimist ning vähendada ohtu, et sellised andmed aeguvad või ei ole enam kättesaadavad. Kui selgub, et isikuandmed on ebaõiged, tuleb need viivitamata parandada või kustutada ja nende töötlemist piirata. Eelkirjeldatud nõuetele vastavust saab kõige paremini tagada ööpäev läbi töötav ühtne kontaktpunkt, kes teabevahetuse nõuete kohase toimimise eest vastutab ja on sellele valdkonnale – erinevalt uurimisasutuste menetlevatest struktuuriüksustest – igapäevatoos spetsialiseerunud.

Lõike 4 kohaselt võib uurimisasutus vahetada iseseisvalt teavet oma pädevuse piires, järgides käesolevas jaotises ühtsele kontaktpunktile sätestatud õigusi ja kohustusi. See tähendab, et teatud juhtudel võib uurimisasutus vahetada teavet ka otse, ilma ühtse kontaktpunkti

³⁹ Selgituseks toonitame, et teise EL-i liikmesriigi ühtne kontaktpunkt või õiguskaitseasutus ei oma juurdepääsu Eesti uurimisasutuste teabele.

⁴⁰ Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK ([ELT L 119, 4.5.2016, lk 89](#)).

sekkumiseta, järgides kõiki teabevahetusele seatud protseduurireegleid, mille adressaat on reeglina ühtne kontaktpunkt. Nii võib uurimisasutus vahetada teavet iseseisvalt, omal algatusel ja oma pädevuse piires:

- 1) teise EL-i liikmesriigi ühtse kontaktpunktiga;
- 2) teise EL-i liikmesriigi õiguskaitseasutusega;
- 3) Europoliga;

arvestades seejuures KrMS 19. peatüki 8. jao 10. jaotises ühtsele kontaktpunktile sätestatud tingimusi.

Üldjuhul toimub teabevahetus ühtse kontaktpunkti kaudu, kes:

- vastab Eestile esitatud teabetaotlustele ise, kontrollides eelnõukohase KrMS § 508⁹⁰ lõike 2 kohaselt eelnevalt teisest EL-i liikmesriigist saabunud teabetaotluse nõuetekohasust, lubatavust ja sellele vastamise võimalikkust. Seejuures võib ühtne kontaktpunkt kaasata vastuse koostamisse ühe või mitu uurimisasutust;
- esitab KrMS § 508⁹⁴ kohaselt teise EL-i liikmesriigi õiguskaitseasutusele või ühtsele kontaktpunktile eelnõukohase KrMS § 508⁹⁵ nõuetele vastava teabetaotluse siis, kui Eesti uurimisasutusel on põhjendatud alus arvata, et teise EL-i liikmesriigi õiguskaitseasutusel on teavet, mis võib aidata avastada, tõkestada või menetleda kuritegu.

Lisaks ühtsele kontaktpunktile kui eelnõukohase KrMS § 508⁸⁵ lõike 3 kohaselt põhilisele teabevahetuse teostajale on teabe vahetamise õigus antud ka uurimisasutustele, EL-i liikmesriikide kontekstis õiguskaitseasutustele. Paindlikkuse võimaldamiseks nähakse Rootsi direktiivis ja eelnõukohase KrMS § 508⁸⁵ lõikes 4 ette, et teatud reeglite järgimisel võivad uurimisasutused vahetada teavet iseseisvalt, ühtse kontaktpunkti sekkumiseta (edaspidi *uurimisasutuse iseseisev teabevahetus*).

Selline võimalus on ette nähtud eelkõige omaalgatusliku teabeedastuse jaoks. Kuna teatud uurimisasutuste (täpsemalt nende struktuuriüksuste) teabevahetus teiste EL-i liikmesriikide õiguskaitseasutustega on tegevusvaldkonna või kaasuse põhiselt sage ja valdkonnale eriomane, ei pruugi sellise suhtluse vahendamine ühtse kontaktpunkti poolt olla alati mõistlik. Seda seetõttu, et valdav osa teabevahetusest leiab aset tööpäeva raames EL-i liikmesriikidega, kes asuvad kokku kuni kolmes ajatsoonis (GMT, GMT+1, GMT+2). Samuti seetõttu, et teabetaotluse täitmiseks on reeglina aega seitse päeva. Olukorrad, kus teavet on vaja kiireloomuliselt vahetada öötundidel, on äärmiselt erandlikud. Seetõttu nähakse eelnõukohase KrMS § 508⁸⁵ lõikes 4 ette võimalus vahetada teavet otse, ilma ühtse kontaktpunkti vahenduseeta. Samuti võib otsesuhtluse tingida operatiivvajadus. Seetõttu võib uurimisasutus iseseisvalt oma pädevuse piires:

- 1) esitada teise EL-i liikmesriigi ühtsele kontaktpunktile või õiguskaitseasutusele teabetaotluse;
- 2) vastata teiselt EL-i liikmesriigi ühtselt kontaktpunktilt või õiguskaitseasutuselt Eestile saadetud teabetaotlusele siis, kui see on adresseeritud otse uurimisasutusele või kui Eesti ühtne kontaktpunkt on selle temale vastamiseks edastanud.

Seejuures tuleb uurimisasutusel hoida Eesti ja teise EL-i liikmesriigi ühtne kontaktpunkt kogu iseseisva teabevahetuse koopias. Eelnimetatud reeglist võib kõrvale kalduda vaid siis, kui esineb eelnõukohase KrMS § 508⁹³ lõikes 3 nimetatud oht, ehk juhul, kui see:

- 1) seaks ohtu isiku turvalisuse;
- 2) võiks märkimisväärselt kahjustada käimasolevat kriminaalmenetlust või
- 3) puudutab terrorikuritegu, mis ei hõlma hädaolukorra lahendamist.

Eelnimetatud ohu esinemisel on lubatud jätta koopia edastamata sellele ühtsele kontaktpunktile, kellest oht lähtub. Ohust tuleb teavitada selle riigi pädevaid asutusi, kelle ühtsest kontaktpunktist oht lähtub, et neil oleks võimalik oht likvideerida, näiteks alustada menetlust ja kõrvaldada teenistusest ühtse kontaktpunkti ametnik, kes teavet lekitab.

Ühtse kontaktpunkti koopias hoidmise nõue on ette nähtud selleks, et ühtsel kontaktpunktil oleks võimalik jälgida kogu riigi osalusel teabevahetust ning teabevahetuse tähtaegadest ja vastamiskohustusest kinnipidamist, viimast vajadusel ise tagades. Nõude järgimise teeb ühtsele kontaktpunktile hõlpsaks asjaolu, et neile on näha kogu Eestit puudutav teabevahetus SIENA-s, välja arvatud eelnõukohases KrMS § 508⁹³ lõikes 3 nimetatud juhul. Näiteks olukorras, kus tavatööaja välisel ajal esitatakse Eesti uurimisasutusele kiireloomulist reageerimist nõudev teave või teabetaotlus, korraldab ühtne kontaktpunkt selle jõudmise pädeva uurimisasutuse struktuuriüksuseni. Ühtne kontaktpunkt jälgib, et teabetaotluse esitanud EL-i liikmesriigi õiguskaitseasutusele oleks tähtaegselt ja reegleid järgides vastatud. Ühtse kontaktpunkti puudumisel ei märgataks tavatööaja välisel ajal tõenäoliselt kiireloomulist reageerimist nõudvat sissetulevat teavet või teabetaotlust, mistõttu jäetaks süüteole reageerimata, süütegu jääks avastamata või tõendid kaoksid.

Lõikega 5 nähakse ette, et teavet vahetatakse järgmistel viisidel:

- 1) teabetaotluse alusel;
- 2) omal algatusel.

Üldsätte eesmärk on kirjeldada olukordi, millal uurimisasutus ja ühtne kontaktpunkt teavet vahetavad. EL-i liikmesriikide õiguskaitseasutuste vaheline teabevahetus toimub kas Rootsi direktiivi või Schengeni infosüsteemi (edaspidi *SIS*)⁴¹ regulatsiooni alusel. SIS-i puhul piirdub teabevahetus hoiatusteadetega, mille eelduseks on, et mõni Schengeni ala liikmesriik märgib ära isiku või eseme, keda või mida otsitakse, ning sisestab SIS-i vastavad andmed, et võimaldada isiku või eseme tuvastamist ja jälgimist Schengeni alal. Rootsi direktiivi kohane teabevahetus on aga laiem, keskendudes isikute ja esemete asemel teabele juba toime pandud või peagi aset leida võivate kuritegude kohta. Rootsi direktiivi kohase teabevahetuse raames saadud teave võib olla aluseks Schengeni alal isiku või eseme otsimiseks, võimaldades SIS-i hoiatusteate seadmist, mille alusel alustatakse otsingut ja jälgimist Schengeni alal.

Rootsi direktiivi alusel toimuv teabevahetus algab tavaliselt ühe EL-i liikmesriigi õiguskaitseasutuse teabetaotlusega teise liikmesriigi õiguskaitseasutusele või ühtsele kontaktpunktile. Teabetaotluses palutakse teavet konkreetse kuriteo kohta, mis on juba toime pandud, kavandamisel või mis võib peagi aset leida. Taotluses võib keskenduda üksnes konkreetsetele asjaoludele, mis on olulised kuriteo avastamiseks, tõkestamiseks või menetlemiseks. Näiteks võib see hõlmata ainult teatud faktilisi asjaolusid või üksikut tõendamise seisukohalt tähtsat detaili. Sellist taotlust saab esitada ainult siis, kui on põhjendatud kahtlus, et teisel liikmesriigil on vajalikku teavet, mis võib aidata kuritegu avastada, tõkestada või menetleda. Piirang on seatud selleks, et mitte koormata teisi liikmesriike asjatute teabetaotlustega, mille täitmine ei ole nende pädevuses või millel puudub oluline eesmärk. See aitab keskenduda ainult vajalike ja asjakohaste kuritegude lahendamisele.

Kehtivad EL-i soovitusel ja sellest tulenevalt ka KrMS-i regulatsioon ei näe ette kohustust teavet omal algatusel edastada. Omaalgatuslikku teabedastust reguleeritakse kehtiva KrMS § 508⁸⁴ lõikega 1, milles on sätestatud vaid järgmine: „Pädev asutus võib edastada välisriigile ilma selleks eelnevat taotlust saamata asjakohast ja vajalikku teavet, mis võib aidata kaasa käesoleva seadustiku § 489⁶ lõikes 1 nimetatud kuritegude avastamisele, tõkestamisele või

⁴¹ Vt täpsemalt Schengeni infosüsteemi kohta: https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system_et.

uurimisele.“ See tähendab, et teabeedastus põhineb pelgalt õiguskaitseasutuste initsiatiivil. Selline vabatahtlikkus pärsib aga oluliselt liikmesriikide võimalusi kasutada juba olemasolevat teavet kuritegude avastamiseks, tõkestamiseks ja menetlemiseks – seda hoolimata asjaolust, et kehtiv õigusraamistik sellist teabevahetust tegelikult lubab. Kuna EL-i liikmesriikide õiguskaitseasutustel ei ole täielikku ülevaadet sellest, millist teavet teised EL-i liikmesriikide õiguskaitseasutused omavad või millele neil on juurdepääs, ning puudub võimalus sellele teabele iseseisvalt juurde pääseda, ei pruugita alati osata küsida vajalikku või asjakohast teavet. Seetõttu nähakse direktiiviga ette kohustus vahetada teavet omal algatusel siis, kui neil olemasolev teave võib aidata avastada, tõkestada või menetleda rasket kuritegu mõnes teises EL-i liikmesriigis; ning võimalus edastada teavet siis, kui tegemist ei ole rasket kuritegu puudutava teabega, ent sellest võib teise EL-i liikmesriigi õiguskaitseasutusele olla kasu kuriteo avastamisel, tõkestamisel või menetlemisel.

Lõike 6 kohaselt vahetatakse teavet inglise keeles.

Rootsi direktiivi artikliga 11 sätestatakse inglise keel EL-i liikmesriikide ühtsete kontaktpunktide ühe kohustusliku töökeelena. Sätte kohaselt peavad kõikide EL-i liikmesriikide ühtsed kontaktpunktid suutma vastata teabetaotlustele täies ulatuses inglise keeles, soovi korral lisaks mõnes muus keeles. Et vältida keelebarjäärist tingitud viivitusi ja piirata tõlkekulusid, peab ühtne kontaktpunkt olema suuteline täitma keelenõuet iseseisvalt. Kui uurimisasutus soovib vahetada teavet iseseisvalt oma pädevuse piires (eelnõukohase KrMS § 508⁸⁵ lõige 4), peab ka tema olema suuteline täitma keelenõuet kas iseseisvalt või ühtse kontaktpunkti abiga.

Rootsi direktiivi põhjenduse nr 24 kohaselt tuleb EL-i liikmesriikidel selleks, et nende ühtsed kontaktpunktid saaksid edastada taotluse alusel või omal algatusel teavet piisavalt ja kiiresti, määrata keeled, milles nende ühtne kontaktpunkt suudab teabetaotlusi ööpäev läbi teenindada. Kuna inglise keel on EL-i õigusalasest koostöös laialdaselt kasutatav ja EL-is üldiselt mõistetav, on see seatud üheks kohustuslikuks keeleks. Lisaks inglise keelele võivad liikmesriigid määrata ka muid keeli, milles saab nende ühtse kontaktpunkti poole pöörduda ja milles see saab suhelda. Selleks tuleb liikmesriikidel koostada loetelu keeltest, milles nende ühtne kontaktpunkt suudab teabetaotlusi teenindada, ning esitada see keelte loetelu Euroopa Komisjonile, kes avaldab vastava koondkogumi internetis ja ajakohastab seda.

Seejuures tuleb silmas pidada, et keelenõudele on allutatud kogu teabevahetus – taotletud teabe esitamine, taotluse rahuldamata jätmine, sealhulgas rahuldamata jätmise põhjused, konkreetse taotlusega seotud taotlused selgituste või täpsustuste saamiseks ning selgitused ja täpsustused.

Lähtudes vajadusest tagada ühtse kontaktpunkti vastavus keelenõudele ööpäev läbi, nähakse eelnõus ette, et teabevahetus EL-i liikmesriikide õiguskaitseasutuste ja ühtsete kontaktpunktidega toimub inglise keeles. Sätte selline sõnastus on tingitud pragmaatilisest kaalutlusest. Esmalt vajadusest tagada, et direktiiviga sätestatud kohustuslik keelenõue oleks kindlasti täidetud. Teiseks, ehkki Eesti ühtse kontaktpunkti ametnikud valdavad kindlasti ka muid keeli, ei pruugi selline ühetaoline võimekus olla tagatav ööpäev läbi. Kolmandaks suurendaks mitmes keeles ühe kaasuse raames teabetaotlusele vastamine töökoormust mõlemas riigis, sest võib juhtuda, et riigisiselt tegeleb teabetaotlusele vastamisega mitu ametnikku. Sellisel juhul muutuks eri keeltes peetav kirjavahetus keeruliselt järgitavaks ja tõusetub tõlkevajadus.

Teabevahetuse keelena inglise keele sätestamine ei puuduta KrMS §-s 10 toodud põhimõtet, mille kohaselt on kriminaalmenetluse keel eesti keel. Praegusel juhul sätestatakse teabevahetuse keel üksnes selleks, et tagada teiste riikide õiguskaitseametnikega parem suhtlus.

Kriminaalmenetlus võib KrMS § 10 lõike 1 kohaselt toimuda menetleja, menetlusosaliste ja kohtumenetluse poolte nõusolekul ka muus keeles, kui nad seda valdavad.

Tulenevalt asjaolust, et Europolil on Rootsi direktiivi ülevõtmise perioodil valminud tõlkemoodul, mis võimaldab SIENA-s edastatud teabe automaattõlget iga EL-i liikmesriigi ametlikust keelest inglise keelde ja inglise keelest iga EL-i liikmesriigi ametlikku keelde, on sisuliselt võimalik SIENA kaudu teavet vahetada ka eesti keeles. Seejuures tuleb silmas pida, et automaattõlge võib vajada järeletoimetamist ehk masintõlgitud teksti läbivaatamist, võrdlust ingliskeelse tekstiga ning parandusi selleks, et saada tulemiks täpne ja ladus tõlge.

§ 508⁸⁶. Ühtne kontaktpunkt

Nii nagu näeb ette kehtiva KrMS § 508⁷⁸ lõige 3, et rahvusvahelise koostöö keskasutus on PPA, nähakse ka eelnõukohases KrMS § 508⁸⁶ lõikes 1 ette, et Eesti kriminaalteavet koondav ja haldav ühtne kontaktpunkt⁴² on PPA. See on tingitud asjaolust, et juba praegu on PPA-sse koondatud kõige olulisemad piiriülese kriminaalteabe vahetuse komponendid (Europoli riiklik üksus⁴³, Schengeni Infosüsteemi täiendava teabevahetuse üksus ehk SIRENE büroo⁴⁴ ja Rahvusvahelise Kriminaalpolitsei Organisatsiooni (edaspidi *Interpol*) riiklik keskbüroo⁴⁵), mis töötavad ööpäev läbi.⁴⁶ Lisaks on PPA valdavas osas kriminaalmenetlustes menetlev uurimisasutus⁴⁷, sealhulgas jälitustoimikuid avav asutus⁴⁸, millest võib järeldada, et PPA on asutus, kes omab kõige rohkem kriminaalteavet. Samuti, kuna Rootsi direktiivi artikli 14 lõike 3 punktist a tuleneb nõue, et ühtne kontaktpunkt peab omama juurdepääsu kogu teabele, mis on kättesaadav tema õiguskaitseasutustele, niivõrd kui see on vajalik talle direktiivist tulenevate ülesannete täitmiseks,⁴⁹ räägib PPA ühtse kontaktpunktina jätkamise kasuks asjaolu, et enamik uurimisasutusi omab juurdepääsu politsei andmekogule (edaspidi *infosüsteem POLIS*)⁵⁰, olles selles andmeandja.

⁴² Selgituseks: nagu eelnõukohase KrMS § 508⁸⁵ selgitustes märgitud, nimetatakse kehtiva KrMS § 508⁷⁸ lõikes 3 nimetatud keskasutust edaspidi rahvusvahelises suhtluses sagedamini kasutatava terminiga „ühtne kontaktpunkt“ (ingl *single point of contact* ehk SPOC), sest seda kasutatakse rahvusvahelises suhtluses kõige enam.

⁴³ Euroopa Liidu lepingu artiklil K.3 põhineva Euroopa Politseiameti konventsiooniga (Europoli konventsioon) ning selle protokollidega ühinemise seadus, § 2.

⁴⁴ Euroopa Liidu Teataja C 85/299 N.SIS-i büroode ja riiklike SIRENE büroode nimekiri. Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=uriserv%3AOJ.C_.2023.085.01.0299.01.ES&toc=OJ%3AC%3A2023%3A085%3AFUL.

⁴⁵ Interpol. Kättesaadav: <https://www.interpol.int/Who-we-are/Member-countries/Europe/ESTONIA>.

⁴⁶ Selgituseks: Europoli riikliku üksuse, SIRENE büroo ja Interpoli riikliku keskbüroo näol ei ole tegemist menetlevate üksustega, vaid n-ö asutusega asutuses ehk PPA struktuuriüksusega, kes on PPA-st iseseisev ja sõltumatu.

⁴⁷ Justiitsministeerium. Kuritegevus Eestis 2022. Kuritegevuse ülevaade. Kättesaadav: <https://www.kriminaalpoliitika.ee/kuritegevus2022/>.

⁴⁸ Justiitsministeerium. Kuritegevus Eestis 2022. Jälitustegevus. Kättesaadav: <https://www.kriminaalpoliitika.ee/kuritegevus2022/jalitustegevus/>.

⁴⁹ Selgituseks: direktiivist tulenev nõue, et ühtsel kontaktpunktil peab olema juurdepääs kogu teabele, mis on kättesaadav tema õiguskaitseasutustele, ei tähenda, et kõigi KrMS § 31 lõikes 1 nimetatud uurimisasutuste kogu teave peaks edaspidi olema Eesti ühtsele kontaktpunktile juurdepääsetav infosüsteemi POLIS või teiste uurimisasutuste infosüsteemide kaudu. Ka uurimisasutuste siseselt ei ole kõikidele menetlejatele tagatud kogu teabele piiramatut ja vahetut juurdepääsu. Eeltoodu tähendab, et ühtsel kontaktpunktil on juurdepääs teiste uurimisasutuste teabele, mis on juurdepääsetav infosüsteemi POLIS kaudu, ning teave, mis on uurimisasutustel olemas, kuid millele POLIS-e kaudu juurdepääs puudub, tuleb ühtsele kontaktpunktile põhjendatud teabetaotluse korral ja keeldumisel puudumisel direktiivis ettenähtud tähtaja jooksul edastada muul viisil, näiteks SIENA kaudu.

⁵⁰ Politsei andmekogu põhimäärus, §-d 15 ja 19.

Lõikega 2 nähakse ette, et ühtse kontaktpunkti töös osalevad:

- 1) iga uurimisasutuse esindaja;
- 2) Europolit riiklik üksus, mis on loodud Europolit määruse artikli 7 alusel;
- 3) riiklik SIRENE büroo, mis on loodud Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1862 artikli 7 lõike 2 alusel;
- 4) Interpolit riiklik keskbüroo, mis on loodud Rahvusvahelise Kriminaalpolitsei Organisatsiooni põhikirja artikli 32 alusel.

Rootsi direktiivi artikli 15 lõikes 2 sätestatakse EL-i liikmesriigi ühtse kontaktpunkti kohustuslik koosseis. See koosseis nähakse ette ka eelnõukohases KrMS § 508⁸⁶ lõikes 2. Ehkki see ei ole Eesti õigusaktidest hõlpsalt leitav, on Europolit riiklik üksus⁵¹, riiklik SIRENE büroo⁵² ja Interpolit riiklik keskbüroo⁵³ PPA ning kõik need struktuuriüksused kuuluvad ühtse kontaktpunkti koosseisu ka käesoleval ajal.

Võrreldes senisega peavad ühtse kontaktpunkti koosseisus olema esindatud kõik asutused, kes on KrMS-i kohaselt pädevad kasutama kuritegude tõkestamisel, avastamisel või uurimisel riiklikku sundi.⁵⁴ Sellised asutused on KrMS § 31 lõikes 1 nimetatud uurimisasutused. Ehkki nimetatud uurimisasutused osalevad rahvusvahelises kriminaalmenetlusalas teabevahetuses ka praegu, on senine teabevahetus tuginenud paljuski tavaõigusele ja haldusorganite koostööle. Eelnõuga soovitakse sätestada teabevahetuse kohustuslikkus ning luua seeläbi õiguslik alus uurimisasutustele teabe vahetamiseks teiste EL-i liikmesriikide õiguskaitseasutustega, sealhulgas kriminaalmenetlusvälises (reeglina menetluseelses) staadiumis selleks, et täita Euroopa Liidu lepingu artikli 3 lõikest 2 tulenevat EL-i üht põhieesmärki – tagada enda kodanikele vabadusel, turvalisusel ja õigusel rajanev ala.

Ühtlasi on see vajalik selleks, et tagada õiguskindlus ja toimepidevus riigi ressursside ja võimalike asutusesiseste töökorralduse muudatuste valguses. Operatiivse teabevahetuse tagamine ööpäev läbi on hädavajalik, et uurimisasutused suudaksid reageerida kuritegevusele võimalikult varajases staadiumis, jõudes parimal juhul kuriteo ära hoida. Kui kuritegu siiski aset leiab, võimaldab kiire reageerimine tõendeid koguda ajal, mil need ei ole veel kadunud. Samuti omab teabevahetuse kiirus olulist tähtsust esialgsete kriminaalmenetluslike tõkendite kohaldamise otsustamisel.

Kuigi seni EL-i õiguskaitseasutuste vahelist teabevahetust reguleerinud Rootsi raamotsus⁵⁵ nägi EL-i liikmesriikidele ette kohustuse teavet ja jälitusteavet kindlate tähtaegade jooksul vahetada, olid selle praktilised aspektid, nagu ühtse kontaktpunkti olemasolu ja selle kaudu ööpäevaringse teabevahetuse toimumine, sätestatud mittekohustuslikus operatiivkoostöö soovitus⁵⁶. Eelkirjeldatu tõttu esines praktikas probleeme teabetaotluste tähtaegse täitmisega. Rootsi raamotsuse artiklis 4 sätestatud kohustuslike tähtaegade asemel täideti teatud EL-i

⁵¹ Euroopa Liidu lepingu artikli K.3 põhineva Euroopa Politseiameti konventsiooniga (Europolit konventsioon) ning selle protokollidega ühinemise seadus, § 2.

⁵² Euroopa Liidu Teataja C85/299 N.SIS-i büroode ja riiklike SIRENE büroode nimekiri. Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=uriserv%3AOJ.C_.2023.085.01.0299.01.ES&toc=OJ%3AC%3A2023%3A085%3AFUL.

⁵³ Interpol. <https://www.interpol.int/Who-we-are/Member-countries/Europe/ESTONIA>.

⁵⁴ Rootsi direktiivi artikli 2 punkti 1 mõistes pädevad õiguskaitseasutused.

⁵⁵ Nõukogu 18. detsembri 2006. aasta raamotsus 2006/960/JSK Euroopa Liidu liikmesriikide õiguskaitseasutuste vahelise teabe ja jälitusteabe vahetamise lihtsustamise kohta (ELT L 386, 29.12.2006, lk 89), artikkel 4.

⁵⁶ Nõukogu 9. juuni 2022. aasta soovitus (EL) 2022/915 õiguskaitsealase operatiivkoostöö kohta (ELT L 158, 13.6.2022, lk 53), 1. peatüki punkt e.

liikmesriikides teabetaotlusi esimesel võimalusel, mis võttis aga raamotsusega lubatust kauem aega.

Ehkki Eesti senisest praktikast nähtub, et direktiivikohane teabevahetus, mida tuleb teostada töövälisel ajal, on erandlik ja harva esinev, ei ole direktiivis sõnaselgelt sätestatud kohustust muul viisil, kui kõikidele uurimisasutustele ööpäevaringse valmiduse kohustuse seaduses sätestamisega, võimalik püsivalt tagada.⁵⁷

Rootsi direktiivi artikli 15 lõike 2 kohaselt on kohustuslik määrata EL-i liikmesriigis ühtse kontaktpunkti koosseisu kuuluvad asutused, ent direktiivis ei seata piiranguid sellele, kuidas osalus teabevahetuses sisemiselt korraldatakse. See tähendab, et direktiivi nõuetekohane ülevõtmine Eesti õigusesse ei eelda, et uurimisasutuste ametnikud peavad alluma PPA-le või töötama füüsiliselt ühtse kontaktpunkti ruumides PPA-s.

Uurimisasutustel on kohustus tagada ööpäev läbi kättesaadavus ja suutlikkus vahetada operatiivselt teavet. Selleks võib kasutada erinevaid tehnilisi lahendusi, mis võimaldavad vajadusel kiiret reageerimist, sõltumata töökorraldusest või füüsilisest asukohast. Uurimisasutuste valmisolek ööpäev läbi teavet vahetada on tingitud Rootsi direktiivi artikli 5 lõikest 1 tulenevatest tähtaegadest, mis esitatakse eelnõukohases KrMS §-s 508⁹² ja mille eesmärk on tagada kiireloomulist reageerimist nõudvate sündmuste puhul asjakohane teabevahetus selleks, et sündmustele kohaselt reageerida. Tähtajast kinnipidamine on aktuaalne eeskätt kiireloomulise teabetaotluse korral, millele tuleb tagada vastamine kaheksa tunni või kolme kalendripäeva jooksul teate ühtsesse kontaktpunkti saabumisest arvates.

Arvestades, et ühtsel kontaktpunktil on juba praegu ööpäevaringne reageerimisvalmidus ning juurdepääs PPA ja teiste uurimisasutuste poolt infosüsteemi POLIS kaudu juurdepääsetavale teabele, mõjutab eelnõukohane säte eeskätt uurimisasutusi, kelle teave infosüsteemi POLIS kaudu juurdepääsetav ei ole. Uurimisasutustel, kelle teave pole ühtsele kontaktpunktile POLIS-e kaudu juurdepääsetav, tuleb tagada, näiteks ametnike valveaja kaudu, ööpäevaringne valmisolek ühtsele kontaktpunktile vajadusel teavet edastada. Selline valmisolek on valdaval osal uurimisasutustest olemas juba praegu, sest praktikas on vaja reageerida ka väljaspool tavapärast tööaega, näiteks kahtlustatavate kinnipidamiseks.

Direktiivi 2023/2123 ülevõtmisega seoses tuleb märkida, et kui Rootsi direktiivist ning eelnõukohase KrMS § 508⁸⁶ lõikest 2 tulenevalt osaleb KAPO ühtse kontaktpunkti töös uurimisasutusena, osaleb ta eelnõukohase KrMS § 508⁸⁵ lõike 4 alusel ühtse kontaktpunkti töös ka julgeolekuasutusena, vahetades kriminaalmenetluseelses või menetlusvälises etapis terrorismiohu tõrjeks vajalikku teavet.

Eelnõukohase KrMS § 508⁸⁵ lõikes 4 sätestatakse, et iga uurimisasutus osaleb ühtse kontaktpunkti töös oma pädevuse piires. Kuna JAS § 6 punkti 5 kohaselt on KAPO uurimisasutus ja JAS § 5 kohaselt ka julgeolekuasutus, on JAS § 6 punkti 2¹ kohaselt KAPO ülesanne terrorismi ja selle rahastamist ning toetamist ära hoida ja tõkestada ning selleks vajalikku teavet koguda ja töödelda. Viimati nimetatud ülesandeid täidab KAPO julgeolekuasutusena. Selleks on tal JAS § 32 lõike 3¹ alusel pädevus edastada julgeolekuasutuse ülesannete täitmisel saadud teavet teisele isikule või asutusele, sealhulgas välisriigile või rahvusvahelisele organisatsioonile, kui see on vajalik välislepingust, Euroopa Liidu õigusaktist või muust õigusaktist tulenevate kohustuste täitmiseks. Samuti annab JAS § 21¹ lõige 5 õiguse töödelda ja kasutada saadud teavet nimetatud kohustuste täitmiseks. Need sätted moodustavad

⁵⁷ Selgituseks: valdav osa teabevahetusest toimub tööpäeva raames. Reeglina on teabetaotlusele vastamiseks aega seitse päeva. Kaheksa tunni jooksul tuleb vastata vaid äärmiselt põhjendatud ja kaalukatel juhtudel siis, kui tegemist on uurimisasutusel olemasoleva teabega.

üldise õigusliku aluse KAPO osalemiseks terrorismialase teabevahetuse kontaktpunktina rahvusvahelises koostöös.

Eelnõukohase KrMS § 508⁸⁵ lõikes 4 sätestatakse, et iga uurimisasutus osaleb ühtse kontaktpunkti töös oma pädevuse piires. Kuna JAS § 6 punkti 5 kohaselt on KAPO uurimisasutus ja JAS § 5 kohaselt ka julgeolekuasutus, ei ole põhjendatud sätestada eraldi, et KAPO esindaja osaleb kontaktpunkti töös ka julgeolekuasutuse esindajana, kuna see ei kuulu KrMS-i reguleerimisesemesse ning vastava ülesande täitmine JAS-is on juba sätestatud.

JAS § 6 punktist 2¹ tulenevat ülesannet – ära hoida ja tõkestada terrorismi ja selle rahastamist ning toetamist ning selleks vajalikku teavet koguda ja töödelda – täidab KAPO julgeolekuasutusena ja direktiivi 2023/2123 kohaselt. Selleks on tal JAS § 32 lõike 3¹ alusel pädevus edastada julgeolekuasutuse ülesannete täitmisel saadud teavet välisriigile või rahvusvahelisele organisatsioonile. Samuti annab JAS § 21¹ lõige 5 KAPO-le julgeolekuasutusena õiguse töödelda ja kasutada saadud teavet nimetatud kohustuste täitmiseks. Need sätted moodustavad üldise õigusliku aluse KAPO osalemiseks terrorismialase teabevahetuse kontaktpunktina rahvusvahelises koostöös.

§ 508⁸⁷. Teabevahetuskanal

Lõike 1 kohaselt kasutavad ühtne kontaktpunkt ja uurimisasutus teiste EL-i liikmesriikide ühtse kontaktpunkti, õiguskaitseasutuse ja Europoliga teabe vahetamiseks SIENA-t.

Rootsi direktiiviga püüti leida lahendus EL-i liikmesriikide vahel õiguskaitsealase teabe edastamiseks kasutatavate sidekanalite arvukuse probleemile. Probleem seisneb selles, et mitme erineva sidekanali kasutamine takistab asjakohase teabe kiiret vahetamist ning suurendab töökoormust ja ohtu isikuandmete turvalisusele. Samuti ei võimalda mitme erineva sidekanali kasutamine Europolil täita enda rolli EL-i kriminaalteabe keskusena, põhjustades omakorda raskusi või suutmatust teha vahetatava teabe pinnalt analüüsi või vältida sama kaasuse paralleelset menetlemist mitme EL-i liikmesriigi poolt. Lisaks raskendab see võimaliku andmelekke puhul toimepanija väljaselgitamist.

Ka praegu on SIENA teabevahetuskanalina kasutuses, kuid seda ei kasutata piisavalt palju ja tõhusalt. Sageli kasutatakse teabe vahetamiseks hoopis Interpoli sidekanalit, kuna suhtlus sellel on vormivabam või kuna sellel on suurem adressaatide ring (SIENA 27 liikmesriiki⁵⁸ ja 23 partnerriiki või -organisatsiooni⁵⁹ vs. Interpol 193 riiki⁶⁰). Ühtlasi on probleemiks asjaolu, et kehtiva KrMS-i järgi ühtset kontaktpunkti teiste EL-i liikmesriikide õiguskaitseasutustega toimunud teabevahetusest ega mis tahes otsesuhtlusest alati ei teavitata. See tähendab, et riiklikul teabevahetust koordineerival kesksel üksusel ehk ühtsel kontaktpunktil ei pruugi olla terviklikku ülevaadet vahetatavast teabest. Kui ühtsel kontaktpunktil puudub ülevaade sellest, kas, millal, kui palju ja millist teavet on vahetatud ning kellega, ei ole võimalik koguda statistikat, mis aitaks võimalikke probleeme lahendada. Tegemist on ka olulise infoturbe riskiga, sest andmete konfidentsiaalsuse, terviklikkuse ja kättesaadavuse rikkumisega seonduvate intsidentide tuvastamine ja nende toimepanijate väljaselgitamine on raskendatud

⁵⁸ Europol. Liikmesriikide tabel. Kättesaadav: <https://www.europol.europa.eu/partners-collaboration/member-states>.

⁵⁹ Europol. Turvaline teabevahetusvõrk (SIENA). Kättesaadav: <https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena>.

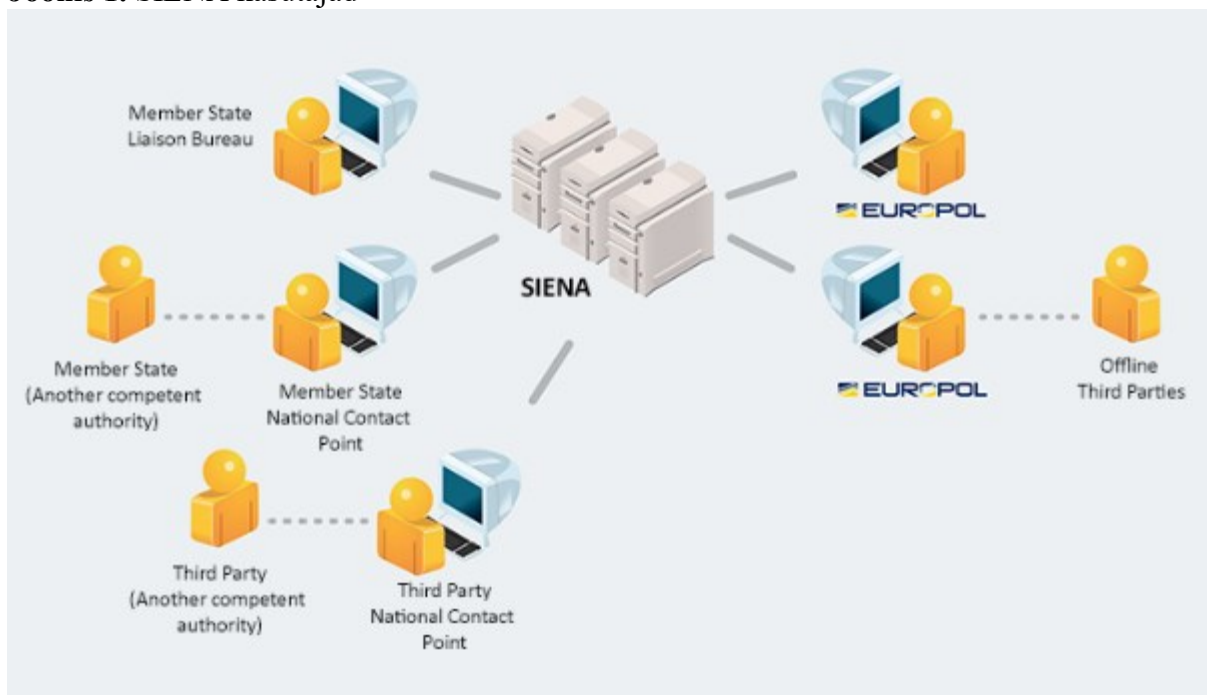
⁶⁰ Interpol. Osalisriikide tabel. Kättesaadav: <https://www.interpol.int/Who-we-are/Member-countries>.

kui mitte võimatu. Kogu suhtluse, sealhulgas kriminaalmenetluse mõistes mitteformaalse teabevahetuse, koondamine SIENA-sse maandab neid riske oluliselt.

SIENA võimaldab operatiivse ja strateegilise kuritegevusega seotud teabe kiiret ja kasutajasõbralikku vahetamist ning seda saavad kasutada:

- Europoli kontaktametnikud, analüütikud ja eksperdid;
- liikmesriigid;
- kolmandad isikud, kellega Europolil on koostöölepingud või -kokkulepped (vt joonis 1).

Joonis 1. SIENA kasutajad



Europoli andmetel on teabevahetus SIENA-s pidevas tõusutrendis. Seda eeskätt seetõttu, et piiriülesest raskest kuritegevusest enim mõjutatud EL-i liikmesriigid on avastanud selle kasutegurid. 2021. aastal on SIENA kaudu:

- registreeritud 123 000 uut juhtumit (kasv 2020. aastaga võrreldes 38%);
- vahetatud 1,54 miljonit operatiivsõnumit (kasv 2020. aastaga võrreldes 22%);
- ühendatud 2400 pädevat riiklikku asutust 51 riigist ja 14 rahvusvahelist organisatsiooni või asutust;
- ühendatud üle 19 000 lõppkasutaja⁶¹.

2024. aasta seisuga kasutab SIENA-t 3500 riiklikku pädevat asutust 27 EL-i liikmesriigist, partnerriikidest ja 16 rahvusvahelisest organisatsioonist⁶². SIENA on muutunud vaikimisi teabevahetuskanaliks erinevatele spetsialiseeritud õiguskaitseüksustele ja algatustele, näiteks varade tagaotsimise talitustele (Asset Recovery Office ehk ARO), politsei- ja tollikoostöökeskustele (Police and customs cooperation centre ehk PCCC), reisijate teabe üksustele (passenger information unit ehk PIU), rahapesu andmebüroodele (Financial

⁶¹ Andmed pärinevad Europoli veebilehelt. Kättesaadav: <https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena>.

⁶² Europol. More than 3 000 law enforcement authorities now connected to Europol, 12.04.2024. Kättesaadav: <https://www.europol.europa.eu/media-press/newsroom/news/more-3-000-law-enforcement-authorities-now-connected-to-europol>.

Intelligence Unit ehk FIU), põgenike aktiivse otsingu meeskondadele (European Network of Fugitive Active Search Team ehk ENFAST), eritaktika üksustele (association of law enforcement special intervention units ehk ATLAS), küberkuritegevuse vastase ühise tööühikuga üksustele (Joint Cybercrime Action Taskforce ehk J-CAT), Põhjamaade kontaktametnike algatusele ja Bodeni järve algatusele.⁶³ 2023. aastal kasvas SIENA kaudu vahetatud sõnumite arv ajalooliselt kõrgeima tasemeni, s.o 1,79 miljonini, mis kajastab SIENA rolli õiguskaitse eelistatud suhtluskanalina Euroopas. Samal aastal algatati SIENA kaudu üle 151 000 juhtumi. Kõige sagedamini märgitud kuritegevuse valdkonnad olid narkokaubandus, pettused ja illegaalne immigratsioon.

Kui SIENA võetakse kasutusele rohkemates riikides ja ühendatakse sellega rohkem õiguskaitseasutusi, siis saab rohkem riike ja asutusi jagada teavet kuritegelike tegevuste kohta, näiteks narkokaubanduse, inimkaubanduse, rahapesu või terrorismi kohta. Selle tulemuseks on täpsem ja põhjalikum ülevaade kuritegevuse ulatusest Euroopas – kui erinevad riigid jagavad teavet sama kuritegeliku grupi või ohu kohta, aitab see paremini mõista, kui ulatuslik on kuritegevus ja kuidas see eri riikides avaldub. Näiteks võib Saksamaa jagada teavet rahapesuga tegeleva kuritegeliku võrgustiku kohta, samas kui Leedu jagatud teave võib paljastada, et sama võrgustik on seotud ka inimkaubandusega. See suurendab ennetus- ja tabamisvõimekust, kuna õiguskaitseorganid saavad operatiivselt teavet vahetada ning kiirelt reageerida, mis võimaldab neil kuritegelikke võrgustikke varakult tuvastada, neid tõhusamalt jälgida ning lõpuks ka likvideerida. Euroopa kodaniku kasu seisneb järgmistes aspektides:

- tõhusam kuritegevusevastane tegevus tagab turvalisema elukeskkonna;
- rahvusvahelised kuritegelikud võrgustikud tabatakse kiiremini;
- vähenevad piiriülesed ohud, nagu narkootikumide, relvade ja ebaseadusliku rände riskid;
- suurenevad õiguskaitseasutuste koostöö ja vastastikune usaldus.

Kokkuvõtvalt, mida rohkem riike SIENA-t kasutab, seda parem ülevaade on EL-i turvalisust mõjutavatest kuritegelikest ohtudest ja seda tõhusam on kuritegevuse vastane võitlus.

Kuna mõned EL-i liikmesriigid ei ole seni pidanud SIENA kasutamist vajalikuks – kas seetõttu, et neil on olnud vähe kokkupuuteid piiriülese kuritegevusega või puudub piisav teadlikkus selle võimalustest –, on EL otsustanud selle olukorra parandamiseks teha SIENA kasutamise teatud juhtudel kohustuslikuks. Nimelt tuleb edaspidi kõik Rootsi direktiiviga seotud teabetaotlused edastada kohustuslikus korras SIENA kaudu. See hõlmab:

- teabetaotluste saatmist ühtsele kontaktpunktile või otse õiguskaitseasutustele;
- teabe edastamist nii vastusena taotlusele kui ka omal algatusel;
- selgituste ja täpsustuste edastamist või nende küsimist;
- teadete edastamist juhul, kui taotlust ei rahuldata;
- ning taotluste või saadud teabe koopiade edastamist ühtsele kontaktpunktile ja Europolile.

See muudatus tagab, et kõik liikmesriigid kasutavad ühtset ja turvalist teabevahetuskanalit, mis parandab koostööd ja suurendab kuritegevusevastase võitluse tõhusust kogu EL-is.

Lõikega 2 nähakse ette, et ühtne kontaktpunkt ja uurimisasutus on SIENA-ga otse ühendatud, sealhulgas mobiilseadme kaudu. Selline kohustus sätestatakse Rootsi direktiivi artikli 13

⁶³ Europol. Turvaline teabevahetusvõrk (SIENA). Kättesaadav: <https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena>.

lõikega 3. Selleks et SIENA-t saaksid kasutada eesliiniametnikud, näiteks politseioperatsioonides osalevad politseiametnikud, peab see toimima ka mobiilseadmetes, näiteks sülearvutis.

Lõike 3 järgi võib ühtne kontaktpunkt või uurimisasutus vahetada teavet ka muul viisil kui SIENA kaudu juhul, kui:

- 1) teabetaotluse kiireloomulisus eeldab ajutiselt teise teabevahetuskanali kasutamist;
- 2) SIENA-t ei ole võimalik kasutada ootamatu takistuse tõttu (nt tehnilise tõrke korral);
- 3) teavet vahetatakse EL-i-välise riigi või rahvusvahelise organisatsiooniga või on alust arvata, et seda on vaja hiljem teha, sealhulgas Rahvusvahelise Kriminaalpolitsei Organisatsiooni (Interpol) kaudu.

Erand SIENA kasutamisest on ette nähtud eesmärgiga tagada paindlikkus olukorras, kus SIENA kasutamine ei ole üldse võimalik, õigel ajal võimalik või otstarbekas. Arvestades SIENA olemasolevat kasutajaliidest, ei ole selle kasutamine igas operatiivolukorras mõeldav – eriti taktikalisel tasandil, kus eesliiniametnikelt nõutakse kiiret reageerimist ja vahetut suhtlust. Sellisteks puhkudeks on mõistlik ette näha võimalus vahetada teavet muude sidepidamisvahendite, näiteks vahetut suhtlust võimaldava raadioside või mobiiltelefoni abil. Teabe vahetamine muul viisil ei tohi olla välistatud ka olukorras, kus SIENA-t ei ole võimalik kasutada leviprobleemi või tehnikavahendi tõrkumise tõttu, sest Rootsi direktiivi eesmärk on suurendada teabele juurdepääsu. Õiguskaitseasutuste suunamine SIENA-t kasutama on vahend eelnimetatud eesmärgi saavutamiseks, mitte eesmärk iseeneses. Seda arvestades on kehtestatud ka erand suhtluses EL-i-väliste riikidega, kellel juurdepääs SIENA-le puudub või on see juurdepääs vaid nende Europolile juurde lähetatud sideohvitseridel. Võimalikult lühikese ja kiire sideahela tagamiseks on mõistlik kasutada nendega teabevahetuseks muid sidekanaleid.

Lõike 4 kohaselt tuleb aga kõik SIENA välised teabevahetused – nii nende toimumise fakt kui ka edastatud teabe sisu – registreerida esimesel võimalusel inglise keeles SIENA-s. Kuna ka uurimis- ja muu menetlustoimingu protokollid üldreegleid sisaldav KrMS § 146 ei sätesta protokollide koostamise aega ega nõua selle koostamist toimingu ajal või vahetult pärast seda, on teabe SIENA-sse talletamise aeg jäetud paindlikuks. Seega võib kiireloomulise teabevahetuse sisestada SIENA-sse tagantjärele, et jääks alles nii teabevahetuse fakt kui ka selle sisu. Oluline on, et infosüsteemi jääks jälg nii toimunud teabevahetusest kui ka vahetatud teabe sisust, et tagada teabevahetuse läbipaistvus ja usaldusväärsus kogu menetlusahela ulatuses. Näiteks võib ühe liikmesriigi õiguskaitseasutus edastada kiireloomulise operatiivinfo teise EL-i liikmesriigi partnerile suulise või muu vahetu kanali kaudu – näiteks teabe isiku võimaliku asukoha kohta, mis annab aluse viivitamatuks kinnipidamiseks. Kui toimingu viib läbi teise EL-i liikmesriigi õiguskaitseasutus ning hiljem tekib küsimus selle menetlusliku korrektsuse või õiguspärasuse kohta, on oluline, et süsteemis oleks selgelt dokumenteeritud, kuidas ja kelle vahel teave liikus ning millele tugines vastav otsus. Selline dokumenteerimiskohustus toetab läbipaistvust ja vastutuse jälgitavust ning aitab maandada õiguskaitseasutuste koostöös tekkivaid õiguslikke ja operatiivseid riske. Samuti on see oluline tõendite säilitamise, järelevalve ja EL-i õiguse kohaste põhiõiguste tagamise seisukohalt. See on vajalik, et oleks võimalik tuvastada andmete konfidentsiaalsuse, terviklikkuse ja kättesaadavuse rikkumisi ning teha kindlaks nende toimepanijad. Samuti tagab see Europolile juurdepääsu kogu vahetatud teabele, mis on vajalik tema rolli täitmiseks EL-i kriminaalteabe keskusena, ning võimaldab ühtsel kontaktpunktil saada täielikku ülevaadet oma riigi osalusel toimunud teabevahetusest.

Samuti täpsustatakse sättes, et ka sellistel juhtudel, kui teavet on vahetatud muude sidepidamisvahendite kaudu, tuleb teabevahetuse talletamisel SIENA-s kinni pidada eelnõukohase KrMS § 508⁸⁵ lõikes 6 sätestatud keelenõudest, mille kohaselt peab teabevahetus toimuma vaid inglise keeles. Tulenevalt suulise teabevahetuse lubatavusest vaid erandjuhtudel,

mil kirjalik teabevahetus ei ole kas kiireloomulisuse või SIENA kasutamise takistuste tõttu võimalik, ei ole võimalik ka SIENA-s pakutava masintõlke kasutamine. Andmetöötluse minimaalsuse põhimõtet silmas pidades tuleb hoida isikuandmete töötlus võimalikult väikeses ringis, mistõttu ei ole suulise tõlke tagamine sellistes olukordades otstarbekas. Suhtluses kolmandate riikide või rahvusvaheliste organisatsioonidega tuleb lähtuda kahepoolsetest kokkulepetest või objektiivsetest võimalustest. Ehkki rahvusvaheline suhtlus toimub valdavalt inglise keeles, ei pruugi see olla iga kolmanda riigi või rahvusvahelise organisatsiooniga võimalik, eriti kiireloomulistel juhtudel. Küll aga on võimalik talletada teabevahetus tagantjärele SIENA-s inglise keeles.

§ 508⁸⁸. Edastatav teave

Sättega määratletakse andmed, mida teabevahetuse käigus vahetatakse. Kehtivas õiguses vastav määratlus puudub.

Lõike 1 kohaselt tuleb teise EL-i liikmesriigi ühtse kontaktpunkti või õiguskaitseasutuse ja Europoliga vahetada Eesti ühtsele kontaktpunktile ja uurimisasutusele otse või kaudselt kättesaadavat teavet. Mõlemad terminid on toodud Rootsi direktiivi artiklis 2.

Otse juurdepääsetav teave on andmekogus sisalduv teave, millele on Eesti ühtsel kontaktpunktil ja uurimisasutustel juurdepääs oma tavapäraste tööülesannete raames. See tähendab, et tegu on andmetega, millele kontaktpunkti või uurimisasutuse ametnik pääseb ligi ilma lisakokkulepeteta või eritaotlusteta.

Teise EL-i liikmesriigi ühtsel kontaktpunktil ja õiguskaitseasutusel puudub otsejuurdepääs Eesti andmekogudes olevatele andmetele. Teabetaotluse esitamise korral tuleb need teise riigi kontaktpunktile edastada. Otse juurdepääsetava teabe näitena võib tuua infosüsteemis POLIS olevad andmed, aga ka andmed, millele on infosüsteemi POLIS kaudu võimalik juurde pääseda. Näiteks saab infosüsteemi POLIS kaudu pärida andmeid rahvastikuregistrist, äriregistrist või kinnistusraamatust. Juurdepääs eelkirjeldatud teabele on ühtsele kontaktpunktile juba praegu tagatud. Uurimisasutuse roll POLIS-e kaudu tehtavate päringute puhul seisneb eelkõige selles, et nad kooskõlastavad teabe edastamise või keelduvad selle edastamisest, kui esineb keeldumisaluseid.

Kuigi Rootsi direktiivi põhjenduse nr 28 kohaselt peaks ühtsel kontaktpunktil olema juurdepääs kogu liikmesriigis kättesaadavale teabele, ei ole Eesti ühtsel kontaktpunktil praegu siiski juurdepääsu kõikide Eesti uurimisasutuste teabele ja infosüsteemidele. Kui ühtne kontaktpunkt saab teabepäringu, millele vastamiseks tal endal juurdepääsu ei ole, vastutab teabe edastamise eest uurimisasutus, kellel see teave on. Uurimisasutus peab olema valmis andmeid edastama ka ööpäev läbi.

Menetlus on järgmine:

1. ühtne kontaktpunkt tuvastab, et päring kuulub konkreetse uurimisasutuse pädevusse;
2. ühtne kontaktpunkt teavitab uurimisasutust ja selgitab välja, kas nõutav teave on neil olemas;
3. kui teave on olemas, peab ühtne kontaktpunkt saama uurimisasutuselt loa selle edastamiseks;
4. uurimisasutus kontrollib, kas esinevad keeldumisalused. Kui neid ei ole, edastab uurimisasutus andmed ühtsele kontaktpunktile turvalise sidekanali, näiteks SIENA, kaudu.

Kaudselt juurdepääsetav teave on teave, mida ühtne kontaktpunkt või uurimisasutus võib saada ilma riiklikku sundi⁶⁴ rakendamata teiselt riigi või kohaliku omavalitsuse asutuselt või füüsiliselt või juriidiliselt isikult. Kaudselt juurdepääsetavaks teabeks on näiteks teave, mida ühtne kontaktpunkt või uurimisasutus küsib eraldi riigisisese päringu abil. Tegemist on andmetega, millele uurimisasutuse ametnikul enda tavapärase töö raames iseseisvat juurdepääsu ei ole.

Kaudselt juurdepääsetav teave on näiteks kohalikult omavalitsuselt saadud vastus e-kirjale, milles uurimisasutus on palunud neil väljastada huvialuse isiku kontaktandmeid. Samuti on kaudselt juurdepääsetav teave kriminaalmenetluse välise vestluse käigus saadav teave. Näitena võib tuua olukorra, kus teine EL-i liikmesriik soovib tuvastada mõne sündmuse tunnistajaid. Ehkki teada võib olla võimalike tunnistajate ring, ei pruugi ressursi piiratuse tõttu olla mõistlik kõiki neid menetlusele allutada ja tunnistajatena üle kuulata. Selleks et teavet sooviv EL-i liikmesriik oskaks esitada KrMS §-s 489³⁷ nimetatud EIO konkreetsete isikute ülekuulamiseks tunnistajana, võib olla asjakohane sellised isikud võimalike tunnistajate ringist välja selgitada vestluse abil ning allutada menetlustoimingule vaid need isikud, kellel reaalselt sündmuse kohta teavet on. Mõistagi on selline menetluseelne vestlus isikule vabatahtlik, ent heauskse tunnistaja puhul ei tohiks see osutuda probleemiks. Seevastu objektiivne õigus peaks tagama võimaluse liikmesriikidele sellisel viisil teavet koguda ja vahetada.

Lõikega 2 nähakse ette, et teavet edastatakse samadel tingimustel ja ulatuses nagu riigisisises teabeedastuses. Sellega võetakse KrMS-i üle Rootsi direktiivi artikli 3 punktis b toodud samaväärse juurdepääsu põhimõtte, mille kohaselt tagab iga EL-i liikmesriik, et teise liikmesriigi ühtselt kontaktpunktilt või õiguskaitseasutuselt teabe taotlemise tingimused ning neile teabe edastamise tingimused on samaväärsed tingimustega, mida kohaldatakse asjaomases EL-i liikmesriigis sarnase teabe taotlemise ja edastamise suhtes. Praegu pärsib tõhusat andmevahetust see, et EL-i liikmesriigid tagavad andmete kättesaadavuse oma partneritele teistes EL-i liikmesriikides väga erinevalt. Sellega kaasneb teabevahetuse tõhususe killustumine liikmesriikide üleselt. Kui õiguskaitseasutused ei suuda vahetada kiiresti kriminaalteavet teiste EL-i liikmesriikide õiguskaitseasutustega, on kurjategijate tabamine piiriüleste kuritegude või kurjategijate piiriülese liikumise puhul keerukas kui mitte võimatu.

Lõikega 2 sätestatav samaväärse juurdepääsu põhimõtte ei tähenda seejuures ühetaoliste menetlus- ega materiaalõiguslike reeglite kehtestamist kogu EL-is, vaid väljendab võrdse kohtlemise põhimõtet: teise liikmesriigi õiguskaitseasutust tuleb käsitleda samaväärselt oma riigi uurimisasutusega juhul, kui ta taotleb samu andmeid samal eesmärgil. Seda põhimõtet rakendatakse teabele juurdepääsu ulatusele ja juurdepääsupiirangutele, sealhulgas salastatuse taseme määramisele. Teisisõnu, kui näiteks Eestis edastatakse teatud teavet PPA ja MTA vahel, tuleb samas ulatuses teavet võimaldada ka teise liikmesriigi õiguskaitseasutusele – tingimusel, et taotlus vastab sisult ja eesmärgilt sarnasele riigisisesele olukorrale. Sellise andmevahetuse puhul ei tohi teise liikmesriigi asutusele kehtestada rangemaid nõudeid, kui kohaldatakse riigisisiselt.

On oluline rõhutada, et samaväärse juurdepääsu põhimõtet ei kohaldata teabevahetuse neile aspektidele, mis on direktiiviga EL-i tasandil ühtselt ja siduvalt ette nähtud: nimelt vastamistähtaegadele ja teabe andmisest keeldumise alustele. Direktiiviga ette nähtud tähtaja- ja keeldumispõhjuseid tuleb aga käsitada autonoomselt, st need ei sõltu enam riigisisestest õigusest, vaid tulenevad otseselt EL-i õigusest – need on reguleeritud ühtlustatult direktiivis endas ning liikmesriigid ei või kehtestada lühemaid või pikemaid tähtaegu ega kitsendada ega

⁶⁴ Selgitus: riikliku sunni rakendamata jätmine tähendab, et teabe saamiseks ei kasutata seaduslikke sunnivahendeid, näiteks kohtu korraldust, trahve või muud sunniviisilist tegevust. Antud kontekstis on tegemist teabega, mida saab vabatahtlikult või koostöö kaudu, ilma et oleks vaja rakendada sunnimeetmeid.

laiendada keeldumise aluseid võrreldes sellega, mis on direktiivis sätestatud. Need ei kuulu liikmesriigi kaalutlusõiguse alla ja neis küsimustes ei tohi riigid direktiivist kõrvale kalduda.

Samuti ei kuulu liikmesriigi kaalutlusõiguse alla teisest EL-i liikmesriigist saadud teabe juurdepääsupiirangute muutmine – selleks ei ole teabe saanud EL-i liikmesriigil õigust. Vastav nõue tuleneb Rootsi direktiivi artikli 3 punktides c ja d sätestatud konfidentsiaalsuse ja andmete omandiõiguse põhimõtetest. Teabe avalikustamise puhul kehtib teabe omandiõiguse põhimõte, mille kohaselt teabe esmane omanik määrab, mis ulatuses ja millistel tingimustel teavet avalikustada tohib. Eeltoodu tähendab, et kui tekib konflikt riigisiseste õigusaktide ja teiste EL-i liikmesriikide õiguse vahel – näiteks juhul, kui ühe liikmesriigi õigus ei luba teavet avalikustada, samas kui teises liikmesriigis oleks see lubatud või isegi nõutav –, tuleb teabe avalikustamisel lähtuda selle riigi õigusest ehk seatud reeglitest, kellelt teave pärineb.

Reeglina tuleb ühes EL-i liikmesriigis kuriteo kohta olemasolev või kättesaadav teave teha (teatavate eranditega⁶⁵) kättesaadavaks ka teistele liikmesriikidele. Seevastu sellise teabe avaldamist andmesubjektidele tuleb piirata, kui selleks on õiguslik alus ja objektiivne vajadus. Kriminaalmenetluse andmete puhul tuleneb Eesti õiguses vastav alus eeskätt KrMS § 15² lõigetest 4 ja 5, aga andmesubjekti juurdepääsuõigust tuleb suurel osal juhtudest piirata ka [avaliku teabe seaduse](#) (edaspidi *AvTS*) § 35 lõike 1 punktide 1 (kriminaalmenetluses kogutud teave, mis ei kuulu avaldamisele), 3 (teave, mille avalikuks tulek kahjustaks riigi välissuhtlust), 5¹ (teave uurimisasutuse tegevuse meetodite ja taktika kohta, kui selle avalikuks tulek võib raskendada süütegude avastamist või soodustada nende toimepanemist), 11 (teave süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist) ja 12 (isikuandmed, kui nendele juurdepääsu võimaldamine kahjustaks oluliselt andmesubjekti eraelu puutumatust) alusel. Rootsi direktiivi artikli 3 punkti c kohaselt on EL-i liikmesriik kohustatud talle usaldatud teavet vastavalt teabe edastanud EL-i liikmesriigi nõuetele kaitsma.

Lõikega 3 on võimalike rikkumiste vältimiseks sõnaselgelt välja toodud, et kaudselt juurdepääsetava teabe puhul ei saa uurimisasutus tugineda KrMS § 215 lõikele 1, mille kohaselt on uurimisasutuse määrused ja nõuded nende menetluses olevates kriminaalasjades täitmiseks kohustuslikud kõigile kogu Eesti Vabariigi territooriumil. KrMS § 215 lõikes 1 nimetatud juhul on esmane takistus asjaolu, et teise EL-i liikmesriigi õiguskaitseasutuse teabetaotlus tehakse selle teise liikmesriigi menetluses olevas kriminaalasjas või kuriteo osas, mille menetluse pädevus ei kuulu reeglina Eestile. Teine takistus on aga asjaolu, et selline nõue on tagatud riikliku sunniga. KrMS § 215 lõike 3 kohaselt võib KrMS § 215 lõikes 1 nimetatud kohustuse (nt uurimisasutuse nõudekirjale vastamine) täitmata jätnud menetlusosalist, kriminaalmenetluses osalevat muud isikut või menetlusvälist isikut prokuratuuri taotlusel eeluurimiskohtunik kohtumääruse alusel trahvida. Küll aga on lubatud see, kui uurimisasutus esitab isikule vabatahtlikuks täitmiseks (nt samasisulise, ent viitamata KrMS § 215 lõikele 1) päringu. Sellisel juhul jääb päringule vastamine või vastamata jätmine adressaadi diskretsiooniks. Teisisõnu, kui adressaat uurimisasutuse päringule ei vastata, siis ei saa talle seetõttu järgneda KrMS-ist tulenevaid sanktsioone.

Eelnõukohase KrMS § 508⁸⁸ lõikega 4 tuuakse eraldi välja, et kohtueelse menetluse andmeid võib avaldada KrMS §-s 214 sätestatud tingimustel ja korras ehk vaid prokuratuuri loal ja määratud ulatuses. Erandina⁶⁶, kui teabetaotlusele vastamisel tuleb avaldada kohtumenetluse

⁶⁵ Selgitus: näiteks juhul, kui taotletud teabe edastamine on vastuolus julgeolekuhuvidega, seab ohtu kuriteo käimasoleva uurimise edukuse vms.

⁶⁶ Selgitus: üldjuhul on kohtupidamine ning kohtuotsuse kuulutamine avalikud, ent kaalukal vajadusel võib kohus seaduses ettenähtud juhtudel, näiteks KrMS § 12 kohaselt, perekonna- ja eraelu kaitseks või alaealise või kannatanu huvides, kuulutada kohtuistungit või selle osa kinniseks.

käigus käsitletud teavet, mille avaldamiseks on vaja kohtu luba (nt kinniseks kuulutatud istungi või lahendi puhul), tuleb see luba kohtult saada. Põhimõtteliselt ei oleks vaja kriminaalmenetluse üldreeglitele eraldi viidata, kuna eelnõus ei nähta ette erireeglit nendest kõrvale kaldumiseks. Üldreegli sõnaselge toonitamata jätmine ei oleks aga õiguse rakendaja seisukohast parim lahendus, kuna muudaks regulatsiooni raskesti jälgitavaks. Otstarbekuse ja õigusselguse⁶⁷ huvides on üldreeglite kohaldamist toonitatud eraldi EL-i liikmesriikidega teabevahetust reguleerivas jaotises.

Kui teabetaotluses küsitud teabe edastamiseks on vaja kohtu või prokuratuuri luba (edaspidi koos *teabevahetusluba*), tuleb eelnõu järgi tagada sellise taotluse lahendamine ööpäev läbi.

Rootsi direktiivi põhjendusega nr 22 kohustatakse ühtset kontaktpunkti ja asjakohasel juhul pädevat õiguskaitseasutust võtma kõik praktilised ja õiguslikud meetmed, et teha koostööd teabetaotluse esitanud EL-i liikmesriigi ühtse kontaktpunkti või volitatud õiguskaitseasutusega. Eesmärk on tagada teabevahetusloa kiire kättesaadavus ning vältida viivitusi ja tõrkeid.

Selleks et tagada ühtsele kontaktpunktile esitatud teabetaotluste kiire menetlemine, nähakse Rootsi direktiiviga ette selged tähtajad, mis võtavad arvesse taotluse kiireloomulisust ja uurimisasutuse juurdepääsu teabele. Rootsi direktiivi artikli 5 lõikega 1 nähakse ette selged tähtajad teabetaotlusele vastamiseks (sama regulatsioon on toodud eelnõukohases KrMS § 508⁹² lõikes 1 ning lõike 2 punktides 1 ja 2):

- **üldjuhul** tuleb teisele EL-i liikmesriigile vastata **seitsme päeva** jooksul (kehtivas KrMS-is on vastav tähtaeg 14 päeva);
- **kiireloomuliste taotluste korral**:
 - **8 tunni jooksul**, kui teave on otse juurdepääsetav (kehtiva KrMS § 508⁸² lõige 1);
 - **3 päeva jooksul**, kui tegu on kaudselt juurdepääsetava teabega, st vajatakse uurimisasutuse vahendust.

Kui teabe avaldamiseks on vaja teabevahetusluba, tuleb see luba või keeldumine anda eespool nimetatud tähtaegade jooksul. Tähtajast on lubatud kõrvale kalduda üksnes erandlikel juhtudel, näiteks kui taotluse keerukus eeldab lisaaega. Rootsi direktiivi artikli 5 lõike 2 kohaselt ka siis, kui soovitud teabe edastamiseks on vajalik õigusasutuse luba. Sellistel puhkudel tuleb KrMS-i §-st 214 tulenevalt tagada, et ka õigusasutus on kontaktpunkti jaoks kättesaadav – kas füüsiliselt kontaktpunkti ruumides või näiteks telefoni teel. Seda eriti olukorras, kus uurimisasutus ei asu samas hoones kui prokuratuur või kohus.⁶⁸

Olukorrad, kus uurimisasutusel tuleb teabetaotlusele vastamiseks küsida luba prokuratuurilt, või veel enam – kohtult, on siiski pigem erandlikud. Üldreeglina ei ole Rootsi direktiivi alusel tehtud teabetaotluste alusel saadud teave menetluses kasutatav ning Europolil andmetel moodustavad 80% SIENA kaudu esitatud teabetaotlustest küsimused, kas EL-i liikmesriigil on isiku X kohta teavet või mitte.⁶⁹ Sellest hoolimata tuleb prokuratuuril ja kohtul niisuguste lubade andmise võimekus ööpäevaringselt tagada, kuivõrd Rootsi direktiivi põhjenduspunkti 22 kohaselt tuleb riigisisest ja liikmesriikide vahelist teabevahetust käsitleda menetluslikult samaväärsel viisil. Siseriiklikult on õigusasutuste reageerimisvalmidus tagatud nn valveprokuröride ja kohtunike näol, s.o [kohtute seaduse](#) § 6 lõikes 4 sätestatud kohtuniku valveaja ja [prokuratuuriseaduse](#) § 22² lõikes 1 sätestatud prokuröri valveaja kaudu. Eelnimetatute puhul on tegemist ajaga, mil prokurör või kohtunik peab olema töövälisel ajal

⁶⁷ Õigusselguse põhimõte tuleneb PS § 13 lõikest 2.

⁶⁸ Rootsi direktiivi põhjendus nr 28.

⁶⁹ Europolil ettekanne. Prüm II määruse ülevõtmise teemaline konverents 30. aprillil 2024. aastal Brüsselis.

kättesaadav ettenägematute või edasilükkamatute teenistusülesannete täitmiseks. Selline regulatsioon on aga Rootsi direktiivi ülevõtmiseks liiga üldsõnaline.

Praktikas tähendab prokuröride ja kohtunike valveaeg seda, et töövälisel ajal on prokuratuuri ja kohtute kontaktiks valveprokurörid ja -kohtunikud graafiku alusel. See tähendab, et taotlusi valveajal peavad lahendama isikud, kelle menetluses kriminaalasi, mille kohta teavet taotletakse, ei ole olnud. Seega ei ole neil võimalik anda ka lõplikku luba andmete edastamiseks, sest sisulise loa saab anda vaid prokurör või kohtunik, kelle menetluses konkreetne kriminaalasi on või on olnud.

Kuivõrd Rootsi direktiivi põhjenduspunkti 22 kohaselt ei tulene direktiivist õigusasutustele uusi kohustusi, välja arvatud nõue kohaldada nende suhtes tingimust, et riigisisest ja liikmesriikide vahelist teabevahetust käsitletakse menetluslikult samaväärsel viisil, on ka muudatuse järgselt põhjendatud teabetaotlusele vastamise tähtaja peatumine. Muudatus loob üksnes eelduse tagada valmisolek selliste taotluste prioriteetseks menetlemiseks esimesel võimalusel, näiteks vaadatakse kell 01.21 laekunud taotlus läbi samal päeval ning kell 23.59 saabunud taotluse menetlemine toimub järgmisel päeval esimese prioriteedina.

§ 508⁸⁹. Teabekasutuse tingimused

Lõike 1 kohaselt on teise liikmesriigi ühtselt kontaktpunktilt või õiguskaitseasutuselt saadud teabe kasutamine, sealhulgas kohtumenetluses tõendina, lubatud selle teise riigi pädeva asutuse nõusolekul ja tingimustel.

Rootsi direktiivi kohase teabevahetuse käigus saadud teabe suhtes kehtib vaikimisi eeldus, et selle kasutamine tõendina ei ole lubatav. Tõendina kasutamiseks mõeldud teabe saamiseks tuleb EL-i liikmesriigil reeglina esitada EIO. Vaikimisi kehtivat tõendina kasutamise keeldu ei kohaldata mõistagi juhul, kui teavet edastav riik on nõustunud teabevahetuse taotluses märgitud teabe kasutamise eesmärgiga või andnud teabe edastamise ajal või hilisemalt loa teabe taotleja soovitud eesmärgil kasutamiseks. Eelkirjeldatu lähtub andmete omandiõiguse põhimõttest, st andmete esialgsel omanikul on õigus otsustada nende edasise töötlemise tingimuste üle. Nagu eespool selgitatud (vt seletuskirja punkt 2.1), aitab Rootsi direktiivi kohane teabevahetus kaasa sihistatud EIO esitamisele, vähendades seeläbi asutuste töökoormust tarbetu EIO koostamisel ja menetlemisel.

Lõike 2 kohaselt, kui teave on saadud EL-i-väliselt riigilt, võib selle edastada teisele liikmesriigile, Europolile või rahvusvahelisele organisatsioonile EL-i-välise riigi pädeva asutuse nõusolekul ja tingimustel.

See reegel juhindub eelkõige andmete omandiõiguse põhimõttest.⁷⁰ Andmete omandiõiguse põhimõtte kohaselt otsustab teabe kasutamise tingimused, sealhulgas sellele seatavad juurdepääsupiirangud riik, kellelt teave algselt pärineb. Riik, kellelt teave algselt pärineb, võib olla EL-i liikmesriik või kolmas ehk EL-i-väline riik. Kui ühtne kontaktpunkt või uurimisasutus soovib edastada teise EL-i liikmesriigi kontaktpunktile või õiguskaitseasutusele teiselt riigilt

⁷⁰ EL-is on andmekaitse ja eraelu puutumatuse peamine õigusakt [Euroopa Liidu isikuandmete kaitse üldmäärus](#) (edaspidi *IKÜM*, milles küll otseselt ei käsitleta omandiõigust, kuid määratletakse üksikisikute õigused oma isikuandmete üle. *IKÜM*-is sätestatakse, et isikuandmed kuuluvad isikule, kelle kohta need käivad, andes neile õigused oma andmete üle otsustada, sealhulgas õiguse nõuda andmete kustutamist, parandamist ja edastamist. *IKÜM*-i artiklites 12–23 käsitletakse andmesubjektide õigusi, sealhulgas õigust andmete kustutamisele („õigus olla unustatud“), andmete parandamisele ja ülekandmisele, mis on seotud andmete omandiõiguse põhimõttega andmesubjekti seisukohast.

saadud teavet, tuleb enne teabe edastamist saada sellelt riigilt, kellelt teave algselt pärines, enne teabetaotlusele vastama asumist nõusolek ja nõuded teabe käitlemisele (nt juurdepääsupiirangu tase ja sellise juurdepääsupiiranguga teabe käitlemisnõuded). Seejuures kehtib teabe kasutamise ja avalikustamise piirang ka teabetaotluse enda kohta. Kui teabetaotluses ei ole märgitud, et taotlust või selle esitamise fakti on lubatud jagada teiste osapooltega kui selle adressaadid, ei tohi seda ilma taotluse esitaja loata teha.

2. alljaotis **Teabetaotlusele vastamine**

§ 508⁹⁰. Teabetaotlusele vastamine

Teabevahetus toimub üldjuhul ühtse kontaktpunkti kaudu. Kõnesoleva sättega võetakse Eesti õigusesse üle Rootsi direktiivi artiklis 4 esitatud põhimõtted.

Lõikega 1 nähakse ette, et ühtne kontaktpunkt vastab teise liikmesriigi ühtse kontaktpunkti või õiguskaitseasutuse teabetaotlusele või edastab selle vastamiseks uurimisasutusele.

Lõike 2 kohaselt kontrollib ühtne kontaktpunkt enne teabetaotlusele vastamist või selle uurimisasutusele vastamiseks edastamist, kas:

- 1) taotlus vastab KrMS § 508⁹⁵ nõuetele;
- 2) esineb KrMS § 508⁹¹ lõikes 1 sätestatud keeldumise alus.

Ühtne kontaktpunkt kontrollib saabunud teabetaotluse nõuetekohasust, sellele vastamise võimalikkust (s.o kas teave on olemas) ja lubatavust (st keeldumisaluste puudumist) ning vastab taotlusele ise või edastab selle vastamiseks ühele või mitmele uurimisasutusele. Kui ühtsel kontaktpunktil on taotletud teabele juurdepääs, vastab ta teabetaotlusele ise, kooskõlastades teabe edastamise vajadusel eelnevalt teabe omaniku ehk uurimisasutusega, kes on selle infosüsteemi sisestanud. Kui ühtne kontaktpunkt tuvastab, et teabetaotlusele vastamine on mõne sellise uurimisasutuse pädevuses, kelle teave ei ole infosüsteemi POLIS kaudu juurdepääsetav, teavitab ta uurimisasutust teabetaotluse laekumisest ning selgitab välja, kas uurimisasutusel on taotletud teavet, ja teabevahetuse lubatavuse. Teabevahetusest keeldumise aluste puudumisel vastab uurimisasutus ise SIENA kaudu saabunud teabetaotlusele või edastab teabe ühtsele kontaktpunktile, kes korraldab teabetaotlusele vastamise. Edastades teabetaotluse täitmiseks mitmele uurimisasutusele, vastutab ühtne kontaktpunkt koondvastuse koostamise eest.

Teabevahetusprotsessi tõhusaks toimimiseks on eelnõu § 508-86 lõike 2 punkti 1 kohaselt sätestatud, et ühtse kontaktpunkti töös osaleb iga uurimisasutuse esindaja. See lahendus aitab tagada, et igal uurimisasutusel on vähemalt oma esindaja kaudu juurdepääs SIENA-le. See, kas ja millisel määral iga uurimisasutus tutvub Eestile laekuvate teabetaotlustega, on nende enda otsustada, kuid võimalus selleks luuakse. Lisaks toimib uurimisasutuse esindaja ühtsele kontaktpunktile sisuliselt sideohvitserina, otsesuhtluse kanalina, kelle kaudu on võimalik kiiresti selgitada, kas teabetaotlusele vastamine kuulub uurimisasutuse pädevusse, kas uurimisasutusel on taotletavat teavet ning, kui see on olemas, kas esinevad teabe edastamisest keeldumise alused ning millised on teabe kasutamise piirangud. Vajadusel annab esindaja ka võimaluse kiiresti tuvastada teabe saanud ametnik ning otsesuhtluses täpsustada teabe kasutamise piiranguid, riske ja töötlemise piirangu vajadusi.

Arvestades Rootsi direktiivi põhjenduses nr 19 toodut, peab ühtne kontaktpunkt taotluse saamisel hindama, kas taotletud teave on kuritegude tõkestamiseks, avastamiseks või

uurimiseks (KrMS-i mõistes menetlemiseks) vajalik ja proportsionaalne ehk kas taotluse aluseks olevad asjaolud ja selgitused on piisavalt selged ja üksikasjalikud selleks, et teabetaotlusele vastata. Eeltoodu tähendab, et teabetaotluse saamisel peab ühtne kontaktpunkt iga kord kaalutlema teabetaotluse asjakohasust ja vajalikkust selleks, et vältida põhjendamatut või ebaproportsionaalselt suures koguses teabe edastamist. Vajadusel tuleb ühtsel kontaktpunktil kaalutlusele kaasata taotletud teabe omanik ehk uurimisasutus, kes on selle teabe infosüsteemi sisestanud.

Kuna reeglina toimub kogu teabevahetus läbi ühtse kontaktpunkti, kes on SIENA vilunud ja ööpäevaringne kasutaja, omab terviklikku ülevaadet kogu teabevahetusest, mille osapool on Eesti (SIENA teabevahetuse puhul toimub see vaikimisi), ning korraldab seda, vastutab teabevahetuse nõuetekohasuse eest reeglina ühtne kontaktpunkt. See aga ei tähenda, et uurimisasutusel puudub igasugune kohustus temale edastatud teabetaotlusi kontrollida. Uurimisasutus peab kontrollima teabetaotluse nõuetekohasust ja keeldumisaluste puudumist siis, kui ta asub eelnõukohase KrMS § 508⁸⁵ lõike 4 järgi ise oma pädevuse piires teavet vahetama, sealhulgas teabetaotlusele iseseisvalt vastama. Sellisel juhul tuleb uurimisasutusel järgida teabevahetusel ühtse kontaktpunktiga samu nõudeid.

Lõikega 3 nähakse ette, et kui teabetaotluses on puudusi, mille kõrvaldamata jätmise korral tuleks sellele vastamisest keelduda, teavitab ühtne kontaktpunkt sellest viivitamata taotluse esitanud EL-i liikmesriigi ühtset kontaktpunkti või õiguskaitseasutust ning palub puudused kõrvaldada. Puuduste kõrvaldamiseks tuleb teabetaotluse esitajale selgitada, millised on puudused, pakkuda vajadusel abi nende kõrvaldamiseks ning hoiatada, et puuduste kõrvaldamata jätmine toob kaasa vastamisest keeldumise vastavalt eelnõukohase KrMS § 508⁹¹ lõike 1 punktile 5. Eelnõuga reguleeritakse KrMS-is haldusorgani omal algatusel selgitamiskohustuse täitmist selleks, et tagada teabevahetuse osapoolte õiguste ja ressursside tõhus kasutamine. Vastasel juhul võib kummalegi osapoolle tekkida kahju pikemalt sama küsimusega tegelemisest ning suutmatusest õigel ajal reageerida. Selgitamiskohustuse KrMS-is sätestamise vajadus tuleneb Rootsi direktiivi põhjendusest nr 20, mille kohaselt tuleb vältida tarbetut taotlustele vastamisest keeldumist ning võimaldada taotluse saajal nõuda selgitusi või täpsustusi. Samuti Rootsi direktiivi artikli 6 lõikest 3, mille kohaselt peab teabetaotluse saaja viivitamata küsima taotluse esitajalt selgitusi ja täpsustusi, kui vastasel juhul tuleks teabetaotlusele vastamisest keelduda.

Tuleb rõhutada, et lisaks teabetaotluses esinevate puuduste kontrollimisele, mille kõrvaldamine ei too kaasa vastamisest keeldumist, on ühtsel kontaktpunktil kohustus kontrollida, ega teabetaotlus ei sisalda eelnõukohase KrMS § 508⁹¹ lõike 1 punktides 1–12 sätestatud aluseid teabe edastamisest keeldumiseks.

Lõikega 4 sätestatakse, et kui KrMS § 508⁹¹ lõikes 1 sätestatud keeldumise aluste esinemise kontrollimisel on vaja teabetaotluse kohta selgitusi või täpsustusi, palub ühtne kontaktpunkt neid teise liikmesriigi ühtselt kontaktpunktilt või õiguskaitseasutusest viivitamata. See on vajalik teabetaotlusele vastamise lubatavuse otsustamiseks. Sätte eesmärk on tagada, et otsused teabetaotluse menetlemisel ei põhineks puudulikul või ebaselgel teabel. Praktikas tähendab see, et kuigi teabetaotluse vormi- ja sisunõuded võivad olla täidetud, võib siiski osutuda vajalikuks hinnata täiendavalt taotluse proportsionaalsust ning andmete taotlemise põhjendatust. Enne lõpliku keeldumisotsuse tegemist tuleb anda võimalus asjaolusid täpsustada ning küsida lisaselgitusi, mis aitavad hinnata taotluse sisulist põhjendatust ja proportsionaalsust. Selline lähenemine toetab rahvusvahelise koostöö tõhusust ja õiguspärasust, aidates ennetada põhjendamatuid keeldumisi, ning tugevdab vastastikust usaldust liikmesriikide õiguskaitseasutuste vahel.

Lõikega 5 nähakse ette, et kui Eesti ühtne kontaktpunkt edastab teabetaotluse vastamiseks uurimisasutusele, siis uurimisasutus kontrollib teabetaotluse vastavust §-s 508⁹⁵ sätestatud nõuetele ja § 508⁹¹ lõikes 1 sätestatud keeldumise aluste esinemist ning seejärel:

1. koostab vastuse ja edastab selle viivitamata Eesti ühtsele kontaktpunktile, kes omakorda vastab teise EL-i liikmesriigi ühtsele kontaktpunktile või õiguskaitseasutusele; või
2. vastab taotlusele oma pädevuse piires iseseisvalt KrMS §-s 508⁹² sätestatud tähtajal, saates vastuse otse teise EL-i liikmesriigi õiguskaitseasutusele või ühtsele kontaktpunktile, edastades samal ajal vastuse koopia Eesti ühtsele kontaktpunktile. Seejuures peab uurimisasutus eelnõukohase KrMS § 508⁹⁰ lõike 5 punkti 2 kohaselt järgima kõiki KrMS-i 10. jaotise „Teabevahetus Euroopa Liidu liikmesriikide vahel ja Europoliga“ sätteid, mis kehtivad muidu üldreeglina Eesti ühtse kontaktpunkti kohta. Selline regulatsioon tagab selged ja paindlikud põhimõtted teabevahetuseks Eesti uurimisasutuste ning teiste EL-i liikmesriikide õiguskaitseasutuste vahel, võimaldades nii koordineeritud kui ka iseseisvat vastamist sõltuvalt juhtumi asjaoludest.

Erinevad vastamise viisid on ette nähtud selleks, et säilitada paindlikkus ning tagada tõhus teabevahetus. Üldjuhul toimub teabevahetus Eesti ja teiste EL-i liikmesriikide vahel ühtse kontaktpunkti kaudu, kes vastab Eestile esitatud teabetaotlustele ise. Selle käigus kontrollib ühtne kontaktpunkt eelnevalt teisest liikmesriigist saabunud taotluse nõuetekohasust, lubatavust ja sellele vastamise võimalikkust vastavalt KrMS § 508⁹⁰ lõikele 2. Vajadusel kaasab ühtne kontaktpunkt vastuse koostamisse ühe või mitu uurimisasutust. Lisaks ühtsele kontaktpunktile, kes on eelnõukohase KrMS § 508⁸⁵ lõike 3 kohaselt põhiline teabevahetuse teostaja, on teabevahetamise õigus KrMS § 508⁸⁵ lõikes 4 antud ka uurimisasutustele ehk EL-i liikmesriikide kontekstis õiguskaitseasutustele. Paindlikkuse suurendamiseks on nii Rootsi direktiivis kui ka KrMS § 508⁸⁵ lõikes 4 sätestatud, et teabevahetuse reeglite täitmisel võivad uurimisasutused vahetada teavet iseseisvalt, ühtse kontaktpunkti sekkumiseta (nn uurimisasutuse iseseisev teabevahetus). See võimaldab uurimisasutustel vastata kiiremini ja otsekontaktidele, järgides samal ajal kehtivaid protseduurinõudeid.

Kuna eelnõukohase KrMS § 508⁹⁰ lõike 1 kohaselt vastab teise liikmesriigi ühtse kontaktpunkti või õiguskaitseasutuse teabetaotlusele või edastab selle vastamiseks uurimisasutusele Eesti ühtne kontaktpunkt ning eelnõukohase KrMS § 508⁸⁵ lõike 3 kohaselt toimub teabevahetus reeglina ühtse kontaktpunkti kaudu, on otsus selle kohta, kas uurimisasutus tohib vastata teabetaotlusele iseseisvalt või peab ta selle tegema ühtse kontaktpunkti kaudu, Eesti ühtse kontaktpunkti pädevuses.

§ 508⁹¹. Teabeedastusest keeldumine

Teabetaotluse saamisel kontrollib ühtne kontaktpunkt või uurimisasutus selle nõuetekohasust ning puuduste korral teabeedastusest keeldutakse. Kõnesolevas paragrahvis esitatakse loetelu asjaoludest, millal on teabeedastus imperatiivselt keelatud. Tegemist on Rootsi direktiivi artikli 6 lõike 1 punktides a–h toodud põhjustega, mille korral peab teabetaotlusele vastamisest keelduma. Rootsi direktiivi põhjenduse nr 20 kohaselt peaksid EL-i liikmesriigid oma üldise hoolsuskohustuse väljendusena alati kontrollima, kas neile esitatud taotlused vastavad vajalikkuse ja proportsionaalsuse põhimõtetele, ning jätma rahuldamata taotlused, mida nad peavad nende põhimõtetega vastuolus olevaks. Seejuures vajab toonitamist, et kui teabetaotlus on ebaselge või selles esinevad formaalsed puudused, tuleb esmalt pöörduda teabetaotleja poole ja selgitada, millised puudused taotluses esinevad, ning paluda need kõrvaldada. Samuti tuleb

selgitada, et puuduste kõrvaldamata jätmisel keeldutakse KrMS § 508⁹¹ lõike 1 punkti 5 alusel teabeedastusest.

Lõike 1 punkti 1 kohaselt keeldutakse teabeedastusest, kui taotletakse teavet kuriteo kohta, mille eest karistatakse karistusseadustiku (edaspidi *KarS*) kohaselt kuni üheaastase vangistusega. Rootsi direktiivi eesmärk on tõhustada riikideülel raskete süütegude tõkestamist, avastamist ja uurimist. Kergema raskusastmega kuritegevust puudutava teabe vahetus direktiivi kohaldamisalasse ei kuulu. Isikuandmete töötlemine ja sellega kaasnev õiguste riive ei ole põhjendatud kuritegude puhul, mille eest karistatakse Eestis *KarS*-i kohaselt maksimaalselt kuni ühe aasta pikkuse vabadusekaotusega. Sellised kuriteod on näiteks ähvardamine (*KarS* § 120 lõige 1), kehaline väärkohtlemine (*KarS* § 121 lõige 1), lapse ülalpidamiskohustuse rikkumine (*KarS* § 169), alaealise kallutamine alkoholi tarvitamisele (*KarS* § 182 lõige 1) jt. Olukorras, kus teise EL-i liikmesriigi esitatud teabetaotlus on seotud või suunatud kergema raskusastmega kuriteoga seonduva teabe saamisele, tuleb teabe edastamisest keelduda.

Lõike 1 punkti 2 kohaselt keeldutakse teabeedastusest, kui taotletakse teavet teo kohta, mis ei ole *KarS*-i kohaselt kuritegu. Siin peetakse silmas Rootsi direktiivi eesmärki, milleks on riikideülese raske kuritegevuse vastu võitlemine. Väärteod või distsiplinaarrikkumised ei ole Rootsi direktiivi kohaldamisalal. Keeldumisasutus on ette nähtud kaitsemeetmena selle eest, et isikule tekivad negatiivsed tagajärjed tegude eest, mida Eesti õiguse järgi ei peeta kas üldse või mitte nii intensiivselt karistamisväärseks, et neid kriminaliseerida. Kaitsemeetme vajadus on tingitud EL-i liikmesriikide karistusõiguse eripäradest. Hüpotetilise näitena võib tuua, et kui mõnes EL-i liikmesriigis on kuriteona määratletud ja vähemalt üle üheaastase vangistusega karistatav väheväärtusliku asja vargus või abielurikkumine ning see riik esitab teabetaotluse Eestile, tuues põhjenduseks sellise süüteo uurimise, peab Eesti ühtsel kontaktpunktil ja uurimisasutusel olema õigus ja kohustus teabetaotlusele vastamisest keelduda.

Lõike 1 punkti 3 kohaselt keeldutakse teabeedastusest, kui taotletud teave on ebaõige, mittetäielik või aegunud. Isikuandmete töötlemise üks põhimõtteid on, et ebaõiged isikuandmed tuleb viivitamata kustutada või parandada. Eelnimetatud andmete õigsuse põhimõte on sätestatud nii Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/680 artikli 5 lõike 1 punktis d kui ka IKS § 14 punktis 4. Rootsi direktiivi kohase andmetöötluse osas ei ole ette nähtud erandit üldpõhimõttest kõrvale kaldumiseks ehk vahetatavad andmed ei tohi olla aegunud, valed või mittetäielikud. Eeltoodu tähendab, et näiteks olukorras, kus teavet soovitakse isiku kohta, kellele on kunagi esitatud kahtlustus ekslikult, tuleks teabetaotlusele vastamisest keelduda. Samuti tuleks keelduda selliste andmete väljastamisest, mille seos nende kogumise aluseks olnud kuriteoga on ebaselge, sealhulgas jäetud välja selgitamata. Näiteks tuleks keelduda kriminaalmenetluse raames sideettevõtjalt saadud sõnumi edastamise fakti kohta käivate andmete ehk nn kõneeristuse edastamisest, kui kõneeristuse subjekti või kõneeristust läbiva isiku seos menetletud kuriteoga on välja selgitamata, teda ei ole hiljem menetlusele allutatud ehk tegemist ei ole tunnistaja ega kahtlustatavaga. Samuti, kui kahtlustatava kõneeristusest nähtub pelgalt fakt selle kohta, et ta on tuvastamata asjaoludel kindla isiku nimel oleva telefoninumbri kasutajaga suhelnud. Keelduda tuleb ka aegunud andmete edastamisest. Näiteks olukorras, kus uurimisasutus on teinud KrMS § 90¹ lõike 1 järgi sideettevõtjale päringu identifitseerimistunnustega seotud andmete kohta ehk nn numbri omanikupäringu, tuleb enne andmete edastamist veenduda, et number on endiselt selle isiku kasutuses. Kui tuvastatakse, et numbri tegelik kasutaja ei ole enam isik, kes on numbri omanik, või on selliste andmete saamisest möödas piisavalt pikk aeg, et isiku elustiili arvestades on tõenäoline, et ta on enda kasutuses olevat telefoninumbrit selleks ajaks juba vahetanud, tuleks andmete edastamisest keelduda. Kui andmete edastamine on kaasuse asjaolude tõttu siiski vajalik (näiteks minevikus mingil hetkel telefoninumbri, sõiduki vms kasutamine), tuleb

kindlasti täpsustada andmete saamise aeg ja asjaolud ning viidata, et andmed ei pruugi olla tõesed.

Lõike 1 punkti 4 kohaselt keeldutakse teabeedastusest, kui taotletakse teavet, mis on saadud riigilt, kes ei ole andnud selle edastamiseks nõusolekut. Keeldumisasutus tuleneb andmete omandiõiguse põhimõttest. Sellel EL-i liikmesriigil või kolmandal riigil, kellelt teave pärines, on õigus otsustada teabe edastamise lubatavuse ja tingimuste üle. Kui teabe algselt Eestile edastanud riik ei ole andnud nõusolekut teabe jagamiseks teiste EL-i riikidega, ei teki uurimisasutusel ega ühtsel kontaktpunktil direktiivi järgi kohustust riikidevahelisest kahepoolsest kokkuleppesest kõrvale kalduda. Reeglina tuleks teabe algset omanikku teise EL-i liikmesriigi teabetaotluse laekumisest teavitada ja temalt teabe edastamise kohta luba küsida. Kui teabe omanik ei luba teavet edastada, tuleb teabetaotlusele vastamisest keelduda. Teabe kättesaadavaks tegemine ühele EL-i liikmesriigile ei tohi muuta teavet vaikimisi kättesaadavaks kõikidele EL-i liikmesriikidele.

Lõike 1 punkti 5 kohaselt keeldutakse teabeedastusest, kui taotlus ei vasta KrMS §-s 508⁹⁵ sätestatud nõuetele ja teise liikmesriigi ühtne kontaktpunkt või õiguskaitseasutus ei kõrvalda puudusi. Eelnõukohase KrMS §-ga 508⁹⁵ sätestatakse loetelu andmetest, mis tuleb teabetaotluses märkida. Nimetatud loetelu on üle toodud Rootsi direktiivi artikli 4 lõike 5 punktidest a–f ning sisaldab ammendavat, lihtsat ja piisavalt üksikasjalikku loetelu üksikasjadest, mida on taotluse kiireks ja hõlpsaks lahendamiseks vaja. Kui teabetaotlus sisaldab puudusi ehk ei vasta eelnõukohase KrMS §-s 508⁹⁴ sätestatud nõuetele, tuleb esmalt täita KrMS § 508⁹⁰ lõike 3 punktide 1 ja 2 kohast selgituskohustust ehk juhtida tähelepanu puudustele taotluses ja paluda need võimalusel kõrvaldada. Kui teabetaotluse esitaja puudusi ei kõrvalda, tuleb taotlusele vastamisest keelduda ulatuses, mille suhtes esineb keeldumisasutus.

Lõike 1 punkti 6 kohaselt keeldutakse teabeedastusest, kui prokuratuur või kohus on teabevahetusloa andmisest keeldunud. Rootsi direktiivi artikli 6 lõike 1 punktis c ja eelnõukohases KrMS-is on peetud vajalikuks toonitada seaduse tasandil sõnaselgelt, et EL-i õigusest liikmesriigile tulev alus saada teiselt EL-i liikmesriigilt teavet ei prevaleeri riigisisese õiguse ees. Olukorras, kus uurimisasutusel tuleb teabeedastuseks küsida teabevahetusloa ja loa andmisest on keeldutud, tuleb lähtuda Eesti õigusasutuse otsusest ning taotlusele vastamisest keelduda. Et välistada selliste teabetaotluste mitmekordne esitamine, on direktiivis ja eelnõus ette nähtud, et tuginedes õigusasutuse otsusele ja keeldumisasutusele, uutele samasisulistele taotlustele ei vastata. Olukorrad, kus prokuratuur või kohus keeldub teabevahetusloa andmisest selle tõttu, et teise EL-i liikmesriigi teabetaotluses esinevad puudused, on välditavad teabevahetuses osalevate liikmesriikide koostöö ja Eesti uurimisasutuse ning ühtse kontaktpunkti poolt selgituskohustuse täitmisega.

Lõike 1 punkti 7 kohaselt keeldutakse teabeedastusest, kui see kahjustaks põhjendamatult juriidilise isiku seadusega kaitstud olulisi huve. PS § 9 lõike 2 kohaselt laienevad PS-is loetletud õigused, vabadused ja kohustused juriidilistele isikutele niivõrd, kui see on kooskõlas juriidiliste isikute üldiste eesmärkide ja selliste õiguste, vabaduste ja kohustuste olemusega. Kuna juriidiline isik kui abstraktsioon saab tegutseda vaid füüsilise isiku kaudu, ei saa juriidilise isiku enda turvalisus sattuda ohtu. Küll aga võivad vajada kaitset juriidilise isiku olulised huvid. Selliseks oluliseks huviks võib olla näiteks ärisaladus ehk eelkõige kaubanduslikku või tehnilist laadi teave, mis ei ole avalikult kättesaadav ja mida ettevõtja hoiab salajas, sest selle teabe teistele isikutele õigustamata teatavaks saamine kahjustab ettevõtja ärihuve.⁷¹ Keeld sellist teavet avaldada sisaldub ka KrMS § 214 lõikes 2, milles sätestatakse, et prokuratuur ei või lubada kohtueelse menetluse andmete avaldamist kriminaalmenetluse, avalikkuse või

⁷¹ [Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus](#), § 5 lõige 2.

andmesubjekti huvides, kui see seab ülemäära ohtu ärisaladuse või kahjustab ülemäära juriidilise isiku tegevust. Kui käimasoleva kohtueelse menetluse andmete avaldamiseks on tarvilik teabevahetusluba, mida KrMS § 214 lõike 1 kohaselt saab anda prokuratuur, siis teabe puhul, mis on saadud alustamata jäetud, lõpetatud või kohtusse saadetud kriminaalasjade raames, tuleb vastav kaalutusotsus võtta vastu uurimisasutusel või ühtsel kontaktpunktil. Seetõttu on mõistlik selgitada, et näiteks tuleks tõenäoliselt keelduda teabetaotluse raames väljastamast teavet legaalse toodete retseptide, keemiliste koostisosade ja tootmissaladuste kohta, mis on saanud kriminaalmenetluse käigus uurimisasutusele teatavaks (nt mõne narkootilise aine valmistamist puudutava uurimise raames). Eelnimetatud näite puhul tuleks keelduda teabe kogumis väljastamisest juriidilise isiku oluliste huvide kaitsel tuginedes, ent mõne konkreetse elemendi käitlemise fakti avaldamine oleks tõenäoliselt lubatav ja võimalik, sest eelnõukohase KrMS § 508⁹¹ lõike 2 järgi võib teabetaotlusele vastamisest keelduda üksnes ulatuses, mille suhtes ilmneb vähemalt üks KrMS § 508⁹¹ lõikes 1 sätestatud keeldumise alustest.

Lõike 1 punkti 8 kohaselt keeldutakse teabeedastusest, kui see võib ohustada riigi julgeolekut. Rootsi direktiivi põhjenduspunkti nr 13 järgi ei kohaldata direktiivi sellise teabe töötlemisele, mis jääb EL-i õiguse kohaldamisalast väljapoole, ehk teabele, mis puudutab riiklikku julgeolekut. Nimetatud keeldumisalust kohaldatakse näiteks terrorikuritegu puudutavale teabele, mis ei hõlma hädaolukorra lahendamist. Eeltoodu ei tähenda kategoorilist keeldu vastavat teavet teiste EL-i liikmesriikidega vahetada, ent seda tuleb teha asjakohaste kanalite kaudu, mida Rootsi direktiiviga ei reguleerita.

Lõike 1 punkti 9 kohaselt keeldutakse teabeedastusest, kui see on ebaproportsionaalne võrreldes taotletava eesmärgiga. Kuna isikuandmete töötlemisega kaasneb alati õiguste riive, peab töötlemine olema mitte ainult vajalik, vaid ka seatud eesmärgi suhtes proportsionaalne. Seaduse ja töökorraldusega tuleb tagada, et selline riive eraelu puutumatusele on võimalikult vähene. Näitena võib tuua olukorra, kus teabetaotlus esitatakse Eestile selleks, et tuvastada röövi toimepanijad, kes on kuriteo toimepanemise järel põgenenud teabetaotluse esitanud EL-i liikmesriiki, kasutades registreerimismärkideta sõidukit. Teabetaotluse esitamine täidab kuriteo menetlemise ja potentsiaalselt ka edasiste kuritegude tõkestamise eesmärgi. Teave on toimepanijate tuvastamiseks ja nende vastutusele võtmiseks vajalik, eriti kui muid teo toimepanijaid välja selgitada võimaldavaid andmeid napib. Ehkki teabetaotlusele vastamine on lubatav ka kuriteo raskusastmest tulenevalt ning teave on eelduslikult Eestil olemas, ei pruugi olla taotlusele vastamiseks proportsionaalne teha kõikide Eesti registris olevate ja olnud vastava värvi, margi, mudeli ja keretüübiga sõidukite ning nende omanike ja kasutajate kohta päring andmebaasides ning edastada need andmed taotlevale liikmesriigile. Eelkirjeldatud tegevusega riivatakse tõenäoliselt põhjendamatult paljude asjassepuutumatute isikute eraelu nii päringu tegemisel kui ka nende andmete edastamisel teisele EL-i liikmesriigile.

Lõike 1 punkti 10 kohaselt keeldutakse teabeedastusest, kui teabevahetus seaks ohtu isiku turvalisuse. Inimeste õiguste austamine on üks EL-i põhikohustusi ning kohustus tagada isiku õigus elule, kehalisele puutumatusele ja füüsilisele vabadusele kaalub üle kriminaalmenetluse huvid. Eeltoodust tulenevalt peab teabetaotlusele vastaja alati hindama teabevahetusega kaasnevat ohtu isiku põhiõigustele ja nende realiseerumise tõenäosust. Pidades piisavalt tõenäoliseks, et teabevahetuse tõttu satub ohtu isiku turvalisus, tuleb taotlusele vastamisest keelduda. Eeltoodu omab erilist tähendust teabe osas, mis on saadud salajase koostöö abil või mis pärineb anonüümselt tunnistajalt. Tuleb silmas pida, et sellise allika paljastumise oht ja sellest tulenev oht tema turvalisusele ei seisne ilmtingimata tema isikuandmete sõnaselges avaldamises. Isiku turvalisus võib sattuda ohtu ka olukorras, kus teabe sisust tulenevalt on võimalik välja selgitada, kellelt, sealhulgas millisest isikute ringist, teave pärineb. Eeltoodu aga ei tähenda, et nimetatud keeldumisalust saaks kasutada kergekäeliselt, üksnes abstraktsele

ohule tuginedes. Oht, et kellegi vastu ütluste andmisega kaasnevad negatiivsed, ütluste andja turvalisust ohustavad tagajärjed, on olemas alati. Oluline on sellise ohu realiseerumise tõenäosus. Keeldumisalusele tuginedes on mõistlik lähtuda KrMS § 67 lõikes 1 sätestatud põhimõttest, mille kohaselt turvalisuse kaalutlusel anonüümsuse tagamine kriminaalmenetluse raames peab olema tingitud eeskätt kuriteo raskusest või erandlikest asjaoludest. Seetõttu tuleb iga kord kaaluda teabevahetusega kaasnevaid riske ja nende realiseerumist, lähtudes objektiivsetest asjaoludest, aga ka osapoolte põhjendatud huvist. Seejuures tuleb tagada valmidus kaalutlusotsust sisuliselt põhjendada, ka tagantjärele.

Lõike 1 punkti 11 kohaselt keeldutakse teabeedastusest, kui see võiks märkimisväärselt kahjustada käimasolevat kriminaalmenetlust. See keeldumisalus on ette nähtud juhuks, kui Eestis on pooleli kriminaalmenetlus ja teabevahetusele vastamine võiks seada ohtu selle kriminaalasja lahendamise. Keeldumise korral tuleb silmas pidada, et seda ei tohi teha kergekäeliselt, üksnes blanketsele normile ja abstraktsele ohule tuginedes.

Saades teiselt EL-i liikmesriigilt teabetaotluse, mis võib negatiivselt mõjutada menetluses oleva kriminaalasja lahendamist, tuleb iga kord kaalutleda riske ja osapoolte põhjendatud huve ning teha nendest lähtuvalt otsus teabevahetuse lubatavuse kohta. Seejuures tuleb tagada valmidus otsust, sealhulgas selle kujunemist, hiljem näiteks Euroopa Komisjonile põhjendada (taotluse esitanud EL-i liikmesriigi ees sellist kohustust täita ei tule). Seda, kas teabetaotlusele saab või ei saa vastata, otsustab õigusasutus. Kohustus selliste teabetaotluste saamisest prokuratuuri või kohut teavitada lasub ühtsel kontaktpunktil ja uurimisasutusel, olenevalt nendevahelisest kokkuleppest või sellest, kumb teabetaotlusele vastamisega tegeleb. Teabevahetusloa taotlemine on vajalik näiteks siis, kui teabetaotlusele vastamine eeldab käimasoleva kohtueelse menetluse andmete avaldamist. Vastavalt KrMS § 214 lõikele 1 võib selliseid andmeid avaldada üksnes prokuratuuri loal ja määratud ulatuses. Kohtult tuleb teabevahetusloa taotleda eeskätt siis, kui teabetaotlusele vastamine eeldab KrMS § 12 alusel perekonna- ja eraelu kaitseks või alaealise või kannatanu huvides täielikult või osaliselt kinniseks kuulutatud kohtuistungil või selle kinniseks kuulutatud osas avaldatud andmete avaldamist.

Lõike 1 punkti 12 kohaselt keeldutakse teabeedastusest, kui ühtsel kontaktpunktil ja uurimisasutusel ei ole taotletud teabele juurdepääsu. Silmas on peetud olukorda, kus uurimisasutusel ei ole otse juurdepääsetavat ega kaudselt juurdepääsetavat teavet. See tähendab, et lisaks sellele, et teavet ei ole uurimisasutusele kättesaadavas andmebaasis, puudub võimalus teabe pärimiseks mujalt. Näiteks ei ole taotletavat teavet Eestis üldse või selle kättesaamisel esinevad takistused, mida ei saa kõrvaldada. Näitena võib tuua olukorra, kus isik, kellel on teist EL-i liikmesriigi õiguskaitseasutust huvitav teave, ei ole nõus seda vabatahtlikult teatavaks tegema ja uurimisasutusel puudub alus tema kohustamiseks. Sellise olukorraga on tegemist näiteks siis, kui uurimisasutus soovib saada teisele riigile huvipakkuvat isiku kohta teavet vestluses võimaliku tunnistajaga, kes uurimisasutusega koostööd teha ei soovi. Samuti siis, kui uurimisasutus soovib saada pangalt isiku pangaandmeid, ent pank, tuginedes pangasaladuse kaitsele, nende avaldamisest keeldub. Sellistel juhtudel võib esitada taotluse andmete saamiseks KrMS §-s 489³⁷ nimetatud EIO abil.

Lõikega 2 nähakse ette, et kui käesoleva paragrahvi lõikes 1 sätestatud keeldumise alus kehtib üksnes teabetaotluse osa kohta, keeldutakse üksnes selles osas taotletud teabe edastamisest. Kui taotluse rahuldamata jätmise põhjused on seotud ainult osaga taotletud teabest, tuleb ülejäänud teave esitada KrMS § 508⁹² lõikes 1 või 2 sätestatud tähtaja jooksul. Sätte eesmärk on toonitada, et ühe või mitme teabe edastamisest keeldumise aluse esinemine ei tähenda, et kogu teabetaotlusele ei saa vastata. Iga teabetaotluse puhul tuleb sellele vastamise lubatavuse kontrollimisel hinnata, kas, ja kui, siis millise teabe edastamine on keelatud ning millist teavet tuleb teabe taotlejale siiski edastada.

Lõike 3 kohaselt tuleb teabeedastusest keeldumise korral teavitada viivitamata teise EL-i liikmesriigi ühtset kontaktpunkti või õiguskaitseasutust. Teavituses tuleb selgelt välja tuua keeldumise alus ja viidata vastavale KrMS § 508⁹¹ lõike 1 punktile. Teavitus tuleb edastada KrMS § 508⁹² lõikes 1 või 2 sätestatud tähtaegade jooksul. Keeldumisalused on imperatiivsed ning nende esinemisel ei tohi teabetaotlusele vastata osas, mille suhtes keeldumisalus esineb. Sellisel juhul tuleb taotluse esitajale selgelt ja põhjendatult teatada, et teavet ei edastata, ning põhjendada keeldumist viitega vastavale sättele. Kui teabetaotluse on esitanud uurimisasutus, tuleb edastada vastamisest keeldumise teate koopia ka teabetaotluse esitanud EL-i liikmesriigi ühtsele kontaktpunktile. Sätte eesmärk on õigusselguse huvides toonitada, et ka teabetaotlusele sisulisest vastamisest keeldumise korral tuleb taotluse esitanud teise EL-i liikmesriigi ühtset kontaktpunkti või õiguskaitseasutust keeldumisest teavitada. See tagab, et ka kontaktpunkt on teadlik keeldumisest ja saab vajadusel korraldada täiendava suhtluse.

Sätte eesmärk on rõhutada õigusselguse tagamiseks, et ka teabetaotlusele sisulisest vastamisest keeldumise korral tuleb taotluse esitajat keeldumisest teavitada. Lihtsalt vaikimisi reageerimata jätmine keeldumisaluse esinemisel ei ole lubatav.

§ 508⁹². Teabetaotlusele vastamise tähtaeg

Rootsi direktiivi eesmärk on tagada kiire reageerimine kuritegevusele võimalikult paljudel juhtudel. Põhjenduse nr 18 kohaselt tuleb selleks kehtestada selged ja proportsionaalsed tähtajad, arvestades taotluse kiireloomulisust ning seda, kas tegemist on otse või kaudselt juurdepääsetava teabega.

Teabetaotlusele vastamise tähtajad on sätestatud Rootsi direktiivi artikli 5 lõikes 1. Artikli 5 lõike 1 punktides a ja b on esitatud kiireloomuliste taotluste tähtajad ning punktis c tähtaja üldreegel. Kõnesolevas sättes nähakse samad tähtajad ette KrMS-is. Nendest tähtaegadest hoolimata tuleb teabetaotlusele vastamisel juhendada aga direktiivi ja seega ka KrMS-i vastavate sätete eesmärgist ning edastada taotletud teave niipea, kui see on ühtse kontaktpunkti valduses, isegi kui see teave ei ole ainus kättesaadav teave, mis on taotluse seisukohast asjakohane. Ülejäänud teave tuleks esitada niipea, kui ühtne kontaktpunkt selle saab.

Põhjendatud juhtudel võib direktiivi alusel tähtaegadest erandkorras kõrvale kalduda, näiteks kui taotluse saanud liikmesriigi pädev õigusasutus vajab lisaaga loa andmiseks või puuduste kõrvaldamiseks. See võib olla tingitud taotluse ulatusest või keerukusest.

Lõikega 1 nähakse ette, et teabetaotlusele vastatakse viivitamata, kuid hiljemalt seitsme päeva jooksul taotluse ühtsele kontaktpunktile saabumisest. See tähtaeg on seni kehtinud 14-päevasest tähtajast poole lühem. Arvestades, et SIENA kaudu edastatavate teabetaotluste ja vahetatud operatiivsõnumite arv on viimastel aastatel stabiilselt kasvutrendis ning et Rootsi direktiivi vastuvõtmise järel lisandub kasutajaid veelgi, suureneb ühtse kontaktpunkti töökoormus. Eeltoodu tingib tõenäoliselt vajaduse suurendada ühtse kontaktpunkti isikkoosseisu selleks, et täita teabevahetuse kohustust õigel ajal.

Lõikega 2 sätestatakse, et kui tegemist on kiireloomulise teabetaotlusega, vastatakse taotlusele ühtsele kontaktpunktile saabumisest arvates:

- 1) kaheksa tunni jooksul, kui tegemist on otse juurdepääsetava teabega;
- 2) kolme päeva jooksul, kui tegemist on kaudselt juurdepääsetava teabega.

Kui tegemist on otse juurdepääsetava teabega, siis ei erine teabetaotlusele vastamise tähtaeg kehtiva KrMS § 508⁸² lõikes 1 sätestatud tähtajast. Kaudselt juurdepääsetava teabe puhul sätestatakse eraldi tähtaeg, mida KrMS varem ette ei näinud. Arvestada tuleb, et sellise teabe saamine sõltub kolmandatest osapooltest ega allu uurimisasutuse kontrollile. Siiski tuleb teha kõik võimalik, et täita taotlus ettenähtud tähtajaks.

Lõike 3 kohaselt on teabetaotlus kiireloomuline, kui selle esitanud teine EL-i liikmesriik on selle nii määratlenud ja põhjendanud seda järgmiselt:

- 1) teave on hädavajalik, et selgitada välja või tõrjuda korrakaitseaduse § 5 tähenduses vahetu oluline või kõrgendatud oht Eestis või teises EL-i liikmesriigis avalikule korrale;
- 2) teave on vajalik, et võtta teises EL-i liikmesriigis vastu otsus kohaldada meedet, millega piiratakse isiku vabadust;
- 3) teave kaotab ajakohasuse, kui seda kiiresti ei edastata, ning kui seda teavet peetakse oluliseks süütegude tõkestamisel, avastamisel ja ennetamisel.

Eelnõukohase KrMS § 508⁹² lõike 3 punkti 1 sisustamisel lähtutakse [korrakaitseaduse](#) §-dest 4 ja 5. Ohu väljaselgitamine on tõendite ja muude andmete kogumine selleks, et anda objektiivne hinnang ohu esinemise võimaluse kohta ohukahtluse korral. KorS § 5 lõikega 6 määratletakse ohukahtlus kui olukord, kus ilmnenu asjaoludele antava objektiivse hinnangu põhjal ei saa tõenäosust, et korrarikkumine aset leiab, pidada piisavaks, kuid mille puhul on alust arvata, et korrarikkumine ei ole välistatud. Ohu tõrjumine aga on väljaselgitatud konkreetse ohu suhtes meetmete rakendamine, et vältida või vähendada kahjulikku tagajärge.

Eeltoodust tulenevalt on teabetaotlus kiireloomuline, kui sellega soovitakse oht välja selgitada või tõrjuda juba aset leidvat või suure tõenäosusega peagi aset leidvat ohtu isiku elule, tervisele, kehalisele puutumatusele, füüsilisele vabadusele, olulise või suure väärtusega varalisele hüvele või keskkonnale, samuti kuriteo toimepanemise ohtu, eeskätt KarS 15. peatükis sätestatud I astme kuriteo või 22. peatükis sätestatud kuriteo toimepanemise ohtu.⁷²

Eelnõukohase KrMS § 508⁹² lõike 3 punktis 2 nimetatud juhuga on tegemist näiteks siis, kui teisest EL-i liikmesriigist saadud teabe alusel tehakse otsus isiku vabaduste piiramise suhtes. See ei tähenda ilmingimata liikumisvabaduse piiramist (nt kinnipidamine ja vahistamine), vaid võib seisneda ka näiteks isiku suhtes jälitustoimingu tegemises, tema menetlusetoimingule allutamises (nt läbiotsimine) või tema suhtes riikliku järelevalve erimeetme kohaldamises korrakaitseaduse alusel. Viimased näited on asjakohased ka eelnõukohase KrMS § 508⁹² lõike 3 punktis 3 sätestatud juhul, ehkki nimetatud sätte eesmärk on avastada kuriteo toimepanemist (sh katsestaadiumis) või tabada kurjategija selle toimepanemisel.

Lõikega 4 nähakse ette, et käesoleva paragrahvi lõikes 1 või 2 sätestatud tähtaja kulgemine peatub ajaks, millal:

- 1) teise liikmesriigi ühtne kontaktpunkt või õiguskaitseasutus kõrvaldab oma teabetaotluse puudused, mille kõrvaldamata jätmise korral keeldutaks KrMS § 508⁹¹ lõike 1 punkti 5 alusel teabeedastusest;
- 2) teise liikmesriigi ühtne kontaktpunkt või õiguskaitseasutus annab oma teabetaotluse kohta selgitusi või täpsustusi;
- 3) prokuratuur või kohus lahendab teabevahetusloa taotlust.

⁷² Selgitus: ohu ennetamine ehk abstraktsete ohutusnõuete järgimise tagamine selleks, et hoida ära konkreetse ohu tekkimist (s.o enne ohukahtluse ilmnemist), teabetaotluse kiireloomulisust ei tingi.

Selline regulatsioon on oluline, et tagada teabetaotluste kvaliteetne ja õiguspärane menetlemine ning välistada alusetu keeldumine üksnes vormiliste puuduste tõttu. Peatumise alused on järgmised:

1. **Teabetaotluse puuduste kõrvaldamine** – tähtaja kulgemine peatub, kui teise liikmesriigi ühtsele kontaktpunktile või õiguskaitseasutusele on antud võimalus kõrvaldada teabetaotluses esinevad puudused. See on oluline, kuna KrMS § 508⁹¹ lõike 1 punkti 5 alusel on võimalik teabeedastusest keelduda, kui taotlus on puudulik ega vasta nõuetele. Et vältida liigseid keeldumisi ja anda koostööpartnerile võimalus taotlust parandada, peatatakse tähtaja kulgemine, kuni puudused on kõrvaldatud või tähtaja jooksul seda ei tehta.
2. **Teabevahetusloa hankimine** – mõnel juhul on teabe edastamine võimalik ainult prokuratuuri või kohtu loal. Näiteks juhul, kui teabetaotlus puudutab käimasoleva kriminaalmenetluse andmeid. Seejuures tuleb silmas pidada, et teabevahetusloa või sellest keeldumine tuleb saada reeglina KrMS-is sätestatud teabetaotlusele vastamise tähtaegade jooksul. Tähtajast võib kõrvale kalduda vaid juhul, kui taotluses tõstatatud küsimused on väga mahukad või keerukad. Teabevahetusloa taotlemiseks ja saamiseks võib kuluda aega. Tähtaja peatumine tagab, et menetleval asutusel on õiguslikult piisav aeg vajaliku loa saamiseks, ilma et seaduses sätestatud tähtaeg lõppeks ja tekiks oht, et vastamata jätmine muutub õigusvastaseks.
3. **Selgituste või täpsustuste saamine** – kui teabe saamiseks on vaja täiendavaid selgitusi või täpsustusi teise EL-i liikmesriigi kontaktpunktilt või õiguskaitseasutuselt, peatub tähtaeg seni, kuni vastused on saadud või mõistliku aja jooksul andmata jäetud. See aitab tagada, et teabetaotlus vaadatakse läbi sisuliselt ja õiguspäraselt, mitte ei jäeta rahuldamata formaalsetel või vältimatult täpsustamist vajavatel põhjustel.

Tähtaja peatumise võimalus teenib õiguskindluse ja koostöö tõhususe eesmärki, aidates vältida põhjendamatuid keeldumisi ning andes osapooltele vajaliku aja puuduste kõrvaldamiseks või otsuste tegemiseks, ilma et see kahjustaks määratud tähtaegu ega tooks kaasa õiguslikke tagajärgi.

Lõikega 5 nähakse ette, et kui käesoleva paragrahvi lõikes 1 või 2 sätestatud tähtajast kaldutakse kõrvale, teavitatakse teise liikmesriigi ühtset kontaktpunkti või õiguskaitseasutust viivituse eeldatavast kestusest ja põhjusest. Sätte eesmärk on täita teavitamis- ja selgitamiskohustust selleks, et taotluse esitanud EL-i liikmesriik saaks kinnituse, et tema taotlusega tegeletakse, ning oskaks prognoosida teabe eeldatava laekumise pinnalt toiminguid riigisiselt.

§ 508⁹³. Teabetaotluse vastuse koopia edastamine

Lõikega 1 sätestatakse, et kui teabetaotluse vastus edastatakse teise EL-i liikmesriigi õiguskaitseasutusele, tuleb selle vastuse koopia edastada samal ajal ka selle liikmesriigi ühtsele kontaktpunktile. Sellise nõude eesmärk on tagada, et igas EL-i liikmesriigis oleks olemas keskne asutus – ühtne kontaktpunkt –, kes omab ülevaadet kogu kriminaalmenetlusalasest rahvusvahelisest teabevahetusest, suudab seda koordineerida ning koguda selle kohta statistikat. See tagab KrMS-i vastavuse Rootsi direktiivi artikli 5 lõikele 3.

Lõikega 2 reguleeritakse aga olukordi, kus teabetaotlusele vastab uurimisasutus – omal algatusel või seetõttu, et Eesti ühtne kontaktpunkt on vastamise suunanud konkreetsele uurimisasutusele. Sellisel juhul peab uurimisasutus teabetaotluse vastuse edastama samal ajal kahele adressaadile: Eesti ühtsele kontaktpunktile ja selle liikmesriigi ühtsele kontaktpunktile, kelle õiguskaitseasutusele teave saadetakse. Sätte eesmärk on tagada, et mõlema riigi ühtsed kontaktpunktid oleksid teadlikud teabe vahetamisest ja vahetatud teabe sisust. Seejuures tuleb

märkida, et kui uurimisasutus edastab teavet SIENA kaudu, ei ole vaja Eesti kontaktpunktile eraldi koopiat saata, kuna kontaktpunkt saab kõigist selle süsteemi kaudu toimunud teabevahetustest automaatselt ülevaate. Küll aga peab uurimisasutus ka SIENA kaudu teavet vahetades tagama, et teise liikmesriigi ühtne kontaktpunkt oleks teabevahetusest teadlik, märkides selle teise EL-i liikmesriigi ühtse kontaktpunkti teabe adressaadiks.

Lõikega 3 sätestatakse erandid, mille kohaselt ei edastata teabevahetuse koopiat Eesti või teise liikmesriigi ühtsele kontaktpunktile. Seda ei tehta siis, kui:

1. see seaks ohtu isiku turvalisuse;
2. see võiks oluliselt kahjustada käimasolevat kriminaalmenetlust;
3. teave puudutab terrorikuritegu, mille käsitlemine ei hõlma hädaolukorra lahendamist.

Säte põhineb Rootsi direktiivi artikli 5 lõikel 3, mille eesmärk on kaitsta tundlikku teavet ning võimaldada loobuda koopia edastamisest juhul, kui on põhjendatud oht andmelekkeks või teabe väärkasutuseks. Näiteks võib uurimisasutusel olla teavet selle kohta, et Eesti või teise riigi kontaktpunkti töötaja võib seada ohtu üksikisiku turvalisuse või käimasoleva kriminaalmenetluse huvid. Ühtse kontaktpunkti teavitamisest keeldumise alus sisaldub ka Rootsi direktiivi artikli 4 lõikes 2, artikli 5 lõikes 3, artikli 7 lõikes 4 ja artikli 8 lõikes 3 ehk kõigi direktiivikohaste teabeedastuse võimaluste puhul. Need alused seavad prioriteediks menetluse edukuse ja üksikisiku turvalisuse, eelistades neid statistika kogumisele.

Lõike 3 punktis 1 nimetatud alus on mõeldud olukordadeks, kus teabe jagamine võiks kaasa tuua vahetu või tõsise riski kellegi elule, tervisele või vabadusele. Selline risk võib tekkida näiteks salajasele koostööle kaasatud isikute tunnistajate, kannatanute või kahtlustatavate puhul, kelle isikuandmed on äärmiselt tundlikud. *Näide:* uurimisasutus on saanud välisriigi õiguskaitseasutuselt teavet varjatud jälitustoimingu käigus tuvastatud isiku kohta, kes on andnud infot kuritegeliku ühenduse tegevuse kohta. Kui see teave jõuaks teise riigi ühtse kontaktpunkti kaudu töötajani, kelle usaldusväärsus on kahtluse all, võib allika ning ta lähedaste elu ja tervis sattuda ohtu (nt paljastumine, ähvardused, vägivallaaktid). Sellisel juhul jäetakse koopia edastamata ja teavet vahetatakse ainult nende kanalite kaudu, mis tagavad allika kaitse.

Lõike 3 punkti 2 puhul on tegemist olukorraga, kus teabe edastamine võiks takistada tõendite kogumist – tuua kaasa tõendite mõjutamise või hävitamise või muul viisil uurimise eesmärgi nurjumise. *Näide:* uurimisasutus uurib rahvusvahelist narkokaubanduse võrgustikku ning on saanud jälitustegevuse (nt inimallikalt laekunud teave) kaudu teavet, mis aitab jälitustoimingut (nt saadetise varjatud jälgimine ja läbivaatus) kasutada. Kui see teave jõuaks enneaegselt teise riigi kontaktpunkti ja sealt kolmandate isikuteni, muudavad kuriteo toimepanijad oma plaane, hävitavad tõendid või põgenevad. Sellisel juhul võib koopia edastamisega viivitada kuni menetlustoimingute lõpuni.

Lõike 3 punkti 3 kohaselt ei edastata teabe koopiat ka juhul, kui see puudutab terrorikuritegu, mille käsitlemine ei ole seotud hädaolukorra lahendamisega. Nimetatud keeldumisaluse eesmärk on tagada, et terrorismialane teave liigub ainult selleks ette nähtud kanalites, kus on tagatud vajalik turvalisuse ja konfidentsiaalsuse tase. Rootsi direktiivi põhjenduspunktiga 13 täpsustatakse, et direktiivi ei kohaldata teabe töötlemisele, mis jääb EL-i õiguse kohaldamisalast väljapoole – sealhulgas teabele, mis puudutab riiklikku julgeolekut. Kuna EL ega ÜRO ei ole terrorismi üheselt määratlenud, lähtutakse Eestis KarS § 237 lõikes 1 sätestatud terrorismi mõistest. Selle järgi on terrorismikuriteo eesmärk sundida riiki või rahvusvahelist organisatsiooni midagi tegema või tegemata jätma, häirida ühiskonnakorraldust või hirmutada elanikkonda. Eestis vastutab terrorismikuritegude menetlemise ja terrorismialase teabevahetuse eest KAPO, olles väliskontakt ja teabevahetaja teiste sarnaste asutustega välismaal. KAPO kogub ja töötleb terrorismi puudutavat teavet ning edastab seda vastavalt julgeolekualastele

põhimõtetele. Seetõttu ei tohi terrorismialane teave levida kanalites, kus on suurenenud risk andmelekkete või väärkasutuse tekkeks. Erandiks on aga olukorrad, kus terrorismikuriteoga seotud teave puudutab hädaolukorra lahendamist. Sel juhul tuleb teave edastada SIENA kaudu ning sellest peab teavitama ka kontaktpunkte, sest hädaolukorra lahendamine eeldab reageerimist või vähemalt reageerimisvalmidust kõikide uurimisasutuste poolt. Kui teave puudutab häda- või kriisiolukorda, on oluline, et kõik liikmesriigid töötaksid samal ajal ning kooskõlastatult, et lahendada olukord kiiresti ja efektiivselt. SIENA kaudu teabe edastamine aitab tagada, et kõik õiguskaitseasutused saavad teavet ühesugusel ja ühtlustatud viisil, mis on hädaolukorras eluliselt oluline.

3. alljaotis **Teabetaotluse esitamine**

§ 508⁹⁴. Teabetaotluse esitamine

Lõikega 1 nähakse ette, et kui Eesti uurimisasutusel on põhjendatud alus arvata, et teise EL-i liikmesriigi õiguskaitseasutusel on teavet, mis võib aidata avastada, tõkestada või menetleda kuritegu, võib ta:

- 1) esitada teabetaotluse ühtsele kontaktpunktile või
- 2) esitada teabetaotluse oma pädevuse piires iseseisvalt teise liikmesriigi ühtsele kontaktpunktile või õiguskaitseasutusele.

Tegemist on üldsättega, millega reguleeritakse teisele EL-i liikmesriigile teabetaotluse esitamist. Nähakse ette, et teabetaotluse esitamiseks peab olema mingi objektiivne asjaolu (nt olemasolev teave), millest tulenevalt võib eeldada, et sellel teisel liikmesriigil on vajalikku teavet. Eeskätt saab sellise teabe olemasolu nähtuda Prümi otsuse ja Prüm II määruse raames toimuvast automaatsest andmevahetusest, mille raames liikmesriigid vahetavad DNA-profiile, daktüloskoopilisi andmeid, sõidukite teatavaid registreerimisandmeid, näokujutisi ning politseiregistrite andmeid. Näiteks, leides ühes EL-i liikmesriigis kuriteopaigalt sõrmejäljekujutise ja võrreldes seda Prümi andmevahetuse raames teiste EL-i liikmesriikide riiklikes andmebaasides olevate sõrmejäljeandmetega ning saades positiivse vaste (kokkulangevuse), saab SIENA kaudu esitada teabetaotluse, et küsida selle sõrmejäljekujutise kohta käivad isikustatud andmed. Samuti saab eelkirjeldatud juhul küsida biograafilisi andmeid ehk isiku tausta puudutavaid andmeid, milleks on teave selle kohta, kas ja mis kuritegudega on seda isikut varem seostatud.

Lisaks Prümi andmevahetusele võib isiku seos mingi EL-i liikmesriigiga nähtuda muudest asjaoludest. Näiteks võib olla põhjendatud teiselt EL-i liikmesriigilt isiku kohta teabe küsimine juhul, kui kuriteoga seostataval isikul on selle riigi kodakondsus. Samuti võib olla põhjendatud teabe taotlemine, kui kuriteo sündmusaigal on nähtud selle liikmesriigi registris olevat sõidukit. Viimati nimetatud juhul võib olla põhjendatud teiselt EL-i liikmesriigilt teabe küsimine selle kohta, kas neil on selle sõiduki omaniku ja kasutajate kohta kriminaalteavet, ning kui on, siis millist (nt kas isik on teises liikmesriigis õiguskaitseasutustega kokku puutunud ja kui on, siis millistel asjaoludel). Vastava aluse sätestamise eesmärk on vältida isikuandmete põhjendamatu töötlemist ning vähendada andmeturbe riske ja töökoormust, mis tekivad sihistamata teabetaotluste tegemisega teistesse EL-i liikmesriikidesse ehk nn andmete kalastamisega.⁷³

⁷³ Selgitus: Europoli andmetel moodustavad 80% SIENA teabetaotlustest küsimused, kas EL-i liikmesriigil on isiku X kohta teavet või mitte. Sellised teabetaotlused esitatakse paljudel juhtudel kõikidele EL-i liikmesriikidele, st sihistamatult.

Lõike 2 kohaselt kontrollib ühtne kontaktpunkt uurimisasutuse edastatud teabetaotluse vastavust KrMS §-s 508⁹⁵ sätestatud nõuetele, kõrvaldab vajadusel puudused ning edastab selle teise EL-i liikmesriigi ühtsele kontaktpunktile või õiguskaitseasutusele.

Lõikega 3 nähakse ette, et teabetaotluse koopia esitamisele kohaldatakse KrMS § 508⁹³. See tähendab, et kui ühtne kontaktpunkt esitab teabetaotluse otse teise EL-i liikmesriigi õiguskaitseasutusele, edastab ta samal ajal taotluse koopia teise EL-i liikmesriigi ühtsele kontaktpunktile, välja arvatud KrMS § 508⁹³ lõikes 3 sätestatud juhul ehk siis, kui:

- 1) see seaks ohtu isiku turvalisuse;
- 2) see võiks märkimisväärselt kahjustada käimasolevat kriminaalmenetlust või
- 3) teavet vahetatakse terrorikuriteo kohta, mis ei hõlma hädaolukorra lahendamist.

Teabetaotluse koopia edastamine ühtsele kontaktpunktile on vajalik selleks, et tal oleks kõikehõlmav vaade riigisisest direktiivkohasest teabevahetusest ja võimalused sellise teabevahetuse korraldamiseks.

Kui uurimisasutus esitab teabetaotluse teise liikmesriigi ühtsele kontaktpunktile, peab ta teabetaotluse koopia edastama ka Eesti ühtsele kontaktpunktile. Samuti, kui uurimisasutus esitab teabetaotluse otse teise liikmesriigi õiguskaitseasutusele, peab ta taotluse koopia edastama nii Eesti kui ka teise EL-i liikmesriigi ühtsele kontaktpunktile. See võimaldab mõlemal ühtsel kontaktpunktil olla teadlik neile esitatud teabetaotlustest, omada ülevaadet nende vastamisest ja teostada kontrolli selle üle, kas teabevahetus on nõuetekohane. Samuti aitab see tagada tähtaegadest kinnipidamist ja statistika kogumist. Kuna Eesti ühtne kontaktpunkt näeb kogu Eesti teabevahetust SIENA-s, ei ole teabetaotluse esitamisel vaja SIENA kaudu ühtset kontaktpunkti eraldi koopias hoida. Kui teavet vahetatakse SIENA-s, loetakse, et ühtne kontaktpunkt on teabetaotluse koopiasse lisatud. See ei vabasta aga uurimisasutust kohustusest saata koopiat teise EL-i liikmesriigi ühtsele kontaktpunktile.

§ 508⁹⁵. Nõuded teabetaotlusele

Kõnesolevas sättes esitatakse loetelu andmetest, mis tuleb teabetaotluses märkida. Teabetaotluses tuleb märkida:

1. Taotletava teabe kirjeldus

Tuleb täpsustada, millist konkreetset teavet taotletakse. See aitab adressaadil aru saada, milles seisneb taotluse sisu ning millistest allikatest või registritest võib teavet otsida.

2. Teabe taotlemise põhjus

Vaja on esitada asjaolud, miks teavet vajatakse, ja viide konkreetsele kuriteole, mille uurimisega seoses teavet küsitakse. See võimaldab hinnata, kas teabe taotlemine on põhjendatud.

3. Seos isikuga, kelle kohta teavet taotletakse

Kui teabetaotlus puudutab konkreetset isikut, tuleb selgitada, kuidas see isik on seotud kuriteoga – näiteks kas ta on kuriteos kahtlustatav, tunnistaja või ohver. Seos peab olema selgelt määratletud, et hinnata taotluse proportsionaalsust ja õiguspärasust.

4. Teabe kasutamise eesmärk

Tuleb kirjeldada, milleks taotletavat teavet kasutatakse – näiteks menetlustoimingute ettevalmistamiseks, loa taotlemiseks, kuriteo tõkestamiseks või ennetamiseks. Kui teavet soovitakse kasutada tõendina, peab see olema taotluses sõnaselgelt märgitud.

5. Põhjendus, miks eeldatakse, et teise EL-i liikmesriigi ühtsel kontaktpunktil või õiguskaitseasutusel on juurdepääs teabele

Uue nõudena tuleb selgitada, miks arvatakse, et teise riigi ühtsel kontaktpunktil või õiguskaitseasutusel on soovitud teave olemas. Selle eesmärk on vältida nn kalastamispäringuid, mis koormavad asjatult ühtseid kontaktpunkte.

6. Kiireloomulisuse põhjendus (vajadusel)

Kui taotlus esitatakse kiireloomulisena, tuleb põhjendada selle kiireloomulisust kooskõlas KrMS § 508⁹² lõikega 3. See aitab teisel riigil prioriseerida ja vajadusel kiirendada menetlust.

7. Teabe muul eesmärgil kasutamise piirangud

Tuleb täpsustada, kas taotletavat teavet soovitakse kasutada ainult taotluses nimetatud eesmärgil või ka muul otstarbel (nt edaspidises kriminaalmenetluses). Kui soovitakse laiemat kasutust, tuleb seda samuti põhjendada.

Rootsi direktiiviga kehtestatakse teabetaotlusele varasemast üksikasjalikumad nõuded. Kehtiva KrMS § 508⁷⁹ lõikega 1 nähakse ette, et välisriigile esitatavas teabetaotluses tuleb märkida taotluse esitamise põhjendus, teabe taotlemise põhjus ning seos taotluse esitamise aluseks oleva põhjuse ja isiku vahel, kelle kohta teavet soovitakse. Direktiiviga nähakse ette poole rohkem kohustuslikke elemente, mille täitmine annab vastuse kõikidele põhiküsimustele, mis on teabetaotlusele vastamise otsustamiseks ja vastama asumiseks vajalikud. Selline üksikasjalik nõuete loetelu aitab tagada, et teabetaotlus annab vastamise seisukohast vajaliku teabe juba esimesel esitamisel. See omakorda:

- vähendab vajadust esitada täpsustavaid päringuid;
- kiirendab teabetaotluste menetlemist;
- võimaldab tõhusamalt hinnata, kas on alust keelduda teabetaotlusele vastamisest (nt KrMS § 508⁹¹ lõike 1 punktide 1–12 alusel).

Eelkirjeldatud muudetud loetelu kehtestamine seaduses peaks lihtsustama ja kiirendama teabetaotluse esitamist. Seni kehtinud Rootsi raamotsus nägi eeltoodud taotluse kohustuslike andmete saamiseks ette vormid, mille pidi kehtiva KrMS § 508⁷⁹ lõike 2 kohaselt kehtestama riigisisest siseminister. Kuna ühtsed kontaktpunktid eelistasid vormivabadusest tulenevalt SIENA teabetaotluste tegemisele Interpoli teabevahetuskanalit, otsustati EL-i tasandil vastavate vormide kasutamisest loobuda. Eeltoodust tulenevalt on eelnõus loobutud vormi kehtestamiseks volitusnormi andmisest.

4. alljaotis

Omaalgatuslik teabeedastus

§ 508⁹⁶. Omaalgatuslik teabeedastus

Rootsi direktiivi artiklis 7 käsitletakse omaalgatuslikku teabeedastust ehk teabe edastamist teabetaotluseta. Sätte eesmärk on tagada, et EL-i liikmesriikide ühtsed kontaktpunktid ja pädevad õiguskaitseasutused edastaksid neil olemasolevat teavet enda partneritele teistes EL-i liikmesriikides omal algatusel siis, kui on alust arvata, et selline teave võib olla kuritegude tõkestamise, avastamise või uurimise jaoks asjakohane. Kuna teisele EL-i liikmesriigile teabetaotluse esitamise eelduseks on millegi kriminaalse asetleidmine ja põhjendatud eeldus, et teisel liikmesriigil on sellega seonduvat teavet, oleks teabe vahetamine teadmislünga tõttu

oluliselt piiratum, kui puuduks õiguslik alus teavet omal algatusel edastada. Uurimisasutused ei ole teadlikud kõikidest kriminaalsetest tegevustest ega oma ülevaadet sellest, milline kriminaalteave on nende ametivendadele teises riigis teada.

Omal algatusel teabeedastust reguleeritakse kehtiva KrMS §-ga 508⁸⁴, mis näeb ette võimaluse edastada PPA kaudu välisriigile asjakohast teavet ilma selleks eelnevat taotlust saamata. Eelnõuga muudetakse rasket kuritegevust puudutava olemasoleva teabe edastamine kohustuseks. Omaalgatusliku teabeedastuse sätestamine kohustusena on vajalik selleks, et täita Rootsi direktiivi põhieesmärki – võimaldada vabadusel, turvalisusel ja õigusel rajaneva ala tagamiseks liikmesriikide õiguskaitseasutustele samaväärne juurdepääs teabele, mis on kättesaadav nende kolleegidele teises liikmesriigis.

Omaalgatusliku teabeedastuse kohta kehtivad teabevahetuse üldreeglid. Näiteks tuleb teave edastada SIENA kaudu ning kui see ei ole ajutiselt võimalik, tuleb teabe edastamine SIENA-s esimesel võimalusel fikseerida. Samuti tuleb keeldumisaluste puudumisel ühtset kontaktpunkti teabevahetusest teavitada (hoida omaalgatusliku teabeedastuse koopias).

Lõikega 1 nähakse ette, et Eestil on kohustus edastada teisele EL-i liikmesriigile teavet kuritegude kohta, mille EL on määratlenud raskete kuritegudena. Rootsi direktiivi järgi peetakse rasketeks selliseid kuritegusid, mille eest on taotlevas riigis karistuse ülemmäärana ette nähtud vähemalt kolmeaastane vangistus. Selliseid kuritegusid puudutava teabe edastamist ei ole otstarbekas jätta liikmesriikide diskretsiooniks, mistõttu muudeti see kohustuslikuks. Seejuures tuleb silmas pidada, et teabe edastamise kohustuslikkus rakendub ka teabele, mis oli uurimisasutusel enne Rootsi direktiivi jõustumist ja mida ei ole veel teise EL-i liikmesriigi ühtsele kontaktpunktile või õiguskaitseasutusele või Europolile teatavaks tehtud.

Loetelu kuritegudest, mida peetakse Rootsi direktiivis rasketeks kuritegudeks, sisaldub kehtiva KrMS § 489⁶ lõikes 1. See tähendab, et Eesti ühtne kontaktpunkt ja uurimisasutus edastavad teisele EL-i liikmesriigi ühtsele kontaktpunktile või õiguskaitseasutusele omaalgatuslikult ehk teabetaotluseta teavet, mis võib aidata avastada, tõkestada või menetleda KrMS § 489⁶ lõikes 1 nimetatud (rasket) kuritegu, välja arvatud juhul, kui esineb eelnõukohase KrMS § 508⁹¹ lõike 1 punktis 6, 7, 8, 10 või 11 sätestatud keeldumise alus:

- **KrMS § 508⁹¹ lõike 1 punkt 6 – teabevahetusluba on vajalik, aga prokuratuur või kohus on sellest keeldunud.** Teatud liiki teabe (käimasoleva kriminaalmenetluse teave, näiteks teatud jälitustoimingutega kogutud andmed) avaldamine on KrMS § 214 lõike 1 kohaselt prokuratuuri ainupädevuses, kuna kohtueelset menetlust juhib – vastutades selle seaduslikkuse ja tulemuslikkuse eest – prokuratuur. Kohtumenetluse puhul on kohtuasja materjalide avalikustamise piiramise üle otsustamine kohtu ainupädevuses. Kui õigusasutus on loa andmisest keeldunud, on tegemist teadliku otsusega tasakaalustada uurimise huvid ja õiguste kaitse. Sellise keeldumise eiramine õhustaks nii riigisisest kriminaalmenetlusõigust kui ka kohtuliku kontrolli põhimõtet.
- **KrMS § 508⁹¹ lõike 1 punkt 7 – teabevahetus kahjustaks põhjendamatult juriidilise isiku seadusega kaitstud olulisi huve.** EL-i koostöö keskmes on kuritegude menetlemine, kuid see ei tohi põhjendamatult rikkuda ärisaladuste kaitset. Kui teave sisaldab näiteks äriplaane, tehnoloogilisi saladusi või finantsandmeid, mille avaldamine ei ole kuriteo menetlemiseks hädavajalik, tuleb neid kaitsta. Selline kaitse vähendab ka riski, et välisriigi asutused kasutaksid teavet eesmärkidel, mis ei ole seotud kuriteo uurimisega.

KrMS § 508⁹¹ lõike 1 punkt 8 – vastuolu riiklike julgeolekuhuvidega. Teatud andmed võivad puudutada riigi julgeolekut, mistõttu kuuluvad need erilise riikliku kaitse alla (teave riigikaitseobjektide kaitsemeetmete kohta, luure käigus saadud teave jms) ning nende edastamine isegi EL-i partnerile võib ohustada Eesti julgeolekut või kahjustada koostöösuhteid kolmandate riikidega. Selliste andmete avaldamise üle otsustamine on liikmesriikide ainupädevuses ja asjaolu, et need võivad sisaldada muu hulgas kriminaalteavet, ei kohusta liikmesriike sellist teavet vahetama. Seda põhjusel, et Euroopa Liidu lepingu⁷⁴ artikli 4 lõigete 1 ja 2 kohaselt ei kuulu riigi julgeoleku küsimused EL-i pädevusse.

- **KrMS § 508⁹¹ lõike 1 punkt 10 – oht isiku turvalisusele.** Teabevahetuses võib edastatav teave seada ohtu isiku või tema lähedaste elu ja tervise (eeskätt tunnistaja, ohvri või salajasele koostööle kaasatud isiku ning nende lähedaste puhul). Kui selline tõsiseltvõetav oht esineb, prevaleerivad Euroopa inimõiguste ja põhivabaduste harta artiklist 2 tulenev õigus elule, artiklist 6 tulenev õigus turvalisusele ja artiklist 7 tulenev õigus eraelu puutumatusele kriminaalmenetluse huvide ees, mistõttu andmete edastamisest tuleb keelduda.
- **KrMS § 508⁹¹ lõike 1 punkt 11 – oluline oht käimasolevale kriminaalmenetlusele.** Kohtueelne menetlus, eelkõige rasket kuritegevust ning piiriüleseid juhtumeid puudutav, nõuab sageli menetluse täielikku või osalist varjatust, et tagada menetluse tulemuslikkus. Teabe enneaegne või kontrollimatu avalikustamine võib oluliselt kahjustada uurimisasutuste võimalust koguda tõendeid, vähendada tunnistajate koostöövalmidust, kahjustada nende au ja väärikust ning takistada uurimisplaani elluviimist. Seetõttu on eriti oluline vältida olukordi, kus tahtlik või tahtmatu infoleke kahjustab kogu menetluse tulemust ja seega riigi õiguskaitse, julgeoleku või isiku põhiõiguste kaitse eesmärgi. Need ei piira põhjendamatult koostööd, vaid väldivad olukordi, kus koostöö võib kaasa tuua pöördumatut kahju.

Lõikega 2 nähakse ette, et ühtne kontaktpunkt ja uurimisasutus võivad edastada teise liikmesriigi ühtsele kontaktpunktile või õiguskaitseasutusele omal algatusel käesoleva paragrahvi lõikes 1 nimetatava teavet, mis võib aidata avastada, tõkestada või menetleda kuritegu.

Erinevalt lõikes 1 sätestatud kohustusest edastada teisele EL-i liikmesriigile rasket kuritegevust puudutavat teavet, on lõike 2 eesmärk seaduse tasandil julgustada uurimisasutusi vahetama kriminaalteavet oma partneritega teistes EL-i liikmesriikides ka siis, kui see teave ei puuduta rasket kuritegevust ehk kuritegusid, mis on loetletud KrMS § 489⁶ lõikes 1. Kuna igasugune kuritegevus ei oma piiriülest mõõdet ja sellist kriminaalteavet võib olla palju, ei kohustata Rootsi direktiiviga liikmesriike niisugust teavet vahetama. Eeltoodu aga ei tähenda, et uurimisasutusel ja ühtsel kontaktpunktil ei peaks olema võimalust vahetada kuritegevust puudutavat teavet, millest võib nende kolleegidele teistes EL-i liikmesriikides kasu olla. Uurimisasutus teeb kaalutusotsuse, hinnates, kas jagatav teave võiks olla teiste EL-i liikmesriikide kolleegidele kasulik või muutuks see neile pigem koormavaks. Eeskätt saab sellise otsuse langetada menetleja teabe infosüsteemi sisestamisel või tagantjärele tema juht. Ei ole mõistlik panna ühtsele kontaktpunktile ülesannet, mis eeldab kogu uurimisasutustes olemasoleva teabe analüüsi ja hindamist. Seejuures tuleb kaalutusotsuse tegemisel silmas pidada, et omal algatusel ei tohi vahetada teavet siis, kui esineb KrMS § 508⁹¹ lõike 1 punktides 7–11 sätestatud keeldumise alus, ehk teabevahetus:

a) kahjustaks põhjendamatult juriidilise isiku seadusega kaitstud olulisi huve (KrMS § 508⁹¹ lõike 1 punkt 7);

⁷⁴ Euroopa Liidu toimimise leping, ELT C 202/1, 7.6.2016, lk 1–390.

- b) läheks vastuollu riiklike julgeolekuhuvidega või kahjustaks neid (KrMS § 508⁹¹ lõike 1 punkt 8);
- c) oleks selle eesmärgi arvestades ebaproportsionaalne (KrMS § 508⁹¹ lõike 1 punkt 9);
- d) seaks ohtu isiku turvalisuse (KrMS § 508⁹¹ lõike 1 punkt 10);
- e) võiks märkimisväärselt kahjustada käimasolevat kriminaalmenetlust (KrMS § 508⁹¹ lõike 1 punkt 11).

Lõike 3 järgi kohaldatakse teabe koopia edastamisele KrMS § 508⁹³. See tähendab, et uurimisasutus peab teabe edastamisel saatma teabe koopia nii Eesti ühtsele kontaktpunktile kui ka teise EL-i liikmesriigi ühtsele kontaktpunktile KrMS §-s 508⁹³ sätestatud korras. Erandiks on vaid olukorrad, kus selline teabeedastus võiks ohustada käimasolevat kriminaalmenetlust, riigi julgeolekut või isiku turvalisust.

5. alljaotis

Teabeedastus Europolile

§ 508⁹⁷. Teabeedastus Europolile

Rootsi direktiivi põhjenduse nr 25 kohaselt on Euroopa kodanike turvalisuse ja julgeoleku tagamiseks oluline, et Europolil oleks vajalik teave, täitmaks oma rolli liidu kriminaalteabe keskusena, mis toetab pädevaid õiguskaitseasutusi. Seepärast tuleb teabevahetuse üksikjuhtumi puhul eraldi hinnata, kas Rootsi direktiivi alusel esitatud teabetaotluse või selle alusel vahetatud teabe koopia või uurimisasutusel olemasolev teave tuleks saata ka Europolile kooskõlas Europoli määruse artikli 7 lõikega 7.

Europoli määruse artikli 7 kohaselt on liikmesriikidel üldine kohustus teha Europolile kättesaadavaks kogu teave, mis on vajalik Europoli ülesannete täitmiseks, eelkõige raske kuritegevuse ja terrorismi ennetamise ja tõkestamise toetamiseks vajalik teave. Artikli 7 lõikega 7 täpsustatakse, et kui liikmesriigi pädev asutus vahetab teavet teise liikmesriigiga või kolmanda riigiga, peab ta hindama, kas see teave on ka Europoli töö seisukohalt asjakohane, ning edastama selle Europolile siis, kui teave on Europolile tema ülesannete täitmiseks vajalik. See tagab, et Europol saab täita oma kesket rolli kuritegevust puudutava teabe kogumisel ja analüüsimisel, vältides samal ajal olukorda, kus oluline teave jääb liidu õiguskaitsealase koostöö tasandil kasutamata.

Eeltoodu tähendab, et kui asjaomane kuritegu on hõlmatud Europoli eesmärkidega ehk puudutab rasket kuritegevust, tuleks vastav teave Europolile edastada.

Rootsi direktiivi artikliga 12 nähakse ette täpsemad reeglid Europolile teabe edastamiseks, mis võetakse Eesti õigusesse üle kõnesolevas sättes.

Lõikega 1 nähakse ette, et kui vahetatakse teavet kuriteo kohta, mille menetlemise toetamine on Europoli määruse artikli 3 kohaselt Europoli eesmärk, hindavad ühtne kontaktpunkt ja uurimisasutus igal üksikjuhul kooskõlas Europoli määruse artikli 7 lõikega 7, kas on vaja edastada teabetaotluse või selle vastuse või omaalgatusliku teabeedastuse korral teabe koopia Europolile. Europoli määruse I lisa kohaselt on Europoli pädevusse kuuluvad kuriteod:

- terrorism;
- organiseeritud kuritegevus;
- ebaseaduslik kauplemine narkootiliste ja psühhotroopsete ainetega;
- rahapesu;
- tuumamaterjali ja radioaktiivsete ainetega seotud kuritegevus;

- immigrantide ebaseaduslik üle piiri toimetamine;
- inimkaubandus;
- mootorsõidukitega seotud kuritegevus;
- tahtlik tapmine ja raskete kehavigastuste tekitamine;
- ebaseaduslik kauplemine inimorganite ja -kudedega;
- inimrööv, ebaseaduslik vabaduse võtmine ja pantvangi võtmine;
- rassism ja ksenofoobia;
- rööv ja vargus raskendavatel asjaoludel;
- ebaseaduslik kauplemine kultuuriväärtustega, sealhulgas antiikesemete ja kunstiteostega;
- kelmus ja pettus;
- liidu finantshuvide vastu suunatud kuriteod;
- siseteabe alusel kauplemine ja finantsturuga manipuleerimine;
- väljapressimine ja raha väljapressimine;
- toodete võltsimine ja piraatkoopiate valmistamine;
- haldusdokumentide võltsimine ja nendega kauplemine;
- raha ja maksevahendi võltsimine;
- arvutikuriteod;
- korruptsioon;
- ebaseaduslik kauplemine relvade, laskemoona ja lõhkeainetega;
- ebaseaduslik kauplemine ohustatud loomaliikidega;
- ebaseaduslik kauplemine ohustatud taimeliikide ja -sortidega;
- keskkonnakuriteod, sealhulgas laevade põhjustatud reostus;
- ebaseaduslik kauplemine hormoonpreparaatide ja muude kasvukiirendajatega;
- seksuaalne kuritarvitamine ja seksuaalne ärakasutamine, sealhulgas laste kuritarvitamist kujutav materjal ja laste ahvatlemine seksuaalsuhte eesmärgil;
- genotsiid, inimsusvastased kuriteod ja sõjakuriteod.

Lõike 2 kohaselt määrab enne Europolile teabe edastamist ühtne kontaktpunkt või uurimisasutus Europolile määruse artikli 19 kohaselt kindlaks teabe töötlemise eesmärgi ja võimalikud piirangud.

Kooskõlas andmete omandiõigusega nähakse lõikega 2 ette, et teave, mis algselt saadi teiselt EL-i liikmesriigilt või kolmandalt riigilt, saadetakse Europolile ainult juhul, kui see teine riik on andnud selleks nõusoleku ja kehtestanud teabele kasutamise tingimused. Europol tohib andmeid töödelda vaid kooskõlas Europolile määruses sätestatud normidega, sealhulgas eesmärgiga.

Kõik isikuandmed, mida ühtne kontaktpunkt või uurimisasutus Europolile edastab, peavad kuuluma Europolile määruse II lisa B jaos sätestatud andmekategooriate hulka. Need on konkreetselt määratletud andmetüübid, mida tohib töödelda kuritegude ennetamise, uurimise ja tõkestamise eesmärgil. Lubatud andmekategooriad on järgmised:

- 1) perekonnanimi, sünninimi, eesnimed ja varjunimed;
- 2) sünniaeg ja -koht;
- 3) kodakondsus;
- 4) sugu;
- 5) elukoht, amet ja asukoht;
- 6) sotsiaalkindlustuse numbrid, identifitseerimiskoodid, juhiloa, isikut tõendavad dokumendid, passiandmed, tolli identifitseerimisnumbrid ja maksukohustuslasena registreerimise numbrid;
- 7) kuritegude kirjeldus, toimepanemise kuupäev ja liik;
- 8) teave juriidiliste isikute kohta, kellel on seos uurimise all oleva isikuga;

- 9) teave isiku kuulumise kohta kuritegelikku organisatsiooni;
- 10) pangakontod ja muud finantskontod;
- 11) telefoninumbrid, SIM-kaardi numbrid, e-posti aadressid, IP-aadressid ja veebiplatvormide kasutajakontod;
- 12) sõidukite registreerimisandmed;
- 13) tuvastatav vara, mida isik omab või kasutab (nt krüptovara ja kinnisvara).

Andmekategooriate piiramine on vajalik selleks, et tagada:

- andmete asjakohasus ja seotus uurimise eesmärgiga;
- isikuandmete kaitse ning
- vältida liigset andmetöötlust.

See tähendab, et isegi kui uurimisasutusel on ligipääs täiendavatele isikuandmetele, ei tohi neid Europolile edastada, kui need ei kuulu määruuses loetletud kategooriate alla ega ole otseselt seotud kuritegevuse uurimisega. Näiteks, kuigi uurimisasutustel võib olla ligipääs isiku etnilise päritolu, poliitiliste vaadete, religioossete uskumuste, terviseandmete või eraelu kohta käivatele andmetele, ei kuulu need määruuses loetletud kategooriate alla ega seega ka vahetamisele.

Eelnõu § 1 punktiga 3 jäetakse KrMS-i normitehnilisest märkusest välja viide Rootsi raamotsusele, kuna Rootsi direktiivi artikli 21 kohaselt tunnistati see alates 2024. aasta 12. detsembrist kehtetuks.

Eelnõu § 1 punktiga 4 täiendatakse KrMS-i normitehnilist märkust viitega Rootsi direktiivile ja direktiivile 2023/2123, et oleks selge, et KrMS-is võetakse üle nende direktiivide sätted.

Eelnõu § 2. KrMSRS-i täiendamine

Eelnõu §-ga 2 täiendatakse KrMSRS §-ga 25⁹, milles nähakse ette KrMS § 508⁸⁷ rakendamise erisus uurimisasutustele SIENA kasutamise suhtes. Rootsi direktiivi artiklis 22 on toodud võimalus teha Rootsi direktiivi artikli 13 nõuete järgimise suhtes erisus ja rakendada SIENA täieliku kasutuselevõtu osas pikemat tähtaega. Nii nähaksegi KrMSRS §-ga 25⁹ ette, et KrMS §-ga 508⁸⁷ sätestatud kohaldatakse 2027. aasta 12. juunini üksnes nendele uurimisasutustele, kes on otse ühendatud SIENA-ga.

Maksimaalne üleminekutähtaeg on vajalik selleks, et kõik uurimisasutused ei ole veel SIENA-ga otse ühendatud. Ühendamisprotsess on alles käimas ning üleminekuperioodil on kavas lõpule viia uue töövoosüsteemi arendus ja koolitada neid uurimisasutuste ametnikke, kes ei ole SIENA-t seni kasutanud. Kuna koolitusi viivad läbi töötajad, kelle põhiülesanne on igapäevane operatiivtöö, ei ole realistlik direktiivi nominaaltähtajast kiiremini üle võtta. Samuti tuleb arvestada, et kuigi olemasolev töövoosüsteem võimaldab teabevahetust, ei vasta see täielikult direktiivis sätestatud automatiseerimisnõuetele. Seetõttu ei ole mõistlik koolitada uurimisasutuste ametnikke vana süsteemi kasutamiseks, kui lähiajal plaanitakse kasutusele võtta uus lahendus. Seniks, kuni uus töövoosüsteem valmib ja kõik uurimisasutused on SIENA-ga liidestatud, tagab teabevahetuse toimimise olemasoleva süsteemi kaudu PPA.

Eelnõu § 3. PPVS-i muudatused

Eelnõu §-s 3 on esitatud Rootsi direktiivi rakendamiseks vajalikud PPVS-i muudatused.

Eelnõu § 3 punktiga 1 parandatakse PPVS § 25² lõike 6 punktis 2 terminikasutust. Kehtiva PPVS § 25² lõike 6 punktis 2 kasutatud Europoli nimetus ei ole korrektne. Alates Europoli määruse jõustumisest on Europoli ametlik nimi „Euroopa Liidu Õiguskaitsekoostöö Amet“.

Europoli varasemat ametlikku nime „Euroopa politseiamet“ ei ole Europoli määruse jõustumisest arvates korrektne kasutada, kuna Europoli määrusega tunnistati kehtetuks nõukogu otsus 2009/371/JSK⁷⁵, millega Europol loodi ja milles oli sätestatud selle asutuse varasem ametlik nimetus.

Eelnõu § 3 punktis 2 täiendatakse PPVS-i uue peatükiga 3¹, milles nähakse ette teabevahetus EL-i liikmesriikide vahel ja Europoliga kuritegude avastamise, tõkestamise ja menetluse läbiviimise eesmärgil. Eelnõu ettevalmistamisel leiti, et kõiki Rootsi direktiivi korrektseks ülevõtmiseks olulisi sätteid ei ole asjakohane lisada KrMS-i kui peamiselt kriminaalmenetlust reguleerivasse õigusakti. Seetõttu lisataksegi eelnõu järgi osa regulatsioonist PPVS-i. Lisatavad normid puudutavad eelkõige ühtse kontaktpunkti toimimist. Kuna ühtne kontaktpunkt on PPA, siis on sobilik lisada vajalikud sätted PPVS-i kui politsei ülesandeid, õigusi ja korraldust reguleerivasse seadusesse.

§ 25⁸. Ühtse kontaktpunkti ülesanded

PPA täidab KrMS § 508⁸⁶ lõikes 1 nimetatud ühtse kontaktpunktina järgmisi ülesandeid:

- 1) korraldab KrMS 19. peatüki 8. jao 10. jaotise kohaselt teabevahetust EL-i liikmesriikide vahel ja Europoliga (edaspidi käesolevas peatükis *teabevahetus*);
- 2) registreerib ja talletab teabevahetuse;
- 3) tagab teabevahetuse kohta statistika kogumise ja selle nõuetekohase edastamise Euroopa Komisjonile.

Need ülesanded on enamjaolt sätestatud KrMS 19. peatüki 8. jao 10. jaotises, kuid ühtse kontaktpunkti töö paremaks korraldamiseks on otstarbekas loetleda need ka PPVS-is. Neid ülesandeid on täpsemalt kirjeldatud seletuskirjas eespool KrMS-i sätete juures.

§ 25⁹. Töövoosüsteem

Rootsi direktiivi kohaselt peavad ühtsed kontaktpunktid kasutusele võtma teatavate miinimumfunktsioonide ja -suutlikkusega ühtse elektroonilise töövoosüsteemi ning seda haldama. See on vajalik selleks, et ühtne kontaktpunkt saaks täita tulemuslikult ja tõhusalt kõiki direktiivikohaseid ülesandeid, eelkõige seoses teabevahetusega. Kõnesoleva sättega võetakse Eesti õigusesse üle Rootsi direktiivi artikkel 16.

Lõike 1 kohaselt registreerib ja talletab ühtne kontaktpunkt kogu KrMS 19. peatüki 8. jao 10. jaotises nimetatud teabevahetuse ning tagab sellekohase statistika kogumise töövoosüsteemis. Normi eesmärk on sätestada töövoosüsteemi olemasolu, mis võimaldab ühtsel kontaktpunktil hallata kogu teabevahetust ning koguda ja analüüsida teabevahetuse statistikat. Süsteem peab vastama Rootsi direktiivis sätestatud miinimumnõuetele, võimaldades seeläbi usaldusväärset, turvalist ja jälgitavat andmevahetust.

Juba praegu on ühtsel kontaktpunktil elektrooniline töövoosüsteem kasutusel. See on praegu eelkõige PPA SIRENE büroo juhtumihaldus- ja töövoosüsteem. Olemasolev elektrooniline töövoosüsteem ei vasta aga Rootsi direktiiviga ettenähtud nõuetele, eelkõige automatiseerituse osas, sest praegu tehakse palju tööd käsitsi. Ühtne kontaktpunkt vastutab ka praegu lõppkasutajate taotluste alusel linkide loomise, märgendite ehk n-ö lippude lisamise, laienduste

⁷⁵ Nõukogu 6. aprilli 2009. aasta otsus, millega asutatakse Euroopa Politseiamet (Europol) ([ELT L 121, 15.5.2009, lk 37–66](#)).

ja SIS-i Eesti hoiatusteadete kättesaadavuse piiramise eest. Ühtse kontaktpunkti ametnikud kontrollivad kõiki saabuvald teabetaotlusi enne konkreetsetele juhtumit lahendavatele ametnikele määramist käsitsi ning kopeerivad ja kleeбивad käsitsi Schengeni ID-d, nimed jm vajalikud andmed teistesse asjakohastesse infosüsteemidesse. Eri andmekomplektide vahel navigeerimisel on vormi kinnitamiseks juhtumile vaja teha mitu klõpsu.

Automatiseerimise puudumine võib kaasa tuua ebatõhusa ja aeglase teabe vahetamise ning ohustada kuritegudele tõhusat reageerimist nii Eestis kui ka teistes EL-i liikmesriikides. Seetõttu on vaja parandada olemasolevat töökorraldust ning tagada ametnikele tänapäevased ja EL-i nõuetele vastavad töövahendid ja IT-lahendused.

Lõikega 2 nähakse ette, et töövoosüsteemi vastutav töötaja ehk asutus, kes teeb otsuse töötlemise teatavate põhielementide kohta, on PPA. Tema määrab kindlaks andmete töötlemise eesmärgid ja vahendid ehk andmete töötlemise põhjuse ja viisi, arvestades nii käesoleva eelnõuga seatavaid ülesandeid kui ka kehtivas õiguses sätestatud andmekaitsereegleid. See roll paneb PPA-le olulised ülesanded ja kohustused nii andmekaitse kui ka töövoosüsteemi haldamise seisukohast. PPA ülesanded vastutava töötlejana on järgmised:

1. Töövoosüsteemi loomine ja haldamine:

- tagab, et töövoosüsteem vastab KrMS-is sätestatud miimumfunktsioonidele ja -nõuetele;
- loob süsteemi, mis võimaldab ühtsel kontaktpunktil täita KrMS-ist tulenevaid teabevahetusülesandeid tõhusalt, kiirelt ja turvaliselt.

2. Andmetöötlemise eesmärkide määratlemine ja järelevalve:

- määrab kindlaks, milliseid andmeid töövoosüsteemis töödeldakse ning kuidas andmete töötlemine toimub, lähtudes Rootsi direktiivis ja riigi seadustes sätestatust;
- jälgib, et andmete töötlemine oleks vajalik, proportsionaalne ja eesmärgipärane.

3. Andmekaitse ja infoturbe tagamine:

- rakendab tehnilisi ja korralduslikke meetmeid, et tagada andmete turvalisus ning konfidentsiaalsus, vältida loata juurdepääsu, kaotsimineku, hävimist või väärkasutust;
- veendub, et andmetöötlus on kooskõlas EL-i üldise andmekaitse regulatsiooni ja IKS-iga.

4. Koolitus ja juhendamine:

- tagab, et kõik töötajad, kes tegelevad töövoosüsteemiga, on teadlikud andmekaitse nõuetest ja direktiivis sätestatud ülesannetest;
- pakub vajalikku väljaõpet süsteemi kasutamiseks ja andmete õiguspäraseks töötlemiseks.

5. Koostöö teiste osapooltega:

- teeb koostööd teiste EL-i liikmesriikide ühtsete kontaktpunktide ja õiguskaitseasutustega;
- koordineerib riiklikul tasandil uurimisasutuste vajadusi ja tagab töövoosüsteemi kasutamise ühtsuse.

PPA kohustused vastutava töötlejana on järgmised:

1. **Õigusaktide järgimine:** PPA peab täitma kõiki KrMS 19. peatüki 8. jao 10. jaotises sätestatud nõudeid ning tagama, et andmetöötlus toimub kooskõlas Eesti seadustega ja EL-i õigusraamistikuga.
2. **Andmesubjektide õiguste tagamine:** PPA vastutab selle eest, et andmesubjektidel oleksid tagatud kõik seadusest tulenevad õigused, nagu juurdepääs isikuandmetele, andmete parandamine ja kustutamine, kui see on õigustatud.
3. **Riskijuhtimine ja auditid:** PPA peab hindama töövoosüsteemiga seotud riske ning tagama, et süsteem on regulaarselt auditeeritud. See hõlmab infoturbe hindamisi ja vastavuskontrolle.
4. **Teavitamine rikkumise korral:** kui töövoosüsteemis esineb andmekaitserikkumine, on PPA kohustatud sellest teavitama järelevalveasutust (Andmekaitse Inspektsiooni) ning vajaduse korral ka andmesubjekte.
5. **Tehnoloogiline arendamine:** PPA peab tagama töövoosüsteemi ajakohasuse, et see vastaks pidevalt muutuvatele tehnoloogilistele ja õiguslikele nõuetele.

Selleks et töövoosüsteem tõhusalt ja õiguspäraselt toimiks, on vaja lisaks seaduses sätestatudle näha alamaktis ette teatud nõuded. Nii antakse lõikega 3 valdkonna eest vastutavale ministrile ehk siseministrile õigus kehtestada nõuded töövoosüsteemi toimimisele, ülesehitusele ja haldamisele ning selle andmete töötlemisele, logimisele, kontrollile, juurdepääsule, väljastatavale statistikale ja järelevalvele (rakendusakti kavand on esitatud seletuskirja lisas 2).

Siseministri määrusega kehtestatakse töövoosüsteemi kasutusele võtmise ja haldamise tingimused, mis tagavad Rootsi direktiivi artikli 16 lõike 1 nõuetele vastava elektroonilise juhtumite haldamise süsteemi. See hõlmab süsteemi arhitektuuri, rahvusvaheliste teabevahetuskanalitega (Europoli SIENA, Schengeni SIRENE, Interpoli i24/7) liidestatust ning nõudeid andmete töötlemisele, statistika kogumisele, logimisele ja turvasemele.

Määruses määratletakse süsteemi haldaja ja vastutava töötaja (PPA) ülesanded ning reguleeritakse töövoosüsteemile juurdepääsu tingimusi, lõppkasutajate õigusi ja kohustusi ning regulaarset kontrolli ja järelevalvet. Lisaks nähakse ette kohustus koguda ja esitada statistikat rahvusvahelise teabevahetuse kohta, et tagada süsteemi töökindlus, õiguslik vastavus ja tõhusus ning toetada poliitikakujundamist ja aruandlust Euroopa Komisjoni suunal.

Isikuandmete töötlemise toiminguid tuleb töövoosüsteemis logida. Andmete väljastamise seaduslikkuse tagamiseks nähakse PPVS § 25⁹ lõike 3 alusel kehtestatavas rakendusaktis ette, et isikuandmete töötlemise toimingud logitakse. Logimise kohustust kohaldatakse kõikidele töötlemistoimingutele, mis teostatakse automatiseeritud viisil ehk infotehnoloogilise lahenduse abil.

Ühtne kontaktpunkt peab läbi mõtlema, millisel viisil teabetaotluse põhjendatuse kontrollimist korraldada (kas käsitsi või rakendatakse automaatkontrolle, mis annavad teatud kriteeriumide esinemisel häireteate). See peab toimima selliselt, et oleks võimalik leida vastuseid järgmistele küsimustele: mida keegi põhjustas (st kasutas), millal ta seda tegi ning milliseid vahendeid ta rakendas. Samuti peaks logimine aitama vastata küsimustele süsteemi seisundi kohta: kellel olid pääsuõigused, millised need olid ja millises ajavahemikus need kehtisid. IT-süsteemide usaldusväärse töö tagamiseks on vajalik, et infokoosluses saaksid logitud kõik turbe seisukohalt kriitilised sündmused. Logimise eesmärk on aidata mõista, miks ja kuidas leidsid IT-süsteemides ja rakendustes aset olulised muutused, et hinnata süsteemide ja rakenduste turvet. Andmekaitse seisukohast on logimise eesmärk tagada, et automatiseeritud töötlemisel säilib jälg teostatud toimingu kohta, mis võimaldab kontrollida töötlemise õiguspärasust ning hinnata tehtud toimingute vastavust kehtestatud nõuetele.

Logisid tuleb pidada järgmiste isikuandmete töötlemise toimingute kohta:

- 1) avalikustamine;
- 2) edastamine;
- 3) kogumine;
- 4) kustutamine;
- 5) lugemine;
- 6) muutmine;
- 7) ühendamine.

Logisid kasutatakse üksnes isikuandmete töötlemise toimingute seaduslikkuse kontrollimiseks, siseseireks, isikuandmete tervikluse ja turvalisuse tagamiseks ning kriminaalmenetluses. Logimine on vajalik selleks, et näiteks andmelekked korral oleks võimalik tuvastada isikuid, kes on neid andmeid lugenud või teisele isikule edastanud.

Rakendusaktis nähakse ette, et **logiandmeid säilitatakse kaks aastat** isikuandmete töötlemise toimingu tegemisest arvates. Kuna ka logid on isikuandmed, tuleb säilitamise põhimõtte täitmiseks kehtestada logide säilitamise tähtajad ning need säilitamise tähtaja möödumisel jäädavalt kustutada. Logiandmete säilitamise tähtaja seadmisel on lähtutud mitmetest teguritest, sealhulgas õiguslikest nõuetest, turvalisusest, andmekaitse ja andmeturbe põhimõtetest ning organisatsiooni spetsiifilistest vajadustest. Logide säilitamise tähtaeg peab arvestama andmekaitse põhimõtteid, sealhulgas proportsionaalsuse, vajalikkuse ja piiratud säilitamise põhimõtteid, nagu on sätestatud EL-i isikuandmete kaitse regulatsioonides (nt direktiiv 2016/680).

1. **Turvalisus.** Logiandmed võivad olla olulised turvaintsidentide uurimisel ja lahendamisel. Tavaliselt on soovitatav säilitada logiandmeid piisavalt kaua, et katta võimalikud turvaohutude avastamise ja uurimise vajadused.
2. **Andmekaitse põhimõtted.** Õiguskaitse direktiivis nõutakse, et isikuandmeid, sealhulgas logiandmeid, säilitatakse ainult nii kaua, kui see on vajalik nende kogumise eesmärgi täitmiseks. See tähendab, et logiandmete säilitamise periood peaks olema proportsionaalne nende kasutuseesmärkidega.
3. **Organisatsiooni vajadused.** Arvestama peab ka seda, kui kaua on logiandmed vajalikud organisatsiooni tegevuse ja operatiivsete vajaduste seisukohalt. See võib hõlmata vajadust tõendada andmete töötlemisega seonduvaid tegevusi või muud olulist teavet.

Kuna tegemist on süütegude menetlemisega seotud andmetöötluse ja -edastusega, siis nähakse määruses ette logide säilitamise tähtaeg, mis lähtub väärkasutuste karistatavuse aegumistähtsajast. Kuna logiandmeid kasutatakse turvalisuse tagamiseks ja turvaintsidentide uurimiseks, on asjakohane säilitada neid kahe aasta jooksul. Arvestades, et AvTS § 54¹ lõike 1 kohaselt on asutusesiseseks kasutamiseks ettenähtud teabe avalikustamise või väljastamise näol tegemist väärteoga, mille aegumistähtaeg on KarS § 81 lõike 3 kohaselt üldreeglina kaks aastat, ja et [avaliku teenistuse seaduse](#) § 77 lõike 1 kohaselt on distsiplinaarrikkumise aegumistähtaeg samuti kaks aastat, on põhjendatud ka logide säilitamine vastava aja, s.o kahe aasta jooksul.

Rootsi direktiivi artikliga 18 nähakse EL-i liikmesriikidele ette kohustus esitada Euroopa Komisjonile teabevahetuse kohta statistikat. Selleks et Rootsi direktiivist tulenevat kohustust paremini täita, nähakse rakendusaktis ette, et **ühtne kontaktpunkt esitab iga aasta 1. märtsiks Euroopa Komisjonile teabevahetuse statistika** eelmise kalendriaasta jooksul teiste EL-i liikmesriikidega toimunud teabevahetuse kohta. Selline nõue tuleneb Rootsi direktiivi artikli 18 lõikest 1. Määruses tuuakse õigusselguse huvides välja, millist statistikat ühtne kontaktpunkt

kogub ja Euroopa Komisjonile esitab. Tegemist on Rootsi direktiivi artikli 18 lõikes 2 esitatud loeteluga. Statistika kogumise eesmärk on tagada EL-is teabevahetuse läbipaistvus ja hinnata liikmesriikide vahelist koostööd. Iga punkt hõlmab konkreetset andmeliiki, mida kogutakse järjepidevalt ning esitatakse Euroopa Komisjonile regulaarselt. Selle järgi hõlmab statistika vähemalt järgmisi andmeid:

1) **ühtse kontaktpunkti või uurimisasutuse teabetaotluste arv** – näitab, kui aktiivselt Eesti kasutab võimalust taotleda kriminaalmenetluses vajalikku teavet teistelt EL-i liikmesriikidelt. Näiteks kui uurimisasutus saadab teabetaotluse Saksamaa kontaktpunktile, kajastub see statistikas ühe juhtumina;

2) **EL-i liikmesriigi teabetaotluste arv** – illustreerib, kui sageli pöörduvad teised liikmesriigid Eesti poole kriminaalmenetlusega seotud teabe saamiseks. Näiteks võib Soome kontaktpunkt paluda Eesti ametiasutustel kinnitada isiku Eestis viibimist kindlal ajahetkel;

3) **EL-i liikmesriikide ja kiireloomulisuse kaupa selliste teise liikmesriigi ühtse kontaktpunkti või õiguskaitseasutuse teabetaotluste arv, mille alusel on ühtne kontaktpunkt või uurimisasutus teavet edastanud** – näitab, milliste riikide taotlustele on Eesti vastanud ning kas taotlused olid märgitud kiireloomuliseks. Näiteks kui Läti ühtne kontaktpunkt märgib, et teavet on vaja viivitamata, kajastub see statistikas kui kiireloomuline vastus Lätile;

4) **EL-i liikmesriikide ja keeldumise aluste kaupa selliste teise liikmesriigi ühtse kontaktpunkti või õiguskaitseasutuse teabetaotluste arv, mille alusel teabeedastusest on KrMS § 508⁹¹ lõike 1 alusel keeldunud** – kogutakse infot juhtumite kohta, kus teabeedastusest keelduti, viidates KrMS § 508⁹¹ lõikele 1. Näiteks võib keeldumise aluseks olla oht isiku turvalisusele või teabele ligipääsu puudumine. Statistika aitab hinnata, kui sageli ja millistel alustel keeldutakse koostööst;

5) **EL-i liikmesriikide kaupa selliste teise liikmesriigi ühtse kontaktpunkti või õiguskaitseasutuse teabetaotluste arv, millele vastamise tähtajast on KrMS § 508⁹² lõike 4 punkti 2 alusel kõrvale kaldunud** – ilmestab olukordi, kus vastamise tähtaega ei ole järgitud põhjusel, et teabeedastuseks on vaja teabevahetusluba. Statistika aitab Euroopa Komisjonil jälgida, kui tihti ja millistes olukordades liikmesriigid tähtaja ületavad.

§ 25¹⁰. Töövoosüsteemi andmed

Paragrahviga 25¹⁰ sätestatakse töövoosüsteemis registreeritavad andmed, mis on vajalikud EL-i liikmesriikide ühtsete kontaktpunktide, õiguskaitseasutuste ja Europoli vahelise teabevahetuse dokumenteerimiseks ja haldamiseks.

Sätestatakse, milliseid andmeid töövoosüsteemis töödeldakse KrMS 19. peatüki 8. jao 10. jaotises reguleeritud rahvusvahelise õiguskaitsealase teabevahetuse käigus. Säte on vajalik, et tagada:

- selgus ja ühtne arusaam sellest, millised andmekategooriad peavad olema töövoosüsteemis dokumenteeritud;
- kooskõla EL-i õigusega, sealhulgas Europoli määrusega;
- läbipaistvus ja jälgitavus piiriüleses teabevahetuses;
- andmetöötluse eesmärgipärasus ning isikuandmete kaitse nõuete täitmine.

Töövoosüsteemis kajastatakse teabetaotluste ja teabeedastuste menetlusega seotud põhiandmeid, sealhulgas taotluse sisu, täpsustused, puudused ja tähtaegade järgimine, samuti teabevahetus ühtse kontaktpunkti ja uurimisasutuste vahel. Regulatsioon aitab tagada menetlusinfo struktureeritusse ja läbipaistvuse ning loob aluse usaldusväärse statistika kogumiseks ja tööprotsesside auditeerimiseks.

Rootsi direktiivi artikli 9 lõike 2 kohaselt peab kriminaalmenetluses toimuva isikuandmete töötlemise ulatus olema piisavalt selgelt sätestatud liikmesriigi riigisisises õiguses. Selle nõude täitmiseks ning töötlemise seaduslikkuse ja õigusselguse tagamiseks sätestatakse töövoosüsteemis töödeldavate isikuandmete kategooriad, lähtudes Europol'i määruse II lisa B jaos sätestatud andmekategooriatest, mille töötlust peetakse kuritegude ennetamise, avastamise ja uurimise eesmärgil vajalikuks. Lisaks eelnimetatud nn Europol'i isikuandmete kategooriatele, mis on faktipõhised – näiteks registripäringutest või dokumentidest pärinevad andmed – võetakse direktiivi ülevõtmisel arvesse vajadust töödelda teavet, mis on saadud uurimisasutuse või välisriigi õiguskaitseasutuse seadusega lubatud toimingute (näiteks ülekuulamised) käigus, sealhulgas jälitustegevuse raames või vihje kaudu. Ehkki sellise teabe tõeväärtus võib olla ebaselge, täpsustamist või tõendamist vajav, on niisuguse menetlusteabe või menetluseelse teabe kiire vahetamine vajalik tõhusaks kuritegude avastamiseks ja tõkestamiseks, aga ka toimepandud kuritegude puhul toimepanijate ja muu tõendusteabe leidmiseks. Seetõttu tuleb töövoosüsteemis sellise teabe puhul selgelt märkida, et tegemist on teabega, mis ei pruugi kajastada faktilist asjaolu, vaid võib põhineda hinnangutel, oletustel (inimallikatelt saadud vihjetel või ütlustel), ning et need andmed tuleb kustutada või parandada koheselt, kui selguvad täpsemad asjaolud. Samuti tuleb märkida, et ehkki sellise teabe kasutamine võib olla oluline teabetaotluse või -edastuse menetlemisel, on andmete töötlemine lubatud üksnes juhul, kui see on vajalik konkreetse kuriteo avastamiseks, tõkestamiseks või menetlemiseks, ning see ei ole mõeldud kuulujuttude või kontrollimata oletuste kogumiseks. Selliselt tagatakse, et töövoosüsteemis kajastuv teave oleks asjakohane ja eesmärgipärane ning selle kasutamine oleks kooskõlas isikuandmete töötlemise põhimõtetega, isegi kui selle tõeväärtus võib algaasis olla veel väljaselgitamisel.

Rootsi direktiivi artikliga 16 sätestatakse kohustus neid andmeid koguda ja selliselt liigitada selleks, et täita Rootsi direktiivi artiklist 19 tulenevat aruandluskohustust. Andmete määratud kujul kogumise eesmärk on lihtsustada andmeanalüüsi, teostada järelevalvet liikmesriikide poolt direktiivi ülevõtmise ja täitmise üle ning paremini tuvastada andmete pinnalt ilmnevaid regulatsiooni probleemkohti. Sama eesmärki täidab ka EL-i liikmesriikide poolt iga-aastase statistika esitamine Euroopa Komisjonile.

PPVS § 25¹⁰ koosneb neljast lõikest, milles on eristatud andmete kogumine vastavalt menetlustoimingu liigile:

1. lõige 1 – andmed, mis dokumenteeritakse teise EL-i liikmesriigi taotlusele vastamisel, sealhulgas taotluse sisu, isikuandmed, kiireloomulisus, puudused, selgitused, vastuse sisu ja tähtaegadest kinnipidamine;
2. lõige 2 – andmed, mis dokumenteeritakse Eesti-poolse taotluse esitamisel, sealhulgas taotluse sisu, isikuandmed, koopia edastamise andmed ja võimalik kiireloomulisus;
3. lõige 3 – andmed omaalgatusliku teabeedastuse kohta, sealhulgas edastatud teabe sisu ja koopia;
4. lõige 4 – andmed Europol'ile edastatud teabe kohta, sealhulgas teave, isikuandmed, koopia ja lisaselgitused.

Kõigis lõigetes on keskne element isikuandmete töötlemine vastavalt Europol'i määruse lisas II sätestatud kategooriatele. See on vajalik nii EL-i õigusest tuleneva kohustuse kui ka menetluste ühtlustamise eesmärgil.

Sätte rakendamine suurendab andmetöötlemise läbipaistvust, kuna töövoosüsteem võimaldab:

- dokumenteerida iga teabevahetuse etappi;
- jälgida tähtaegade järgimist;
- põhjendada otsuseid, sealhulgas teabeedastusest keeldumist.

Isikuandmete töötlemisel järgitakse IKS-i ja Europoli määruse nõudeid. Sätte sõnastus välistab ebaseadusliku või eesmärgipäratult laia andmekogumise.

§ 25¹¹. Töövoosüsteemi andmete säilitamine

Lõikega 1 nähakse ette, et töövoosüsteemis säilitatakse isikuandmeid kuni kaks aastat teabevahetuse lõppemisest arvates, arvestades käesolevas paragrahvis sätestatud erisusi. Lõike 1 eesmärk on määrata isikuandmete säilitamise tähtaeg töövoosüsteemis, lähtudes proportsionaalsuse põhimõttest ja Rootsi direktiivi artikli 16 lõike 3 nõudest, mille kohaselt tuleb andmeid säilitada vaid nii kaua, kui see on vajalik ühtse kontaktpunkti ülesannete täitmiseks. Üldreeglina on selleks piisavaks ajaks kaks aastat pärast teabevahetuse lõppu. Samas ei säilitata vaikimisi kõiki andmeid kogu selle perioodi vältel – Rootsi direktiivi artikli 16 lõike 4 kohaselt tuleb hiljemalt kuus kuud pärast teabevahetuse lõppu hinnata, kas andmete säilitamine on jätkuvalt vajalik, ning kustutada need enne maksimaalse tähtaja saabumist siis, kui nende säilitamine ei ole enam põhjendatud.

Kaheaastase säilitamistähtaja kehtestamine lähtub vajadusest tagada andmete kättesaadavus perioodi jooksul, mil võib osutuda vajalikuks kontrollida direktiivikohase andmetöötluse õiguspärasust. Rootsi direktiivi artikli 18 lõike 1 kohaselt peavad liikmesriigid edastama Euroopa Komisjonile kord aastas statistika direktiivikohase andmetöötluse kohta ning Komisjoni poolt statistika koondamise ja võrdlemise käigus võivad ilmned viited andmetöötlusnõuete rikkumistele. Rikkumiste kontrollimiseks peab liikmesriigil olema võimalik andmeid säilitada ja vajaduse korral taasisikustada selleks, et tagada andmesubjektide õiguste kaitse ning võtta rikkumiskahtluse tõeks osutumisel toimepanijad vastutusele. Kuna eelkirjeldatud rikkumised saavad olla valdavalt distsiplinaarsüüteo, mille aegumistähtaeg on avaliku teenistuse seaduse § 77 lõike 1 kohaselt kaks aastat alates süüteo toimepanemisest, on ka töövoosüsteemis isikuandmete säilitamise tähtaeg määratud samaks perioodiks. Seeläbi on säilitustähtaeg piiratud üksnes hädavajalikkuga, tagades tasakaalu järelevalve- ja aruandlusvajaduste ning isikuandmete kaitse põhimõtete vahel.

Samas sätestatakse lõikega 2 selged erandid, mille puhul võib isikuandmeid säilitada kauem kui kaks aastat. Töövoosüsteemis võib säilitada teabevahetuse isikuandmeid üle kahe aasta teabevahetuse lõppemisest arvates, kuni infosüsteemis POLIS, Schengeni infosüsteemi riiklikus registris või Interpoli andmebaasides on andmesubjekti kohta kehtiv tagaotsimisteade või muu hoiatusteade. Pikem säilitamine on põhjendatud olukorras, kus teabevahetus konkreetse isiku kohta on kestva iseloomuga, näiteks kui kriminaalmenetlus kestab üle kahe aasta või kui õiguskaitseasutus esitab sama isiku kohta korduvalt teabetaotlusi. Kui õiguskaitseasutus uurib ohtlikku kurjategijat, kes on vabaduses, või kuritegeliku võrgustiku liikmeid ja toimimist, võivad õiguskaitseasutused vajada pidevat teabevahetust isikute liikumiste, viibimiste või suhtlusringkonna kohta, et koguda tõendeid ning planeerida edasisi tegevusi. Samuti võib pideva ja kahest aastast pikema teabevahetuse säilitamine koos isikuandmete säilitamisega olla põhjendatud selleks, et tuvastada tagaotsitava või teadmata kadunud isiku asukoht. Sellistel juhtudel on oluline, et kogu varasem teabevahetus oleks üheselt jälgitav ja kättesaadav, vältimaks töö dubleerimist, põhjendamatuid päringuid ning viivitusi teabe edastuses ja menetluses. Seejuures tuleb aga silmas pidada, et isegi kui on põhjendatud andmete säilitamine kauem kui kaks aastat, tuleb tagada, et iga kuue kuu tagant hinnataks nende andmete säilitamise vajalikkust ja kui isikuandmete säilitamise vajadus on ära langenud, siis need andmed kustutatakse töövoosüsteemist (täpsemalt kajastatud lõike 3 selgitustes).

Lõikega 3 nähakse ette, et ühtne kontaktpunkt hindab töövoosüsteemis teabevahetuse isikuandmete töötlemise jätkamise vajalikkust ja proportsionaalsust esimest korda kuue kuu

jooksul teabevahetuse lõppemisest arvates ning seejärel korrapäraselt vähemalt iga kuue kuu tagant. Iga hindamisetapi lõpetamisel kustutatakse need andmed, mille suhtes on ära langenud selle teabe töötlemise vajadus. Sättega võetakse üle Rootsi direktiivi artikli 16 lõige 4, mille järgi liikmesriik tagab, et tema ühtne kontaktpunkt vaatab esimest korda hiljemalt kuus kuud pärast teabevahetuse lõppu ja seejärel korrapäraselt üle, et juhtumite töövoosüsteem sisaldab isikuandmeid ainult seni, kuni see on vajalik ja proportsionaalne, et ühtne kontaktpunkt saaks täita talle Rootsi direktiiviga pandud ülesandeid, ning et selles sisalduvad isikuandmed kustutatakse seejärel jäädavalt.

Teabevahetuse lõppemine määratletakse seoses ülesannete täitmisega ühe teema, subjekti või objekti kohta. Teabevahetus loetakse lõppenuks, kui on täidetud kõik ülesanded, mis on seotud viimasena registreeritud sõnumiga. Kui ülesanded on täidetud, loetakse teabevahetus lõppenuks ning alates sellest hetkest hakkab ühtne kontaktpunkt hindama, kas isikuandmete töötlemine, sealhulgas nende säilitamine, on endiselt vajalik ja proportsionaalne.

Sätte eesmärk on tagada, et isikuandmete töötlemine oleks kooskõlas EL-i õigusnormidega, täpsemalt direktiiviga (EL) 2016/680, mis käsitleb isikuandmete kaitset õigus- ja õiguskaitse valdkonnas. Kõik isikuandmete töötlemise toimingud peavad olema vajalikud, proportsionaalsed ja kooskõlas kehtivate säilitamise tähtaegadega. Ühtne kontaktpunkt on kohustatud regulaarsete hindamiste käigus tagama, et isikuandmete töötlemine ei riku andmesubjektide õigusi ega suurenda nende kaitse riske. Konkreetsemalt tähendab see, et ühtne kontaktpunkt peab hindama, kas teabevahetuses sisalduvate isikuandmete säilitamine on jätkuvalt vajalik ja proportsionaalne, arvestades andmesubjektide õigusi. Kui isikuandmete töötlemise eesmärgid on täidetud ja säilitamise alused on kadunud, tuleb andmed viivitamata kustutada.

Hindamine peab toimuma hiljemalt kuue kuu jooksul pärast teabevahetuse lõppemist, mis tähendab, et ühtne kontaktpunkt peab vaatama läbi, kas andmete säilitamine on jätkuvalt õigustatud. Kui andmete säilitamise eesmärgid on saavutatud ja andmed ei ole enam vajalikud, tuleb need viivitamata kustutada. Kui andmete säilitamine on endiselt vajalik, määrab ühtne kontaktpunkt kui eelnõukohase PPVS § 25⁸ punkti 1 kohaselt KrMS 19. peatüki 8. jao 10. jaotises reguleeritud teabevahetuse korraldaja, uue tähtaja, mille jooksul tuleb andmete vajalikkust ja proportsionaalsust jätkuvalt hinnata.

Ühtse kontaktpunkti poolt andmete säilitamise vajaduse regulaarne hindamine tagab, et isikuandmeid ei töödelda kauem kui vajalik, ning et see on kooskõlas proportsionaalsuse ja eesmärgipärasuse põhimõtetega. Samuti aitab see tagada, et isikuandmete töötlemine vastab direktiivis (EL) 2016/680 kehtestatud säilitamise ja läbivaatamise tähtaegadele, pakkudes andmesubjektidele vajalikku kaitset.

Andmete usaldusväärsuse põhimõtte kohaselt tuleb ebaõiged, mittetäielikud või aegunud isikuandmed parandada, kustutada või nende töötlemist piirata ning teavitada sellest andmete vastuvõtjaid viivitamata. Seda põhimõtet küll PPVS-is ei sätestata (tuuakse välja PPVS § 25⁹ lõike 3 alusel kehtestatavas rakendusaktis), kuid on oluline rõhutada, et isikuandmed peavad olema täpsed, ajakohased ja õiged, et nende töötlemine oleks seaduslik ning eesmärgipärane.

Andmete täpsuse ja ajakohasuse nõue tähendab seda, et töödeldavad isikuandmed peavad olema tõesed ning täpsed. Kui selgub, et andmed on valed, mittetäielikud või aegunud, tuleb vastutaval töötlejal võtta viivitamata meetmeid nende parandamiseks või kustutamiseks. See välistab olukorra, kus valedele või aegunud andmetel põhinevad otsused võivad isikut kahjustada. Kui andmed on juba edastatud kolmandatele isikutele (näiteks teiste EL-i liikmesriigi õiguskaitseasutustele), tuleb neid teavitada muudatustest, tagamaks, et ka nende

käsituses olevad andmed oleksid täpsed ja ajakohased. See aitab vältida ebaõigete andmete levimist ja kasutamist. Kui andmete täpsuse või täielikkuse suhtes on kahtlusi, tuleb andmete töötlemine ajutiselt peatada või piirata, kuni probleem on lahendatud.

See põhimõte vastab IKS § 22 lõikele 2, millega sätestatakse, et isikuandmete töötlemisel peab vastutav töötleja tagama, et andmed oleksid täpsed, ajakohased ja usaldusväärsed. Kui isikuandmed osutuvad ebaõigeks või mittetäielikuks, tuleb need vastutava töötleja algatusel või andmesubjekti nõudel parandada või täiendada. Lisaks on oluline IKS § 27 lõige 1, sest selles nõutakse, et ebaõigete andmete töötlemise korral tuleb andmete töötlemine lõpetada või piirata ning võtta meetmed isiku õiguste kaitsmiseks.

Kuna töövoosüsteemis on sellised andmed, mis vastavad AvTS § 35 lõikele 1, tuleb need tunnistada asutusesiseseks kasutamiseks mõeldud teabeks. Andbesubjektide ja teiste isikute juurdepääsuõigust tuleb piirata näiteks jAvTS § 35 lõike 1 punktides 1 (kriminaalmenetluses kogutud teave, mis ei kuulu avaldamisele), 3 (teave, mille avalikuks tulek kahjustaks riigi välissuhtlust), 5¹ (teave uurimisasutuse tegevuse meetodite ja taktika kohta, kui selle avalikuks tulek võib raskendada süütegude avastamist või soodustada nende toimepanemist), 11 (teave süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist) ja 12 (isikuandmed, kui nendele juurdepääsu võimaldamine kahjustaks oluliselt andmesubjekti eraelu puutumast) sätestatud alusel. See tähendab järgmist:

1. **Juurdepääsupiirang:** andmetele on seatud piirangud, mis tähendab, et need andmed ei ole avalikkusele vabalt kättesaadavad. Neile pääseb ligi ainult kindlaksmääratud isikute ring, kellel on seaduslik alus ja vajadus nende andmetega tutvuda.
2. **Asutusesisene kasutamine:** andmed on määratud kasutamiseks ainult asjaomase asutuse sees. Need andmed on mõeldud üksnes asutuse töötajatele või ametnikele, kes vajavad neid oma tööülesannete täitmiseks. Sellise teabe edastamine väljapoole asutust on keelatud või rangelt piiratud.

Eelnõu § 3 punkti 3 kohaselt täiendatakse PPVS-i normitehnilist märkust viitega Rootsi direktiivile, et oleks selge, et PPVS-is võetakse üle teatavad Rootsi direktiivi sätted.

4. Eelnõu terminoloogia

Eelnõuga võetakse õigusaktides kasutusele uued terminid, nagu „ühtne kontaktpunkt“, „õiguskaitseasutus“, „teabevahetusluba“, „töövoosüsteem“, „otse juurdepääsetav teave“ ja „kaudselt juurdepääsetav teave“ ning „uurimisasutuse omaalgatuslik teabeedastus“. Uute terminite tähendust on selgitatud seletuskirjas konkreetsete sätete selgituste juures.

5. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu ei ole vastuolus EL-i õigusega. Eelnõuga viiakse KrMS-i ja PPVS-i regulatsioon vastavusse Rootsi direktiiviga ning KrMS-i täiendatakse viitega direktiivile 2023/2123. Direktiivide ülevõtmise kohta on seletuskirja lisades 1 ja 2 esitatud võrdlustabelid.

6. Seaduse mõjud

Direktiivi 2023/2123 ülevõtmisega mõjusid ei kaasne, mistõttu neid siin ei hinnata.

Rootsi direktiivi eelnõu menetlemisel koostas Euroopa Komisjon selle kohta mõjuanalüüsi⁷⁶. Eelnõu koostajad pidasid vajalikuks teatud mõjusid täiendavalt hinnata. Mõjuanalüüsis on valitud lähenemisviis, mille kohaselt kirjeldatakse valdkonna mõjusid tervikuna, pannes mõnevõrra suuremat rõhku muudatustele, mille suhtes on Rootsi direktiiv EL-i liikmesriikidele otsustusruumi jätnud või mis on olemuselt ulatuslikuma mõjuga. Arvestades muudatuste hulka, ei ole mõjuanalüüsis kajastatud väga väheste mõjuga muudatused.

Eelnõuga kavandatakse järgmisi suurema mõjuga muudatusi:

- 1) teabevahetuse tõhustamine, sealhulgas teabevahetuse tähtaja lühenemine, SIENA kasutamine ja isikuandmete kaitse tagamine;
- 2) ühtse kontaktpunkti senisest suurem roll teabevahetuse koordineerijana.

6.1. Kavandatav muudatus: teabevahetuse tõhustamine, sealhulgas SIENA kasutamine ja isikuandmete kaitse tagamine

Eelnõu kohaselt sätestatakse seaduse tasandil kuritegevust puudutava teabe kättesaadavuse ja sellele samaväärse juurdepääsu põhimõtte. Selle järgi vahetatakse teise EL-i liikmesriigi õiguskaitseasutuse ja Europoliga kuritegude avastamise, tõkestamise ja kriminaalmenetluse läbiviimise eesmärgil teavet samadel tingimustel ja ulatuses kui riigisisese teabevahetuse puhul. Selline teabevahetus peab toimuma ainult SIENA kaudu selleks, et tagada isikuandmete kaitse vastavalt EL-i õigusele.

Valdavas osas muudetakse seni EL-i liikmesriikide õiguskaitseasutuste vahelise teabe ja jälitusteabe vahetamist reguleerinud Rootsi raamotsuses sätestatud põhimõtted koos nende rakendamist reguleerinud mittekohustusliku iseloomuga operatiivkoostöö soovitude sätetega kohustuslikuks. Võrreldes kehtiva õigusega nähakse teabevahetuse tõhustamise eesmärgil suurima erinevusena ette teabe vahetamine muul alusel kui üksnes teabetaotlustele vastamine. Kui teave puudutab rasket kuritegevust, on Eesti uurimisasutustel kohustus edastada see teisele EL-i liikmesriigi õiguskaitseasutusele ja Europolile. Kui teave võib objektiivsetel põhjustel olla teise EL-i liikmesriigi õiguskaitseasutusele vajalik kuritegude tõkestamise, avastamise või uurimise eesmärgil, võib uurimisasutus selle edastada omal algatusel.

Muudatused loovad suurema õigusselguse, tõhustavad võitlust piiriülese kuritegevusega ning vähendavad praktikas ette tulevaid probleeme KrMS-i ja PPVS-i tõlgendamisel ja rakendamisel.

Mõju valdkond I: mõju siseturvalisusele

Mõju sihtrühm I: kõik Eestis elavad või viibivad isikud

Kriminaalteabe kiirem ja ulatuslikum vahetamine mõjutab positiivselt kõiki Eestis elavaid isikuid. Sihtrühm I hõlmab kõiki Eesti alalisi elanikke ehk 1,37 miljonit inimest ning Eestis ajutiselt viibivaid isikuid, kelle hulk on ajas muutuv ja ei ole teada.⁷⁷

Positiivne mõju sihtrühmale väljendub selles, et raskete kuritegude toimepanijate kiirem ja tõhusam tuvastamine pärsib kuritegevust. Kurjategijad ei ole huvitatud õiguskaitse huviorbiiti

⁷⁶ Euroopa Komisjoni koostatud esialgne mõjuanalüüs (ei sisalda hiljem EL-i nõukogu töörühmas tehtud muudatusi), punkt 3. Kättesaadav: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021SC0374>.

⁷⁷ Statistikaamet. Rahvaarv Eestis 2024. aasta alguse seisuga. Kättesaadav: <https://www.stat.ee/et/avasta-statistikat/valdkonnad/rahvastik/rahvaarv>.

sattumisest, veel vähem uurimisasutuste sekkumisest nende tegevusse, mistõttu hoidutakse tegutsemast piirkondades, kus selliste riskide realiseerumise tõenäosus on suur.

Samuti avaldab sihtrühmale I positiivset mõju see, et uurimisasutustel tekib võimalus enda piiratud ressursse tõhusamalt kasutada. Ulatuslikum juurdepääs kriminaalteabele annab parema ülevaate riiki mõjutavast kuritegevusest ning võimaldab sellest tulenevatele ohtudele mõjusamalt ja eelistatult proaktiivselt reageerida. Operatiivsem teabevahetus hõlbustab uurimisasutuste kiiremat sekkumist, tõendite kogumist ja optimeeritumat menetlust kohtueelses etapis. Kuna teabevahetuse tulemusena muutub tõhusamaks eeskätt raske kuritegevuse vastane võitlus, saab efektiivsuse arvelt vabanevat ressursi kasutada enam sellise kuritegevuse ennetamisel, tõkestamisel, avastamisel ja menetlemisel, mis kehtivas kuritegevuse vastaste prioriteetide loetelus⁷⁸ ei sisaldu, ent mille menetlemisega tuleb KrMS §-s 6 sätestatud legaliteedipõhimõtte kohaselt ja avalikkuse turvatunnet silmas pidades tegeleda.

Mõju ulatus sihtrühmale on väike, kuna muutusi Eesti elanikkonna kui terviku käitumises ei toimu ning puudub tarvidus nendega kohanemiseks. Tulenevalt sellest, et valdav osa Eestit puudutavast raskest kuritegevusest on latentne ehk varjatud (narkokaubandus, käibemaksupettused, rahapesu, inimkaubandus, laste seksuaalne ärakasutamine internetis) ning selle tagajärjed avalduvad kaudselt, ei taju avalikkus selle olemasolu ega tunnetata vahetult selles positiivseid ega negatiivseid muutusi. Sellele osale Eesti elanikkonnast, kes on seotud raskete kuritegude toimepanemisega, avaldab muudatus suurt negatiivset mõju, kuna alamsihtrühma senine toimimine muutub tõenäoliselt märkimisväärselt selleks, et neile avalduva mõju negatiivsetest tagajärgedest hoiduda. Alamsihtrühma puhul eeldab nende suunatud negatiivsest mõjust hoidumine sihiteadlikku kohanemist, mis ongi muudatuse eesmärk.

Mõju avaldumise sagedus on väike, kuna valdav osa elanikkonnast ei ole raskest kuritegevusest vahetult mõjutatud või vähemalt selle mõjust teadlikud ega taju vahetult mõjusid, mis kõnesoleva teabevahetuse tõhustamisega kaasnevad. Mõju avaldumine valdavale osale elanikkonnast on ebaregulaarne, juhuslik ja harv, väljendudes eeskätt meedias avaldatud uurimisasutuste töövõitudest teadasaamises ning nende pinnalt pikema perioodi vältel siseturvalisuse olukorra suhtes tunnetuse kujunemises, mida kajastavad näiteks avaliku arvamuse uuringud⁷⁹.

Järeldus mõju olulisuse kohta sihtrühmale I: mõju sihtrühmale on enamasti kaudne.

Mõju sihtrühmale II: PPA, KAPO, MTA, Konkurentsiamet, Sõjaväepolitsei, Keskkonnaamet ning Justiits- ja Digiministeeriumi vanglate osakond ja vangla, prokuratuur, kohus

Sihtrühma II moodustavad eelkõige uurimisasutuste ametnikud, kes tegelevad kriminaalasjade kohtueelse menetlemisega. Kõige suurem osa uurijatest, keda kavandatakse muudatused mõjutada võivad, kuuluvad Siseministeeriumi valitsemisalasse. Sihtrühma põhiosa suurust on raske hinnata, sest teave PPA, KAPO, MTA, Konkurentsiameti, Sõjaväepolitsei, Keskkonnaameti ning Justiits- ja Digiministeeriumi vanglate osakonna ja vangla kriminaalmenetlusi läbiviivate üksuste isikkoosseisu kohta ei ole avalik. Juurdepääs vastavatele andmetele on juurdepääsupiiranguga, sest muu hulgas kohaldatakse PPVS § 4 lõiget 5, mis välistab teabe avaldamise kriminaalpolitsei struktuuri ja isikkoosseisu kohta, ning AvTS § 35 lõike 1 punkti 12, mis välistab isikuandmete avaldamise, kui sellisele teabele juurdepääsu

⁷⁸ Justiitsministeerium. 04.10.2023 justiitsministri ja siseministri kinnitatud õiguskaitse prioriteedid. Kättesaadav: <https://www.just.ee/kuritegevus-ja-selle-ennetus/oiguskaitse-prioriteedid>.

⁷⁹ Näiteks Siseministeeriumi siseturvalisuse uuringutes, mis on kättesaadavad aastate kaupa: <https://siseministeerium.ee/ministeerium-ja-kontaktid/ministeerium-ja-minister/uuringud-ja-analuusid#avaliku-korra-tagami>.

võimaldamine kahjustaks oluliselt andmesubjekti eraelu puutumatust, ja AvTS § 35 lõike 1 punkti 19, mis välistab seaduses sätestatud muu teabe avaldamise.

Samuti kuuluvad sihtrühma kokku kuni 195 prokuröri⁸⁰ Riigiprokuratuurist ja Põhja, Lõuna, Lääne, Ida ning Majandus- ja Korruptsioonikuritegude ringkonnaprokuratuurist, kes otsustavad käimasolevas kriminaalmenetluses kohtueelsete andmete avaldamise.

Kavandatavad muudatused võivad mõnevõrra puudutada ka kohtunikke, eeskätt nelja esimese astme kohtu – Harju Maakohus, Tartu Maakohus, Pärnu Maakohus ja Viru Maakohus – kohtunikke, kes tegelevad kriminaalasjade lahendamise. Teabetaotlustega seoses võib tekkida vajadus lahendada kohtute pädevusse kuuluvaid taotlusi, kuid eelnõu koostajad peavad seda vähetõenäoliseks, sest üldjuhul on kohtupidamine ning kohtuotsuse kuulutamine avalikud. Kohtuistung või selle osa võib kuulutada kinniseks ainult kaalukal vajadusel kohus seaduses ettenähtud juhtudel, näiteks KrMS § 12 alusel perekonna- ja eraelu kaitseks või alaealise või kannatanu huvides.

Schengeni ala on kogu maailmas suurim vaba reisimise ala, mis võimaldab 420 miljoni inimese vaba liikumist ning takistuse kauba- ja teenustevoogusid. Schengeni alal peaks ühe EL-i liikmesriigi politseiametnikel olema EL-i ja riigisisese õiguse alusel võimalus saada samaväärne juurdepääs teabele, mis on kättesaadav nende kolleegidele teises EL-i liikmesriigis. Turvalisuse tagamiseks peaks õiguskaitseasutuste koostöö olema EL-is tulemuslik ja tavapärane. Seetõttu on Schengeni alal, kus ollakse üksteisest vastastikku sõltuvad, avaliku julgeoleku aluseks olevate meetmete oluline osa politseikoostöö õiguskaitse eesmärkidel asjakohase teabe vahetamisel.

Kohustus vahetada rasket kuritegevust puudutavat teavet teiste EL-i liikmesriikide õiguskaitseasutuse ja Europoliga ning võimalus vahetada asjakohast kriminaalteavet nendega omal algatusel, kasvatab oluliselt vahetatava kriminaalteabe mahtu. Uuele teabele juurdepääs suurendab uurimisasutuste teadlikkust kuritegevuse hetkeolukorrast ja trendidest ning kuritegelikest võrgustikest ja nende tegutsemisviisidest (*modus operandi*), aga ka nende teises riigis asuvast varast. Eeltoodu võimaldab uurimisasutustel kuritegevusega seotud ohte paremini ennetada ja nende vastu võidelda. Uurimisasutustele tekib teabevahetuse suurenemisel võimalus analüüsida enam andmeid ja koostada põhjalikumaid analüüse, mille tulemusel on võimalik rakendada piiratud ressursse sihistatumalt, nii ohtude tõrjumisel kui ka kriminaalmenetluste läbiviimisel.

Kriminaalmenetluse tõhustamise aspektist omab olulist tähendust teabe senisest selgem, mugavam ja kiirem vahetamine. Selgete reeglite kehtestamine muudab rahvusvahelise teabevahetuse uurimisasutuse eesliiniametnikele kasutajasõbralikumaks. Võib eeldada, et suureneb uurimisasutuste ametnike teadlikkus sellest, millal ja millist teavet teiste riikide kolleegidega vahetama peaks. Teadmine, et teabevahetus fikseeritakse, teabe adressaatide ring ja kasutamine on kontrollitavad ning teabe vahetamise ja kasutamise üle teostatakse järelevalvet nii riigisisel kui ka EL-i tasandil, peaks maandama praktikas sageli esinevaid kahtlusi, et teabe teisele riigile kättesaadavaks tegemine on allika turvalisust või käimasoleva menetluse edukust silmas pidades niivõrd riskantne, et sellest tuleks hoiduda. Ehkki SIENA kasutamise peamine mõju sihtrühm on isikud, keda teabetaotlused puudutavad, mõjutab see oluliselt ka kohut, prokuratuuri ja uurimisasutusi, kuna nende usaldusväärsus ja maine võivad kannatada, kui allikad paljastuvad. Ehkki teabe adressaatide ringi suurenemisel kasvab andmelekkete oht, on

⁸⁰ Prokuratuur. Juhtkond ja personal. Kättesaadav:

<https://www.prokuratuur.ee/prokuratuurist/prokuratuur/asutuse-struktuur#personal>.

teabe edastamine SIENA kaudu palju turvalisem kui näiteks telefonitsi või e-kirja teel. Sidekanalite puhul, mida eesliiniametnikud praegu enamjaolt kasutavad, on hiljem pea võimatu tuvastada ja tõendada, kas teabevahetus leidis aset⁸¹, millist teavet vahetati ja kellega ning kellele seda jagati. Tuleb toonitada, et isegi kui suudetakse kindlaks teha potentsiaalne teabe saajate ring, ei ole see piisav andmelekke põhjustaja vastutusele võtmiseks.

Mugavus vahetada teavet ühtse kontaktpunkti kaudu peaks innustama teabevahetuses osalema ametnikke, kellel on näiteks kasin nõutava keele oskus või vähene kokkupuude rahvusvahelise teabevahetusega. Samuti peaks eelkirjeldatud ametnikke ärgitama teavet vahetama SIENA masintõlke võimekus, mille tõttu on ka kasina võõrkeeleoskuse puhul võimalik eestikeelne teave tõlkida hõlpsasti inglise keelde, muus keeles SIENA-sse sisestatud teave inglise keelde ning sellest omakorda eesti keelde. Ametnikele, kelle töövaldkonnas on tihe teabevahetus tavapärane, luuakse mugav võimalus vahetada teavet kiirelt ja ise ning pidada teabevahetuse üle järke.

Uurimisasutuste töö muudab mugavamaks ja kiiremaks võimalus esitada menetluse raames vajalike asjaolude väljaselgitamiseks lihtne ja kiire teabetaotlus. Ehkki taotluse alusel vastuseks saadav teave ei ole reeglina tõendina kasutatav, saab selle teabe alusel otsustada, kas esitada EIO või mitte. Lisaks on teabetaotluse puhul EIO-ga võrreldes oluliselt lihtsam kõrvaldada taotluses puudusi või esitada täpsustusi või selgitusi. Kuna teabetaotluse koostamine ja esitamine on vähem ajamahukas kui EIO puhul, võimaldab see saada vastust kiiremini.

Teabevahetuse positiivne mõju prokuratuurile seisneb kohtueelse menetluse aja lühenemises menetlustes, milles Eesti on teiselt EL-i liikmesriigilt teavet taotlenud. Samuti paraneb süüdistuse kvaliteet, kuna prokuratuuril on eelduslikult rohkem teavet, millele tugineda näiteks jälitustoimingute taotlemisel, või teadmine, kas ja kustkohast on sellist teavet võimalik ja mõistlik küsida. Teadmine, kas või millisesse riiki on lisateabe saamiseks EIO koostamine mõistlik, hoiab kokku prokuröride ressursi, mis kuluks tarbetute või menetluse vaates vähese kasuteguriga EIO-de koostamisele ja nende vastuste ootamisele. Menetluse juhtimisel on rohkemate andmete pinnalt parem seada prioriteete nii menetletavate kuritegude järjekorra kui ka menetlussihtmärkide osas. Prokuratuurile võib EL-i liikmesriikidega teabevahetuse tihenemine tuua negatiivse aspektina kaasa mõningase töökoormuse kasvu. Töökoormuse kasv seisneb eeskätt selles, et kui Eestile laekuv teabetaotlus puudutab käimasoleva kriminaalmenetlusega seotud andmeid, peab vastavat kriminaalasja lahendav prokurör kui menetluse juht langetama KrMS § 214 lõike 1 järgi otsuse andmete avaldamise lubatavuse kohta. Selliste taotluste lahendamine ei põhjusta prokuröridele tõenäoliselt erilist ajakulu, sest see taotlus on riigisiseses praktikas vormivaba ja seisneb sageli telefonitsi kinnituse andmises. Silmas tuleb aga pidada, et andmete avaldamise taotlused võivad laekuda ööpäev läbi.

Kohtute tööle avaldab direktiivikohane teabevahetus positiivset mõju, võimaldades teatavatel juhtudel teha otsuseid, eeskätt jälitustoimingute lubatavuse kohta, rohkema teabe alusel. Erandlikes olukordades, kus kohtul on vaja saada uurimisasutuse kaudu teavet mõnest teisest EL-i liikmesriigist, kulub sellise teabe saamiseks vähem aega. Teabevahetusega kohtute tööle kaasnevat negatiivset mõju on keeruline hinnata, kuna teabevahetus mõjutab siiski peamiselt uurimisasutuste ja prokuratuuri tööd. Võib eeldada, et vähene negatiivne mõju tekib

⁸¹ Selgitus: õiguskaitseasutuste vahelise teabevahetuse asetleidmise fakti taasesitamise võimalus võib omada teatavatel juhtudel tähendust ka uurimisasutuse tegevuste õiguspärasuse hindamisel. Näiteks olukorras, kus teabevahetuse raames saadud teabele tuginedes on läbi viidud menetlustoiminguid, eeskätt isik kahtlustatavana kinni peetud, teostatud läbiotsimisi või jälitustoiminguid. Kui uurimisasutus ei suuda tõendada muul viisil kui ühepoolselt ja paljasõnaliselt, et nimetatud toimingute tegemise aluseks oli vastav kiireloomuline teave – eriti olukorras, kus isiku suhtes tõusetunud kahtlus ei ole leidnud kinnitust –, satub kahtluse alla uurimisasutuse tegevuse legaalsus.

olukordades, kus teabetaotlusele vastamiseks on vaja töövälisel ajal kohtu luba. Nagu varem korduvalt selgitatud, on selline vajadus äärmiselt erandlik, sest reeglina on kohtupidamine ja kohtuotsuse kuulutamine avalikud. Kohtute pädevusse peaks teabetaotlustele vastamise üle otsustamine langema vaid siis, kui teisele EL-i liikmesriigile avaldamiseks taotletav teave puudutab kinniseks kuulutatud kohtumenetluse andmeid. Veel erandlikum on olukord, kus selliste erandlike andmete avaldamise luba küsitakse töövälisel ajal, sest tegemist peab olema äärmiselt kiireloomulist sekkumist nõudva vajadusega.

Arvestades eeltoodut, võib kaasneva mõju ulatuse sihtrühmale II hinnata tervikuna keskmiseks, sest sihtrühma käitumises võivad kaasneda muutused, kuid nendega ei kaasne eeldatavalt kohanemiskursi.

Mõju avaldumise sagedus on sihtrühma II kuuluvate asutuste lõikes ilmselt erinev, sest näiteks ühtne kontaktpunkt tegeleb teabevahetusega igapäevaselt, kuid mõnda uurimisasutust, kes rahvusvaheliselt teavet nii palju ei vaheta, võivad kavandavad muudatused puudutada harva. Kogu sihtrühma II suhtes võib kavandatavate muudatuste mõju sageduse hinnata keskmiseks, arvestades, et kokkupuude on regulaarne või reeglipärane, aga mitte igapäevane.

Järeldus mõju olulisuse kohta sihtrühmale II. Kavandatavad muudatused avaldavad positiivset mõju siseturvalisusele. Eesmärkide realiseerumisel tiheneb koostöö naaberriikide õiguskaitseasutustega, avanevad uued võimalused koostööks ning täienevad meetmed võitluseks kuritegevusega. Kui politseiametnikele antakse digitaalseid vahendeid juurde, mis avaldavad otsest ja vahetut kasu operatiivtasandile, suureneb kindlasti siseturvalisuse pakkumine. See tähendab, et riigi suutlikkus tagada oma elanike turvalisus ja õiguskord paraneb. Kui politseiametnikud saavad kasutada uusi digitaalseid töövahendeid, mis muudavad nende töö operatiivtasandil tõhusamaks, vabanevad ressursid ja aeg, mida saab kasutada teiste oluliste ülesannete täitmiseks. See tähendab, et politsei suudab kiiremini ja tulemuslikumalt reageerida kuritegudele, lahendada keerulisi juhtumeid, ennetada õigusrikkumisi ning pakkuda paremat kaitset avalikule korrale ja julgeolekule. Nii kasvab üldine turvatunne ning paraneb riigi võimekus hoida korda ja kaitsta kodanike õigusi.

Mõju valdkond II: mõju riigiasutuste töökorraldusele

Mõju sihtrühm: PPA, KAPO, MTA, Konkurentsiamet, Sõjaväepolitsei, Keskkonnaamet ning Justiits- ja Digiministeeriumi vanglate osakond ja vangla

Põhilised teabevahetuse tõhustamisega kaasnevad mõjud uurimisasutuste töökorraldusele seisnevad SIENA-ga otseühenduse loomises ning ööpäev läbi teabevahetusvõimekuse tagamises.

Ehkki on ilmne, et juurdepääs aitab kasutada tõhusamalt piiratud ressursse ja võidelda kuritegevuse vastu, sõltub nende võimaluste realiseerumine aktiivsest osalemisest teabevahetuses. Selleks et uurimisasutuste ametnikud saaksid teabevahetuses aktiivselt osaleda, tuleb neile tagada otsene juurdepääs SIENA-le ka eesliinitasandil. Seejuures ei tähenda otsene juurdepääs, et igal kriminaalasju menetleval ametnikul oleks igal ajahetkel võimalik SIENA-sse pääseda oma nutiseadme kaudu. Pigem on oluline, et sideskeem oleks võimalikult lühike ja selge, tagamaks kiire teabevahetuse. Optimaalseks lahenduseks võiks olla SIENA otseühenduse loomine uurimisasutuse sisese kontaktpunkti ja nende struktuuriüksustega (nt regionaalsed üksused), millel on sagedane kokkupuude rahvusvahelise teabevahetusega. Kuna SIENA-sse pääsemine on võimalik näiteks politseivõrgus töötava sülearvuti kaudu, võiks uurimisasutustele võimaldada juurdepääsu PPA kaudu. Selline lahendus ei tooks uurimisasutustele kaasa märkimisväärsed lisakulusid. Siiski on vajalik sõlmida asutustevahelised kokkulepped

politseivõrgus töötavate seadmete kasutamiseks. Kavandatud muudatus tekitab teatavat lühiajalist töökoormuse kasvu nii PPA-le kui ka uurimisasutustele, kuna vastavate lepingute koostamine ja sõlmimine nõuab lisatööd. Siiski ei ole see mõju pikaajaline.

Suurem negatiivne mõju uurimisasutuste töökorraldusele tuleneb kohustusest tagada operatiivses teabevahetuses osalemise võimekus ööpäev läbi. Ühtsel kontaktpunktil ei ole juurdepääsu kõikidele uurimisasutuste kasutuses olevatele andmebaasidele. Seetõttu ei ole võimalik tagada KrMS §-s 508⁹² sätestatud tähtaegade järgimist siis, kui uurimisasutuste võimekus teavet vahetada piirneb vaid tavapärase tööajaga. Kuna teabevahetuse vajadus on uurimisasutuste lõikes erinev ning mõnel uurimisasutusel pigem vähene, ei ole mõttekas uurimisasutustel luua selle jaoks eraldi üksust. Tõenäoliselt on optimaalne tagada ööpäev läbi teabevahetuse võimekus seeläbi, et uurimisasutuste siseselt määratakse enda n-ö kontaktpunkt või teabevahetuses osalevate ametnike ring, kellel on juurdepääs asjakohasele teabele ning kelle võimekus seda ööpäev läbi vahetada tagatakse valveaja kehtestamisega. Arvestades, et muudatuse sihtrühma moodustavad uurimisasutused, kes on kuriteoasjaolude ilmnemisel kohustatud menetlust alustama, peavad nad operatiivse reageerimise tagama ööpäev läbi ka praegu. Asjaolu, et teatavatel uurimisasutustel ei realiseeru ööpäevaringse reageerimise vajadus nende pädevusest tulenevalt sageli, ei too see kaasa olulisi muudatusi nende kohustustes ja seega senises töökorralduses. Uurimisasutustele, kes peavad igapäevaselt sageli ööpäev läbi sündmustele reageerima, ei too käesolev muudatus kaasa muid muudatusi senises töökorralduses kui konkreetsetest teabevahetustähtaegadest lähtumine ning kindla sidekanali kasutamine.

Järeldus mõju olulisuse kohta. Muudatuse mõju sagedus ja ulatus sihtrühmale on keskmised. Sihtrühmale avaldub üldjoontes positiivne mõju. Muudatused tugevdavad sihtrühma võimekust osaleda rahvusvahelises koostöös ning toetavad tõhusamat kuritegevusevastast tegutsemist, võimaldades kiiremat ja struktureeritumat teabevahetust SIENA kaudu. Lühiajalises plaanis toob muudatus siiski kaasa mõõduka töökoormuse kasvu, mis on seotud tehniliste ja juriidiliste eelduste (nt juurdepääsuprotokollide ja andmetöötluslepingute) loomisega ning vajadusega tagada ööpäevaringne reageerimisvõimekus. Kuna paljudel uurimisasutustel on juba praegu kohustus reageerida operatiivselt ööpäev läbi, ei tähenda see enamikule olulist muutust senises töökorralduses.

Kokkuvõttes on muudatuse mõju sihtrühmale positiivne, kuna see suurendab töö tõhusust ja õiguskaitseüsteemi üldist toimivust, ent eeldab asutustelt mõõdukat, kuid hallatavat kohandumist uute korralduslike nõuetega.

Mõju valdkond III: mõju majandusele

Mõju sihtrühm: Eestis tegutsevad ettevõtted

Nagu on selgitatud mõjuvaldkonna I (mõju siseturvalisusele) juures, toetab kavandatav muudatus tõhusamat rahvusvahelist koostööd ja info liikumist õiguskaitseasutuste vahel. See avaldab positiivset mõju mitte üksnes elanikkonna turvatundele, vaid ka Eestis tegutsevatele ettevõtjatele, keda Statistikaameti andmetel oli 2024. aastal Eestis 158 378 (majanduslikult aktiivset ettevõtet)⁸², ja majanduskeskkonnale laiemalt.

Kuritegevuse mõju majandusele on oluline ja sageli alahinnatud – see pärsib ausat ettevõtlust, kahjustab investeerimiskeskonda ning suurendab äririske. Organiseeritud kuritegevus

⁸² Statistikaamet, ER025: statistilisse profiili kuuluvad ettevõtted aasta ning tegevusala (EMTAK 2008). – https://andmed.stat.ee/et/stat/majandus_majandusüksused_ettevetjad/ER025/table/tableViewLayout2.

tegutseb süsteemselt ja rahvusvaheliselt, mõjutades kõiki EL-i liikmesriike, sealhulgas Eestit. 2019. aastal hinnati organiseeritud kuritegevuse tekitatud kahju Euroopa Liidu majandusele ligikaudu 139 miljardile eurole, mis moodustab ligikaudu 1% EL-i SKP-st. See summa pärineb peamiselt ebaseaduslikest tegevustest, nagu uimasti- ja inimkaubandus, finantskuriteod, pettused ning rahapesu – valdkonnad, mis kahjustavad otseselt ka ausalt tegutsevaid ettevõtteid.

Eesti ettevõtjad puutuvad kuritegevuse mõjudega kokku näiteks olukordades, kus konkureeritakse ebaausate turuosalistega, kes kasutavad kriminaaltulu legaalse äritegevuse kattevarjuna. Samuti võivad ettevõtted sattuda pettuste, küberkuritegude või rahapesuskeemide sihtmärkiks. Uimasti- ja inimkaubandusega seotud tegevused võivad mõjutada töajouturgu, sotsiaalset stabiilsust ning tekitada varjatud kulusid ka ettevõtlusele.

Kavandatavad muudatused – eelkõige teabe kiirem ja täpsem liikumine EL-i liikmesriikide õiguskaitseasutuste vahel – toetavad kuritegude kiiremat avastamist ja menetlemist. See omakorda vähendab kriminaaltulu teenimise võimalusi ning tugevdab ausa konkurentsi ja läbipaistvuse aluseid. Tugev ja tõhus õiguskaitseüsteem suurendab usaldusväarsust ning muudab Eesti majanduskeskkonna stabiilsemaks ja atraktiivsemaks, mis on otseselt kasulik ka ettevõtjatele.

Eesti ettevõtetele tähendab see eelkõige riski vähenemist sattuda pettuste või muude majanduskuritegude ohvriks. Samuti kahaneb tõenäosus, et ettevõtlusruumi hõivavad ebaseadusliku kapitali toel tegutsevad turuosaliselised, mis loob võrdsemad konkurentsitingimused ning soodustab ausat ettevõtlust.

Lõppkokkuvõttes aitavad muudatused luua õiglasemat ja turvalisemat ärikeskkonda, kus aus ettevõtlus saab areneda ilma, et seda ohustaks organiseeritud kuritegevuse varjatud mõju.

Järeldus mõju olulisuse kohta. Kavandatavate muudatuste mõju sagedus ja ulatus sihtrühmale on vähenenud, kuid nende mõju iseloom on selgelt positiivne ja toetab majanduskeskkonna tugevnemist. Muudatusega ei kaasne negatiivseid mõjusid, mistõttu hinnatakse mõju ebaoluliseks, kuid suunalt kasulikuks ja soovitavaks.

6.2. Kavandatav muudatus II: ühtse kontaktpunkti senisest suurem roll teabevahetuse koordineerijana

Muudatusega tugevdatakse ühtse kontaktpunkti rolli rahvusvahelise teabevahetuse koordineerijana selleks, et tagada teabevahetuse nõuetekohasus, sujuvus, kiirus ja korralduse selgus. Sellega seoses sätestatakse:

- uurimisasutusele kohustus edastada teabevahetuse koopia alati ühtsele kontaktpunktile;
- ühtse kontaktpunkti kohustus koguda Eestit puudutava teabevahetuse kohta statistikat;
- ühtse kontaktpunkti kohustus täita iga aasta aruandluskohustust Euroopa Komisjoni ees.

Mõju valdkond I: mõju siseturvalisusele

Mõju sihtrühm I: PPA kui ühtne kontaktpunkt

Mõju sihtrühm II: PPA, KAPO, MTA, Konkurentsiamet, Sõjaväepolitsei, Keskkonnaamet ning Justiits- ja Digiministeeriumi vanglate osakond ja vangla

Sihtrühmale I ei ole kavandatavate muudatustega lisanduvad ülesanded uued. PPA on KrMS § 508⁷⁸ lõike 3 kohaselt EL-i liikmesriikidega teabevahetuse keskasutus ka praegu. Kuna KrMS

§ 508⁷⁸ lõike 2 kohaselt osalevad teabevahetuses vaid KrMS § 126² lõikes 1 nimetatud jälitusasutused ehk PPA, KAPO, MTA, Sõjaväepolitsei ning Justiits- ja Digiministeeriumi vanglate osakond ja vangla, on PPA-l tulnud seni korraldada üksnes jälitusasutuste teabevahetust. See tähendab, et teavet on vahetatud kavandatavate muudatustega võrreldes väiksemas mahu. Tulenevalt sellest, et suureneb teabevahetuses osalejate ring ja vahetatava teabe ulatus, aga ka sellest, et teatava teabe vahetamine muutub kohustuslikuks, tekib riigiülesest kõikehõlmav vaade kuritegevuse hetkeolukorrast ja trendidest ning suureneb uurimisasutuste kohalolu rahvusvahelise kuritegevuse vastase võitluse areenil. See suurendab EL-is, eeskätt aga Balti- ja Põhjamaades, Eesti riigi ja uurimisasutuste nähtavust usaldusväärse partnerina.

Sihtrühma I suurem roll teabevahetuse koordineerijana on siseturvalisuse seisukohalt väga oluline, eriti kui Prüm II andmevahetus 2027. aastaks täies mahu rakendub. Prüm II raames toimub automaatne andmevahetus riikide vahel, hõlmates DNA-profiile, sõrmejälgi, sõidukite registreerimisandmeid, näokujutisi ja politseiregistrite andmeid, mis on kogutud riigisisest süütegude menetlemise eesmärgil. See loob uurimisasutustele võimaluse lahendada kriminaalasju kiiremini ja tõhusamalt, kuna automaatsed andmevõrdlused aitavad kiiremini tuvastada kokkulangevusi. Kui süsteem tuvastab kokkulangevuse ühe riigi andmebaasiga, on isikustatud andmete saamiseks vaja esitada teabetaotlus vastava riigi ühtsele kontaktpunktile. See tähendab, et igas riigis peab olema koordineeriv asutus, mis suudab kiiresti ja tõhusalt vastata teabetaotlustele ning edastada vajaliku teabe. Kuna kõigil uurimisasutustel ei ole seni olnud kogemust selliste teabetaotluste koostamisel ja esitamisel, on ühtse kontaktpunkti rolli suurendamine hädavajalik, et tagada süsteemi sujuv ja tõhus toimimine.

Ühtne kontaktpunkt toimib omamoodi vahendajana, aidates uurimisasutustel Prüm II raames toimuvat andmevahetust paremini kasutada. See tagab mitte ainult kiirema juurdepääsu olulisele teabele, vaid aitab ka vähendada sihtrühmade I ja II halduskoormust ning võimalikku segadust, mis võiks tekkida otse suhtlemisel eri riikide andmebaaside haldajatega. Seega aitab ühtse kontaktpunkti tugevdamine saavutada Prüm II eesmäärke ning parandada rahvusvahelist koostööd ja siseturvalisust.

Sihtrühm II vahetab teavet ka teiste EL-i liikmesriikidega juba praegu. Ehkki muudatuse tulemusena suureneb tõenäoliselt teabevahetuse maht ja saab kohustuslikuks konkreetse teabevahetuskanali kasutamine, ei mõjuta see sihtrühma II tööd oluliselt, sest teabevahetuse korraldamise kohustus on sihtrühmal I (sh näiteks teabe tõlkimine). Eeltoodust tulenevalt on muudatuse mõju sagedus ja ulatus sihtrühmale II keskmine ning positiivne.

Mõju sihtrühmale II sõltub suuresti iga uurimisasutuse spetsiifikast ja kokkupuutest rahvusvahelise kriminaalkoostööga. Asutuste puhul, kellel on sagedane vajadus rahvusvahelise teabevahetuse järele (nt PPA, KAPO, MTA), on mõju sage ja suure ulatusega. Teistel uurimisasutustel (nt Keskkonnaamet või vangla) võib mõju olla harvem, kuid strateegiliselt siiski oluline.

Prüm II rakendumine toob kaasa vajaduse kiireks reageerimiseks ja teabetaotluste esitamiseks, mis tähendab, et uurimisasutused peavad kohandama oma sisemist töökorraldust – sealhulgas määrama pädevad kontaktisikud, looma ligipääsu SIENA-le ning tagama ööpäevaringse reageerimisvõimekuse. Kuigi see ei too alati kaasa olulist lisakoormust (paljud uurimisasutused juba tagavad ööpäevaringse reageerimisvõimekuse), võib siiski oodata mõningast töömahu kasvu ning vajadust täiendava koolituse ja tehnilise toe järele.

Järeldus mõju olulisuse kohta. Kuna PPA roll ühtse kontaktpunktina laieneb ning hõlmab edaspidi lisaks jälitusasutustele ka teisi uurimisasutusi, on mõju sihtrühmale I pidev ja igapäevane.

Mõju valdkond II: mõju riigiasutuste töökorraldusele

Mõju sihtrühm I: PPA uurimisasutusena, KAPO, MTA, Konkurentsiamet, Sõjaväepolitsei, Keskkonnaamet ning Justiits- ja Digiministeeriumi vanglate osakond ja vangla

Sihtrühma moodustavad uurimisasutused, kes tegelevad kriminaalasjade kohtueelse menetlemisega. Muudatuse põhiline mõju tuleneb kohustusest vahetada SIENA kaudu teavet teiste EL-i liikmesriikide õiguskaitseasutuste ja Europoliga. Muudatuse tulemusena peavad uurimisasutused tagama võimekuse edastada, võtta vastu ja vastata ööpäev läbi teistelt EL-i liikmesriikidelt saabunud teabetaotlustele. Juba praegu kasutab osa uurimisasutusi – PPA, KAPO ja MTA – SIENA-t teabevahetuseks igapäevaselt. Nendele uurimisasutustele, kes praegu SIENA-ga ühendatud ei ole, rakendub SIENA kasutamise kohustus 2027. aasta 12. juunist.

Muudatus toob kõikidele uurimisasutustele kaasa täiendava ametnike koolitamise vajaduse. Tuleb tagada, et ametnikud on teadlikud nii kohustusest kui ka võimalusest vahetada teavet ning täidavad õigesti seaduse nõudeid.

Teabevahetuses osalemine ööpäev läbi võib nõuda uurimisasutustelt töökorralduse kohandamist. Arvestades uurimisasutuste seniseid teabevahetuse mahte ja asjaolu, et ühtne kontaktpunkt töötab juba praegu ööpäev läbi, jälgib kõiki sissetulevaid teabetaotlusi, vastab neile ise või edastab need vastamiseks pädevale uurimisasutusele, ei ole vajalikud muudatused uurimisasutuste töökorraldusele ulatuslikud. Peamine töökorralduse muutus seisneb valveaja kehtestamises ametnikele, kes suhtlevad ühtse kontaktpunktiga asutuse nimel. Praeguste tehniliste võimaluste juures tähendab ööpäevaringne juurdepääs SIENA-le ligipääsu politseivõrgus töötavale sülearvutile. See tähendab, et eraldi ööpäevaringse töögraafikuga üksust ei ole vaja luua. Piisab sellest, kui uurimisasutus on funktsionaalselt kättesaadav ehk suudab kiiresti reageerida kontaktpunkti pöördumistele ja vastata neile ettenähtud tähtaegade jooksul. Uurimisasutus ja ühtne kontaktpunkt peavad omavahel kokku leppima täpses töökorralduses. Väiksema koosseisuga uurimisasutuste puhul võib ööpäevaringse teabevahetusvõimekuse tagamine tähendada, et määratud ametnik on valveajal kättesaadav telefonitsi ning omab juurdepääsu SIENA-le ja muudele tööks vajalikele andmebaasidele mobiilseadme kaudu. Sellise korraldusega saab teabetaotlustele vastata asukohast sõltumata. Valveaja kehtestamine võib põhjustada uurimisasutusele mõningaid lisakulusid, kuid kuna sihtrühma kuuluvad uurimisasutused tagavad üldjuhul juba praegu operatiivse ööpäevaringse reageerimise, ei ole lisakulud märkimisväärsed. Selliste kuludega tuleb siiski arvestada asutuse eelarve planeerimisel.

Mõju sihtrühm II: ühtne kontaktpunkt

Teabevahetuse mahu ja selles osalevate uurimisasutuste ringi suurenemisega kasvab ühtse kontaktpunkti töökoormus, ent muudatuse mõju neile on valdavalt positiivne, sest edaspidi on ühtsel kontaktpunktil võimalik saada operatiivselt teavet kõikidelt uurimisasutustelt kindla kanali kaudu. Näiteks vahetab Sõjaväepolitsei regulaarselt teavet liitlaste sõjaväepolitsei üksustega, kes tavaliselt asuvad Eestis kohapeal, ent teave vastavate rikkumiste kohta ei jõua politseini üldse või ei jõua õigel ajal, sest puudub muu teabevahetuse platvorm kui füüsiline osapoolte kohtumine. Kuna teabevahetuses osalemisega liituvad uurimisasutused peavad olema SIENA-ga otse ühendatud, saavad nad edaspidi sisestada SIENA-sse teavet ise. Sellest on

huvitatud näiteks Keskkonnaamet, kelle teabevahetuse vajadus teiste EL-i liikmesriikidega on kasvutrendis ja jõudnud tasemeni, kus PPA koormus keskkonnakuritegusid puudutavate SIENA teadete vahendajana on jõudnud talumispiirini. Pea iga nädal vahetab Keskkonnaameti ligikaudu 15 uurijat keskkonnakuritegudega seonduvat teavet teiste EL-i liikmesriikidega. Eelkõige vahetatakse teavet riikidevahelise jäätmeveo, ohustatud liikidega kaubitsemise ja (mere) reostusjuhtumite kohta. Praegu vahetatakse keskkonnakuritegusid puudutavat teavet PPA kaudu pelgalt seetõttu, et Keskkonnaametil puudub juurdepääs SIENA-le. See takistus tekitab lisakoormust ja ebamugavusi nii Keskkonnaametile kui ka PPA-le, kuna teavet ei saa otse ja iseseisvalt vahetada.

Ühtse kontaktpunkti töökorraldusele avaldab positiivset mõju ka uurimisasutuste kohustus tagada suutlikkus teabetaotlustele vastata ööpäev läbi, sest see teeb võimalikuks lühikestes vastamistähtsagades püsimise. Konkreetse sidekanali ja kontakti olemasolu uurimisasutuses aitab ühtse kontaktpunkti ametnikke säästa aegkriitilises olukorras tarbetust ajakulust ning lisapingetest, mis tekivad teises asutuses taotlusele vastamiseks pädeva ametniku otsimisega. Muudatusega kaasnev negatiivne mõju ühtse kontaktpunkti töökorraldusele seisneb vajaduses tagada olemasoleva ressursiga teabevahetuses osalevate uurimisasutuste ametnike koolitamine. Kuna suur osa uurimisasutustest ei kasuta SIENA-t praegu ning nende senine kokkupuude rahvusvahelise teabevahetuse ja ühtse kontaktpunktiga on pigem juhuslikku laadi ja harv, tuleb tagada nende koolitamine. Eeltoodu põhjustab keskmist negatiivset mõju ühtse kontaktpunkti töökorraldusele, kuna vastavaks koolitamiseks on praegu pädev vaid nende personal ning koolitused tuleb tagada olemasolevate ametnikega põhitöö kõrvalt. Mõju esinemise sagedus on väike, sest koolitusvajadus esineb seadusemuudatuste jõustumisel, misjärel on uurimisasutuste koolitatud ametnikud võimelised tulevikus lisanduvaid kolleege ise koolitama.

Järeldus mõju olulisuse kohta. Muudatuse mõju sagedus ja ulatus sihtrühmale I on keskmine, kuid muudatusega ei kaasne olulist negatiivset mõju, vaid eeldatav mõju on positiivne. Muudatuse mõju sagedus ja ulatus sihtrühmale II on keskmine. Sihtrühmade I ja II käitumises kaasnevad küll muutused, kuid nendega ei kaasne eeldatavalt kohanemiskulusi.

6.3. Mõju isikuandmete töötlemisele

Käesoleva eelnõuga Rootsi direktiivi Eesti õigusesse ülevõtmisel lähtutakse reeglitest ja protseduuridest, mis võimaldavad tõhusat ja turvalist andmevahetust õiguskaitseasutuste vahel, säilitades samas isikuandmete kaitse kõrge taseme. Eelnõu eesmärk on parandada õiguskaitseasutuste koostööd ja teabevahetust, et tõhustada kuritegevuse ennetamist, uurimist ja avastamist. See hõlmab isikuandmete töötlemist, sealhulgas kogumist, säilitamist, kasutamist ja edastamist EL-i liikmesriikide õiguskaitseasutuste vahel.

PPA koostab kavandatavate muudatustega seoses andmekaitsealase mõjuhinnangu 2025. aasta lõpuks. Selle koostamine on vajalik, et hinnata isikuandmete töötlemise ja vahetamise mõjusid, tuvastada võimalikud riskid andmesubjektide õigustele ja vabadustele ning määratleda meetmed nende riskide maandamiseks. Koostatav analüüs on mõeldud asutusesiseseks kasutamiseks.

Andmetöötluse kirjeldus

- **Töödeldavad andmed:** isikuandmed, sealhulgas nimed, sünniajad, aadressid, kontaktandmed, kriminaalmenetluse andmed, biomeetrilised andmed ja muud isiku kohta teadaolevad andmed, mis on seotud andmetöötluse eesmärgiga.
- **Andmete saajad ja andjad:** uurimisasutused ja õiguskaitseasutused teistes EL-i liikmesriikides.

- **Andmetöötluse eesmärgid:** kuritegude ennetamine, uurimine, avastamine ja menetlemine.
- **Andmete säilitamine ja neile juurdepääs:** andmeid säilitatakse KrMS-is ette nähtud tähtajani. Andmetele juurdepääs on piiratud ja kaitstud turvameetmetega. Juurdepääs võimaldatakse üksnes konkreetse eesmärgi täitmiseks ja kindlatele teenistujatele; seejuures on tagantjärele võimalik kindlaks teha, kes ja milliste andmetele ligi on pääsenud (logimine). Andmeid edastatakse ainult teabetaotluse esitajale.

Riskid

- **Privaatsus ja konfidentsiaalsus:** võimalus, et isikuandmed lekivad, neid töödeldakse lubatust suuremal määral, kasutatakse väärtalt või neid säilitatakse kauem, kui lubatud.
- **Andmete täpsus ja ajakohasus:** risk, et andmed ei ole täpsed ega ajakohased, mis võib viia valede otsuste tegemiseni õiguskaitseasutustes.
- **Andmesubjektide õiguste rikkumine:** oht, et andmesubjektide õigusi, nagu juurdepääsu- ja parandamisõigust, ei austata piisavalt, ning risk, et töödeldakse isikuandmeid isiku kohta, kelle andmete töötlemiseks pole õigustatud alust.

Maandamismeetmed

- **Tehnilised meetmed:** krüpteerimine, logimine ja turvalised kommunikatsioonikanalid.
- **Organisatsioonilised meetmed:** selged asutusesised reeglid ja protseduurid andmete töötlemiseks, juurdepääsupiirangud ja ametnike koolitamine andmekaitse teemal.
- **Õiguslikud meetmed:** kooskõla IKS-iga ja EL-i andmekaitseõigusaktidega, sealhulgas õiguskaitse direktiiviga.
- **Järelevalve ja audit:** regulaarne järelevalve ja audit, et tagada andmekaitsemeetmete tõhusus ja vastavus õigusaktidele.

Rootsi direktiivist tekkiv kohustus tagada põhiõiguste kaitse isikuandmetöötluse kontekstis tuleneb juba praegu nii PS-ist, kehtivast EL-i õigusest kui ka Eestile siduvatest rahvusvahelistest inimõigusi tagavatest instrumentidest. Teabevahetus riivab õigust isikuandmete kaitsele ning on tihedalt seotud õigusega era- ja perekonnaelu austamisele ning informatsioonilisele enesemääramisõigusele.

Kuna IKS-is ja KrMS-is on juba praegu ette nähtud ja tagatud nõutaval tasemel isikuandmete kaitse, ei minda ka Rootsi direktiivi üle võtvas KrMS-i ja PPVS-i regulatsioonis sellest kaugemale, vaid tagatakse täielik kooskõla isikuandmete kaitse regulatsiooniga.

Teabevahetus peab toimuma SIENA kaudu selleks, et tagada isikuandmete kaitse vastavalt EL-i õigusele. SIENA kasutamine sidekanalina suurendab isikuandmete töötlemise turvalisust ja isikuandmete üldist kaitset võimaliku kuritarvitamise eest.

Isikuandmete suuremas mahus töötlemisega suureneb paratamatult isikuandmetega seotud rikkumise risk, näiteks andmelekk (konfidentsiaalsuse kadu), teenuste häirituse (käideldavuse kadu), andmete volitamata muutmise (tervikkuse kadu) või väärkasutuse ja juurdepääsu kuritarvitamise asetleidmise tõenäosus. Võrreldes praegusega on need riskid tulevikus oluliselt paremini maandatud, sest isikuandmete töötlemine SIENA kaudu on palju turvalisem kui alternatiivsete sidepidamisvahendite ja -kanalite kaudu. SIENA on spetsiaalselt loodud turvaliseks teabevahetuseks õiguskaitseasutuste vahel, järgides kõrgeid küberturvalisuse standardeid. See hõlmab krüpteeritud andmeedastust, autentimist ja juurdepääsupiiranguid, mis muudavad selle turvalisemaks kui alternatiivsed sidekanalid, nagu e-post või avalikud suhtlusplatvormid. SIENA võimaldab toimingute jälgitavust ja logimist, mis tagab, et iga toiming on dokumenteeritud ning volitamata juurdepääsu korral on võimalik kiiresti tuvastada rikkumised. See vähendab oluliselt riske võrreldes vähem struktureeritud ja vähem jälgitavate

kanalitega. SIENA kasutamine nõuab osalevatelt asutustelt ühtsete turva- ja töötlemisstandardite järgimist, mis tagab, et andmeid käideldakse kooskõlas rahvusvaheliste andmekaitse- ja turvanõuetega. Alternatiivsed suhtluskanalid, nagu e-post või mittekrüpteeritud andmeedastus, on sageli haavatavad andmelekete, andmepüügirünnakute ja küberturvalisuse rikkumiste suhtes. SIENA kasutamine maandab neid riske, pakkudes oluliselt paremat turvalisust.

Ühtne kontaktpunkt kasutab teabevahetuse andmete töötlemiseks töövoosüsteemi, mis võimaldab:

- täpselt tuvastada, kes ja millise kaasuse raames andmeid töödeldud on;
- vältida andmete ja päringute dubleerimist;
- ennetada põhjendamatute päringute tegemist.

Töövoosüsteem vähendab märkimisväärselt isikuandmete põhjendamatut töötlemise riski, mis võib tuleneda eksimusest või hooletusest. Süsteem kuvab andmete töötlejale selgelt, millised toimingud teabevahetusega on juba tehtud ja millised vajavad veel tegemist. PPA vastutab töövoosüsteemi loomise, nõuetelevastavuse ning õiguspärase kasutamise tagamise eest. PPA peab samuti tagama, et töövoosüsteemi logimisreeglid vastavad IKS-ile ja teistele andmekaitsealustele. Vajadusel tuleb teha ka täiendavaid IT-arendusi, et süsteem vastaks kõigile nõuetele.

Kavandatavad muudatused ühtlustavad, arendavad ja täpsustavad õiguskaitseasutuste omavahelist teabevahetust, muutes selle tõhusamaks ning samal ajal kaitstes paremini isikute põhiõigusi. Muudatustega luuakse suurem õigusselgus, määratledes selgelt:

- millist teavet võib ja tuleb vahetada EL-i liikmesriikide õiguskaitseasutuste vahel;
- kuidas selline teabevahetus peab toimuma.

Need täpsustused vähendavad praktikas tekkivaid probleeme KrMS-i ja PPVS-i rakendamisel. Muudatuste abil kehtestatakse selged ja üksikasjalikud juhised teabevahetuseks teiste EL-i liikmesriikide ja Europoliga. Samuti sätestatakse konkreetsed alused, mille korral võib teabevahetusest põhjendatult keelduda. Selline raamistik tagab õigusselguse ja aitab õiguskaitseasutustel oma ülesandeid tõhusamalt täita.

7. Seaduse rakendamisega seotud riigi ja kohaliku omavalitsuse tegevused, eeldatavad kulud ja tulud

Nii ühtsele kontaktpunktile (PPA) kui ka uurimisasutustele lisanduvad eelnõu rakendamisega teatud kulud ja täiendav töökoormus, samuti kaasnevad eelnõukohaste muudatuste rakendamisel kulud seoses koolitusvajadusega ning IT-süsteemide arendamisega.

7.1. Ühtne kontaktpunkt

Praegu töötleb ühtne kontaktpunkt eri kanalites (SIS, Interpoli-i 24/7 ja SIENA) kokku umbes 130 000 – 150 000 teabeühikut aastas (koos kolmandate riikidega üle 200 000). Eelnimetatud töötlus hõlmab näiteks teabetaotlusi ja operatiivinfo sisestusi infosüsteemidesse. Juba praegune statistika näitab teabevahetuse mahu kasvu. Eelnõuga kavandatavad muudatused, eeskätt kohustus vahetada veel rohkem teavet ja teabevahetuse tähtaegade lühenemine, suurendavad teabevahetuse mahtu veelgi.

Käesoleva eelnõuga kavandatavate muudatustega suureneb ühtse kontaktpunkti koordineeriv roll nii organisatsioonisiselt kui ka -väliselt. Esiteks seetõttu, et teatav teabevahetus muutub

kohustuslikuks. Samuti seepärast, et senine teabevahetuse tähtaja üldreegel lüheneb poole võrra ehk seniselt 14 päevalt seitsmele. Lisaks tuleb välja töötada ja ajakohasena hoida tööprotsessid, mis toetavad teabevahetust mitmete uurimisasutustega, kellega senine kogemus teabevahetuses on olnud kasin või puudunud.

Tagamaks rahvusvahelise teabevahetuse ning uute tööprotsessidega kaasneva töö (nt andmete säilitamine ja statistika kogumine) nõutaval tasemel – sealhulgas olemasolevate ametnike puhkuste, töö- ja puhkeaja tagamine, tööalaste teadmiste ja oskuste arendamiseks vajalikel koolitustel osalemine, töötervishoiuga seotud aja võimaldamine –, on PPA hinnangul vaja ühtset kontaktpunkti täiendada seitsme ametnikuga. Täiendavate ametikohtade loomine lisab igasse vahetusse ühe ametniku, tagab rahvusvahelisele teabevahetusele esitatud nõuete täitmise, sealhulgas tähtaegadest kinnipidamise, ning vahetatava teabe ja süsteemidesse kantavate andmete kvaliteedi. Kuna suurim koormus langeb vahetustega töötavatele ja kogu töövoogu haldavatele operatiivinfo halduritele, on vaja lisada igasse vahetusse üks täiendav ametnik ehk kokku tuleks PPA-sse juurde viis operatiivinfo halduri ametikohta. Arvestades Rootsi direktiivi rakendamisega kaasnevaid täiendavaid kvaliteedinõudeid, on vaja luua ka üks rakenduseksperdi ametikoht, kelle ülesanne on toetada teisi ametnikke andmekvaliteedi küsimustes ning korraldada töövoogu sujuvus ja tähtaegade järgimine. See on vajalik, kuna SIENA kasutajaid on väljaspool ühtset kontaktpunkti ligikaudu 50 ning tegemist on ametnikuga, kes oma menetlustes teevad iseseisvalt teabetaotlusi välisriikidesse, kuid mitte oma põhitööna. Samuti on hiljemalt kolm aastat peale Rootsi direktiivi ülevõtmist vaja vähemalt ühte eraldi ametikohta selleks, et hinnata kõiki toimunud teabevahetusi ehk vaadata need üle eesmärgiga otsustada isikuandmete edasise säilitamise põhjendatuse üle.

Täiendavate ametikohtade loomiseks vajab PPA 2025. aastal 500 000 eurot ja alates 2026. aastast 481 000 eurot aastas. Siseministeeriumi valitsemisala eelarves puuduvad vahendid täiendavateks kuludeks ning vajalike ametikohtade loomiseks on vaja tagada PPA-le lisarahastus riigieelarvest. Taotlused lisarahastuse saamiseks on PPA esitanud, kuid täiendavaid vahendeid ei ole käesoleval hetkel eraldatud.

7.2. IT-arendused

Eelnõuga nähakse ette, et teabevahetuse tõhusaks korraldamiseks peab ühtsel kontaktpunktil olema elektrooniline töövoosüsteem. PPA olemasolev töövoosüsteemi rakendus on kasutusel 2013. aastast ning Siseministeeriumi infotehnoloogia- ja arenduskeskuse (edaspidi *SMIT*) hinnangul on tegemist amortiseerunud tarkvaraga, mis ei vasta enam sellisele süsteemile esitatud turvanõuetele (ISKE K3T2S2). Samuti ei ole võimalik arendada uusi vajalikke funktsionaalsusi ehk tagada teabevahetust erinevate EL-i IT-süsteemide ja riiklike süsteemide vahel. Erinevate hindamiste tulemusel (nt Schengeni hindamised, Andmekaitse Inspektsiooni kontrollkäik Sirene büroosse) on Eestile tehtud korduvad ettekirjutused rahvusvahelise teabevahetuse töövoogu automatiseerimiseks ja liidestamiseks teiste infosüsteemidega, sealhulgas SIENA-ga.

PPA olemasolev elektrooniline töövoosüsteem ei sisalda võimalust automaatselt integreerida teabevooge, mis on seotud teiste EL-i liikmesriikide poolt vastu võetud või neile saadetud sissetulevate ja väljaminevate teabetaotlustega. Lisaks ei võimalda praegune töövoosüsteem automaatselt salvestada asjakohast suhtlust või teabevahetust ühtse kontaktpunkti ja uurimisasutuste vahel. Interpoli ülemaailmne politsei sidekanal I-24/7 ei ole täielikult integreeritud elektroonilisse töövoosüsteemi ja seda hallatakse sõnumite käsitsi registreerimise kaudu ühtse kontaktpunkti töövoosüsteemis, samas kui SIENA ei ole sellesse integreeritud. Selline eraldamine võib viivitada või isegi takistada eri rahvusvaheliste kanalite kaudu toimunud teabevahetuse seoste tuvastamist. Lisaks ei võimalda see tõhusat teabehaldust, kuna

äriprotsesse ei saa automatiseerida ja lõppkasutajad peavad täiendavalt käsitsi salvestama teavet, mis võib kahjustada analüüsi ja piiriülese teabevahetuse tõhusust ja tulemuslikkust. Töövoosüsteem ei paku praegu peaaegu mingit automatiseerimist, kuna see ei hõlma võimalust otsida ja salvestada saadaolevat teavet asjakohastes riiklikes, EL-i ja rahvusvahelistes andmebaasides, ning see ei ole ühendatud kõigi asjakohaste õiguskaitsealase koostöö kanalitega, nagu SIENA ja Interpoli ülemaailmne politsei sidekanal I-24/7.

Arvestades eeltoodut, peab PPA eelnõuga kavandatavate muudatuste rakendamiseks kas uuendama olemasolevat töövoosüsteemi või looma täiesti uue süsteemi.

PPA ja SMIT on hinnanud, et olemasoleva elektroonilise töövoosüsteemi (vana platvorm) mittetoimimine võib tuua kaasa andmekaitsealaste rikkumise, näiteks andmete säilitamisel, ning platvorm on vastuvõtlik eri turvanõrkustele. Samuti võib vanal platvormil töövoosüsteemi mittetoimimine tuua kaasa täiendava töövoogu rakendamise, mis erineb rahvusvahelisest kokkuleppest ja koormab nii riigisisesid kui ka rahvusvaheliste välispartnerite ressursse.

Tulenevalt eeltoodust on PPA ja SMIT hinnanud vajalikuks viia töövoosüsteem uuele platvormile. Sellega seoses kaasneb PPA-le kulu ligikaudu 500 000 eurot. Kuna Siseministeeriumi valitsemisala eelarves puudusid selleks vajalikud lisavahendid, oli IT-arenduste elluviimiseks vaja tagada PPA-le täiendav riigieelarveline rahastus. Käesolevaks ajaks on vajalik lisarahastus tagatud ning vastavad taotlused on rahuldatud.

7.3. Koolituskulud

Arvestades üha suurenevat vajadust piiriülese õiguskaitsealase koostöö järele, sealhulgas sellega seonduvat tundliku teabe käsitlemist, on oluline, et ühtse kontaktpunkti ja uurimisasutuse töötajatel oleksid KrMS-i ja PPVS-i kohaste ülesannete õiguspäraseks, tõhusaks ja tulemuslikuks täitmiseks vajalikud teadmised ja oskused. Selleks tuleb nii ühtse kontaktpunkti töötajatele kui ka uurimisasutuste ametnikele pakkuda asjakohaseid ja korrapäraseid koolitusi, mis vastavad nende ametialastele vajadustele ja konkreetsele taustale ning hõlbustavad kehtestatavate normide täitmiseks vajalikke kontakte teiste EL-i liikmesriikide ühtsete kontaktpunktide ja pädevate õiguskaitseasutustega. Koolitused peaksid olema suunatud eelkõige andmetöötlusprogrammide ja IT-süsteemide nõuetekohasele kasutamisele. Samuti on vajalik täiendada ametnike teadmisi EL-i ja liikmesriikide justiits- ja siseküsimuste valdkonna õigusraamistike osas, keskendudes eelkõige isikuandmete kaitsele, õiguskaitsealasele koostööle ja juurdepääsupiiranguga teabe käitlemisele. Kindlasti on oluline parandada rahvusvahelises koostöös osalevate ametnike inglise keele oskust, et aidata ületada keelebarjääri.

Ametnike koolitamiseks on võimalik kasutada ka Euroopa Liidu Õiguskaitsekoolituse Ameti⁸³ (edaspidi *CEPOL*) pakutavaid koolitusi ja asjakohaseid vahendeid. Uurimisasutused ja ühtne kontaktpunkt võiksid kaaluda võimalust, et nende töötajad saaksid veeta ühe nädala Europoli tööga tutvudes. Samuti tuleks võimalusel kasutada muid asjakohaseid pakkumisi, mida on tehtud EL-i eelarvest rahastatavate programmide ja projektide, näiteks CEPOL-i vahetusprogrammi raames.

Eelnõu rakendamisega seonduvad koolituskulud näeb iga uurimisasutus ja ühtne kontaktpunkt ette oma eelarves, kuna tegemist on mahult ja sisult tavapärase väikesemahuliste kuludega. Koolituste korraldamisega seotud otsesed kulud (nt koolitajate töö, koolitusmaterjalid ja

⁸³ Euroopa Liidu Õiguskaitsekoolituse Amet (CEPOL). Kättesaadav: <https://www.cepola.europa.eu/et>.

ruumide kasutamine) katab koolitaja, samas kui ametnike osalemisega kaasnevad kulud (nt sõidu- ja majutuskulud ning töölt eemalviibimise aeg) jäävad vastavate uurimisasutuste enda kanda.

Kõigil Eesti uurimisasutuste töötajatel, kelle teenistusülesanded seda nõuavad, on juba praegu võimalik osaleda Euroopa Liidu Õiguskaitsekoolituse Ameti (*CEPOL*) pakutaval koolitustel, sealhulgas SIENA süsteemi kasutajakoolitustel. CEPOL-i koolitused on liikmesriikidele tasuta ja kulud kaetakse EL-i vahenditest. Tegemist on süvendatud taseme väljaõppega, mis kestab kuni viis päeva, ning on mõeldud eeskätt ühtse kontaktpunkti töötajatele, kelle töö põhiülesanne on töödelda vaid rahvusvahelist operatiivinfot. Lisaks võib koolitamine toimuda ühtse kontaktpunkti poolt või ka uurimisasutuste sees, sarnaselt uute töötajate tavapärasele väljaõppele, kus kogenumad ametnikud koolitavad kolleege. Selline koolitusmudel võimaldab – erinevalt CEPOL-i koolitustest, mis toimuvad nende koolituskalendri alusel – tagada koolituste korraldamise uurimisasutuste vajadustest lähtuvalt siis, kui uurimisasutusel koolitusvajadus tekib (eeskätt uue töötaja tulekul).

Koolituste täpsem korraldus ja osapoolte rollid lepitakse kokku asutustevahelistes kokkulepetes, kuna need sõltuvad ühtse kontaktpunkti töökorraldusest, mis on samuti asutustevahelise kokkuleppega sätestatav ning võib asutuste lõikes erineda. Näiteks võib uurimisasutus lähetada ametniku alaliselt ühtse kontaktpunkti koosseisu, tagada asutuse teabevahetuses osalemise nn valvetelefoni kaudu või säilitada eraldiseisva asutusesisese kontaktpunkti (nt MTA). Ühtse kontaktpunkti koosseisu korralduse alusel kujuneb ka koolituste täpsem ülesehitus ja sisu, kuid kõik variandid on korraldusliku iseloomuga ega too kaasa märkimisväärsed lisakulusid.

8. Rakendusaktid

Seaduse rakendamiseks on PPVS § 25⁹ lõike 3 alusel vaja kehtestada üks uus rakendusakt:

- siseministri määrus „Nõuded töövoosüsteemi toimimisele, ülesehitusele ja haldamisele ning selle andmete töötlemisele, logimisele, kontrollile, juurdepääsule, väljastatavale statistikale ja järelevalvele“.

PPVS § 25⁹ lõikes 3 käsitletakse töövoosüsteemi, mis on osa seaduse rakendamiseks vajalikust tehnilisest ja korralduslikust raamistikust. Seaduses sätestatakse üldised põhimõtted, kuid tehnilised, turvalisuse ja andmetöötluse nõuded on oma olemuselt detailirohked ning ajas kiiresti muutuva iseloomuga. Selliseid detaile ei ole otstarbekas ega isegi võimalik seaduse tasandil ammendavalt reguleerida, sest nende täpsustamine nõuab muu hulgas tehniliste standardite ja infosüsteemi arhitektuuri määratlemist, turva- ja logimisnõuete ajakohastamist vastavalt IT-turbe arengule, samuti andmetöötlusprotsesside täpsustamist, et tagada isikuandmete kaitse ja andmete terviklikkus.

Tegemist on põhiõigusi (PS § 26, eraelu puutumus; § 43, side- ja teabevahetuse saladus; § 44, info vaba liikumine) riivavate tehniliste tingimustega, mis peavad olema seaduses sätestatud üldpõhimõtete alusel, kuid mille üksikasjad peab kindlaks määrama täitevvõim. Volitusnorm annab siseministrile õiguse kehtestada täpsemad rakendusnõuded seaduse elluviimiseks, tagades õigusselguse, tehnilise turvalisuse ja andmekaitse vastavuse.

Volitusnormiga määratletakse, milliseid teemasid minister määruses reguleerib. See hõlmab järgmist:

- **töövoosüsteemi toimimise nõuded** – töökindlus, reageerimisvõime, katkestuskindlus;
- **süsteemi ülesehitus** – arhitektuurilised põhimõtted, andmebaaside ja liideste kirjeldus;

- **halduse kord** – süsteemi administreerimise ja hoolduse põhimõtted, turvameetmed;
- **andmete töötlemise kord** – millised andmed sisestatakse, kuidas neid säilitatakse, säilitustähtaegade ja kustutamise kord;
- **logimise nõuded** – milliseid sündmusi logitakse, logide säilitamise kord ja turvameetmed;
- **kontroll ja järelevalve** – kes teostab, milliste vahenditega ja mis sagedusega;
- **juurdepääsu tingimused** – autentimis- ja autoriseerimismeetodid, rollipõhine ligipääs;
- **statistika väljastamise kord** – millisel kujul ja kellele andmeid antakse.

Olemasolevaid rakendusakte muuta vaja ei ole. Kehtetuks muutuvad:

- siseministri 10. juuni 2015. aasta määruse nr 32 „[Euroopa Liidu liikmesriigile teabe ja jälitustoiminguga kogutud teabe edastamise vorm](#)“ redaktsioon avaldamismärkega RT I, 12.06.2015, 3;
- siseministri 22. detsembri 2014. aasta määruse nr 58 „[Euroopa Liidu liikmesriigilt teabe ja jälitustoiminguga kogutud teabe taotlemise vorm](#)“ redaktsioon avaldamismärkega RT I, 29.12.2014, 51.

9. Seaduse jõustumine

Seaduseelnõu on kavandatud jõustuma üldises korras. Eelnõu jõustumine on kavandatud üldises korras, kuna selle eesmärk on tagada õigusaktide vastavus EL-i õigusele ning lõpetada Eesti suhtes Rootsi direktiivi ülevõtmisega viivitamisega seoses algatatud rikkumismenetlus. Arvestades, et rikkumismenetluse jätkumine võib kaasa tuua Eesti suhtes sanktsioonide kohaldamise, on oluline, et seadus jõustuks viivitusteta pärast vastuvõtmist ja avaldamist. Üldine jõustumiskord võimaldab eelnõuga kavandatavad muudatused ellu viia võimalikult kiiresti, tagades samal ajal õigusselguse ja rakendusvalmiduse.

10. Eelnõu koostööstamine, huvirühmade kaasamine ja avalik konsultatsioon

Eelnõu esitatakse Vabariigi Valitsuse istungile. Eelnõu on läbinud koostööstusringid eelnõude infosüsteemis (EIS). Eelnõu kohta esitatud märkuste ja ettepanekute arvestamise tabel on esitatud seletuskirja lisa 4.

Lauri Hussar
Riigikogu esimees

Tallinn, 2025

Algatab Vabariigi Valitsus 2025