Väljaandja:	Vabariigi Valitsus
Akti liik:	määrus
Teksti liik:	terviktekst
Redaktsiooni jõustumise kp:	01.01.2025
Redaktsiooni kehtivuse lõpp:	Hetkel kehtiv
Avaldamismärge:	RT I, 21.03.2025, 22

Jälitustoimingute infosüsteemi asutamine ja infosüsteemi pidamise põhimäärus

Vastu võetud 19.02.2015 nr 17
RT I, 20.02.2015, 19
jõustumine 01.09.2015

Muudetud järgmiste aktidega

Vastuvõtmine	Avaldamine	Jõustumine
11.12.2024	RT I, 30.12.2024, 1	01.01.2025, Vabariigi Valitsuse seaduse § 105.19 lõike 12 alusel asendatud sõna „Justiitsministeerium” sõnadega „Justiits- ja Digiministeerium” vastavas käändes

Määrus kehtestatakse kriminaalmenetluse seadustiku§ 126[17]lõike 2 alusel.

1. peatükk
ÜLDSÄTTED

§ 1. Infosüsteemi asutamine ja nimetus

Määrusega asutatakse riigi infosüsteemi kuuluv andmekogu ametliku nimetusega jälitustoimingute infosüsteem (edaspidi *infosüsteem*).

§ 2. Infosüsteemi eesmärk ja rahastamine

(1) Infosüsteemi asutamise ja pidamise eesmärk on:
1) tagada ülevaade jälitusasutuste poolt tehtavatest jälitustoimingutest;
2) tagada ülevaade jälitusasutuste ja prokuratuuri jälitustoimingu tegemise taotlustest;
3) tagada ülevaade prokuratuuri ja kohtute poolt antud jälitustoimingu tegemise lubadest;
4) tagada ülevaade jälitustoimingust teavitamisest ja jälitustoiminguga kogutud andmete tutvustamisest;
5) kajastada andmeid tehtud jälitustoimingute kohta;
6) võimaldada jälitusasutuste, prokuratuuri ja kohtute töö korraldamist;
7) tagada kriminaalpoliitiliste otsuste tegemiseks vajaliku jälitustoimingute statistika kogumine;
8) võimaldada andmete ja dokumentide elektroonilist edastamist.

(2) Infosüsteemi asutamist, arendamist ja pidamist rahastatakse Justiits- ja Digiministeeriumi eelarve kaudu. [RT I, 30.12.2024, 1- jõust. 01.01.2025, Vabariigi Valitsuse seaduse § 105.19 lõike 12 alusel asendatud sõna „Justiitsministeerium” sõnadega „Justiits- ja Digiministeerium” vastavas käändes]

§ 3. Infosüsteemi ülesehitus, liidestatus ja seotus teiste infosüsteemidega

(1) Infosüsteemi peetakse ühetasandilise digitaalse andmekoguna.

(2) Infosüsteemi pidamisel kasutatakse automatiseeritud andmetöötlust ning andmeid säilitatakse digitaalsel kujul. Infosüsteemi andmete kandmise alusdokumente võib säilitada ka paberkandjal.

(3) Infosüsteem on täisdigitaalne keskkond, kus § 5 lõikes 1 nimetatud volitatud töötlejad saavad kriminaalmenetluse seadustiku 3^1. peatükis sätestatud korras ja pädevuse piirides koostada ja esitada taotlusi ning koostada ja anda lube jälitustoimingute tegemiseks, sisestada jälitustoimingute tegemise andmeid ja jälitustoimingutega riivatud isikute andmeid, suunata isikuid tehtud jälitustoimingutest teavitamisele ja toimingute tutvustamisele või koostada ja anda lube tutvustamata ja teavitamata jätmise kohta.

(4) Infosüsteemi tehtud kanded, sisestatud andmed ja koostatud dokumendid seotakse kindla jälitustoimiku numbriga, mille alusel moodustub infosüsteemis täisdigitaalne toimik (edaspidi *digitaalne jälitustoimik*). Kanne käesoleva määruse tähenduses on jälitustoimingut puudutavate andmete ja dokumentide sisestamine, parandamine või kustutamine.

(5) Andmete infosüsteemi kandmisel esitatakse päringuid ja saadakse andmeid sellega liidestatud andmekogudest.

(6) Andmete dubleeritud sisestamise vältimiseks võib infosüsteemi liidestada muude andmekogudega, mis on seotud infosüsteemi pidamise eesmärgiga või vajalikud infosüsteemi pidamise terviklikkuse tagamiseks.

2. peatükk
VASTUTAV TÖÖTLEJA, VOLITATUD TÖÖTLEJA JA HALDUR

§ 4. Vastutav töötleja ja tema pädevus

(1) Infosüsteemi vastutav töötleja on Justiits- ja Digiministeerium.
[RT I, 30.12.2024, 1- jõust. 01.01.2025, Vabariigi Valitsuse seaduse § 105.19 lõike 12 alusel asendatud sõna „Justiitsministeerium" sõnadega „Justiits- ja Digiministeerium" vastavas käändes]

(2) Vastutav töötleja:
1) lahendab infosüsteemi puudutavaid õiguslikke küsimusi ning nõustab infosüsteemi kasutajat õiguslikes küsimustes;
2) korraldab infosüsteemi kasutajate koolitamise ja infosüsteemi kasutamisel puuduste ilmnemise korral puuduste kõrvaldamise ning infosüsteemi eesmärgipärase pidamise ja andmetöötluse;
3) teavitab volitatud töötlejat ja haldurit viivitamata registri pidamist puudutavate kohustuste täitmist takistavatest asjaoludest ja registri pidamist reguleerivate õigusaktide muutmise kavatsusest ning annab muud infosüsteemi pidamisega seotud vajalikku teavet;
4) vastutab infosüsteemi pidamise, ajakohastamise, järjepideva toimimise ning andmete väljastamise õiguspärasuse eest;
5) korraldab infosüsteemi pidamiseks vajalike projekteerimis- ja arendustööde tegemise;
6) määrab infosüsteemi turvanõuded ja juhib infosüsteemi pidamist, andes volitatud töötlejale selleks vajalikke juhiseid;
7) piirab ühepoolselt kasutaja juurdepääsu infosüsteemile või peatab selle, kui esineb reaalne või võimalik oht infosüsteemi turvalisusele.

§ 5. Volitatud töötleja ja tema pädevus

(1) Infosüsteemi volitatud töötlejad (edaspidi *volitatud töötleja*) on:
1) prokuratuur;
2) uurimisasutused;
3) kohtud.

(2) Volitatud töötleja:
1) sisestab infosüsteemi kasutajateks oma asutuse ametnikud, kellel on ametiülesannetest tulenev õigus sisestada, töödelda ja kasutada infosüsteemi andmeid, samuti lõpetab juurdepääsu, kui kasutaja ametiülesanded lõpevad;
2) määrab infosüsteemi kasutajateks sisestatud ametnike juurdepääsuõiguse ja rolli infosüsteemis andmete töötlemisel, samuti laiendab juurdepääsuõigust vastavalt ametialasele teadmisvajadusele;
3) sisestab infosüsteemi kõik jälitustoimingute tegemiseks nõutavad load ja taotlused, jälitustoimingu tegemise andmed, jälitustoiminguga oluliselt riivatud isikute andmed ning isiku teavitamise ja jälitustoiminguga kogutud andmete tutvustamise andmed;
4) vastutab enda poolt infosüsteemi sisestatud andmete õigsuse eest;
5) korraldab koostöös halduriga infosüsteemi ebaõigesti sisestatud andmete ja tehtud kannete parandamise või kustutamise ja sisestamata jäetud andmete sisestamise;
6) annab infosüsteemi andmetes puuduste avastamise korral sellest viivitamata teada haldurile, välja arvatud juhul, kui tal on võimalik puudused iseseisvalt kõrvaldada, tagades sellisel viisil infosüsteemi sujuva töövõimekuse, või kui avastatud puudus on ebaoluline;
7) annab infosüsteemi sujuva kasutamise takistustest ja tõrgetest viivitamata teada haldurile;
8) rakendab andmete turvalisuse – käideldavuse, tervikluse ja konfidentsiaalsuse – tagamiseks infosüsteemi turvanõuetele vastavaid organisatsioonilisi, füüsilisi ja infotehnoloogilisi turvameetmeid, rakendab neid järjepidevalt;

9) teostab teenistuslikku järelevalvet oma asutuse kasutajate poolt infosüsteemi eesmärgipärase, tähtaegse ja teadmisvajaduse põhise kasutamise üle. Volitatud töötleja volitatud ametnik kontrollib, kas kasutajad peavad kinni seadustest, käesolevast määrusest ning vastutava töötleja juhistest ja korraldustest.

(3) Lõike 2 punktis 1 nimetatud toiminguid võib teha volitatud töötleja juht või tema poolt kirjalikult volitatud isik.

§ 6. Registrite ja Infosüsteemide Keskuse pädevus

(1) Infosüsteemi arendab, hooldab ja majutab Justiits- ja Digiministeeriumi hallatav riigiasutus Registrite ja Infosüsteemide Keskus (edaspidi *haldur*).
[RT I, 30.12.2024, 1- jõust. 01.01.2025, Vabariigi Valitsuse seaduse § 105.19 lõike 12 alusel asendatud sõna „Justiitsministeerium" sõnadega „Justiits- ja Digiministeerium" vastavas käändes]

(2) Halduri ülesandeks on volitatud töötleja nõustamine ja abistamine infosüsteemi kasutamisel, sealhulgas:
1) infosüsteemi kasutamise takistuste ja tõrgete kõrvaldamine ning infosüsteemi sujuva töövõimekuse kiire taastamine ja tagamine;
2) infosüsteemis täitmist nõudvatest tööülesannetest kasutajate teavitamise mehhanismi töökindluse ja täpsuse tagamine vastavalt kasutaja valitud seadistusele;
3) koostöös volitatud töötlejaga infosüsteemi sisestatud andmete nõuetekohase säilimise ja selleks varukoopiate tegemise korraldamine ja tagamine;
4) infosüsteemi ebaõigesti sisestatud andmete ja tehtud kannete parandamine või kustutamine ning infosüsteemi sisestamata jäetud andmete sisestamine volitatud töötleja taotlusel, kui volitatud töötleja seda ise teha ei saa;
5) statistilistest vajadustest lähtuvalt vaatleja rolliga ametnikele infosüsteemile juurdepääsu tagamine mahus, mis võimaldab statistiliste andmete kogumist, välistades seejuures isiku tuvastamise ja jälitustoiminguga kogutud info nähtavuse;
6) andmete turvalisuse – käideldavuse, tervikluse ja konfidentsiaalsuse – tagamiseks infosüsteemi turvanõuetele vastavate organisatsiooniliste, füüsiliste ja infotehnoloogiliste turvameetmete rakendamine ning infosüsteemi pidamiseks eraldatud vahendite otstarbeka kasutamise tagamine;
7) vastutava töötleja viivitamatu teavitamine infosüsteemi pidamist või kasutamist takistavatest probleemidest koos ettepanekuga probleemide efektiivseks kõrvaldamiseks;
8) teiste ülesannete täitmine, mis tulenevad käesoleva määrusega tema pädevusse antud ülesannetest või on käesoleva määrusega antud tema pädevusse.

(3) Halduril on õigus esitada volitatud töötleja juhile päring, kui volitatud töötleja kasutaja ei ole loginud infosüsteemi sisse järjest ühe aasta jooksul, et selgitada välja selle kasutaja infosüsteemile juurdepääsu vajadus ning lõpetada volitatud töötleja taotlusel selle kasutaja juurdepääs, kui ametialane vajadus selleks on ära langenud.

(4) Halduril on lõikes 2 sätestatud ülesannete kiireks ja lõplikuks lahendamiseks ja lõikes 3 nimetatud juhul infosüsteemist kustutatud andmete ja logide nägemise õigus, selliste kannete muutmise õigus, mida kasutaja muuta ei saa, ning klassifikaatorite ja õigusaktide muudatustest tulenevalt infosüsteemis muudatuste tegemise õigus.

§ 7. Halduri kasutajate registreerimine

(1) Halduri kasutajate üle peab nimelist arvestust haldur.

(2) Uue kasutaja registreerimiseks edastab kasutaja vahetu juht halduri juhile registreerimistaotluse. Halduri kasutaja registreerimisel tuleb veenduda, et kasutajal on juurdepääsu õigus piiratud taseme riigisaladusele.

(3) Halduri kasutaja riigisaladusele juurdepääsu õiguse lõppemisel, volituste lõppemisel või halduri teenistusest lahkumisel esitab kasutaja vahetu juht halduri juhile taotluse kasutaja infosüsteemile juurdepääsu õiguse lõpetamiseks.

3. peatükk
ANDMETE KAITSE JA JUURDEPÄÄS INFOSÜSTEEMILE

§ 8. Infosüsteemis töödeldavate andmete kaitse

(1) Infosüsteemis töödeldakse kuni piiratud tasemel salastatud teavet riigisaladuse ja salastatud välisteabe seaduse tähenduses.

(2) Vastavalt andmete liigile ja sisule korraldatakse infosüsteemis töödeldavate andmete kaitset kriminaalmenetluse seadustiku, isikuandmete kaitse seaduse, avaliku teabe seaduse ning riigisaladuse ja salastatud välisteabe seaduse ja selle alusel antud õigusaktide alusel.

(3) Juurdepääs infosüsteemis töödeldavatele andmetele tagatakse ainult vastutava ja volitatud töötleja kasutajatele ning halduri kasutajatele, kellel on juurdepääsu õigus piiratud taseme riigisaladusele.

(4) Andmeid töötlevad infosüsteemi kasutajad on kohustatud hoidma saladuses neile infosüsteemi andmete töötlemisel teatavaks saanud mis tahes andmed.

(5) Infosüsteemi andmete kaitseks rakendatakse nõuetekohaseid organisatsioonilisi, füüsilisi ja infotehnoloogilisi teabeturbe meetmeid.

§ 9. Juurdepääs infosüsteemile

(1) Vastutav töötleja võimaldab infosüsteemile juurdepääsu volitatud töötleja ja halduri töötajale, kellel on riigisaladuse ja salastatud välisteabe seaduses sätestatud juurdepääsu õigus piiratud taseme riigisaladusele.

(2) Infosüsteemis kannete tegemise ja andmetöötluse õigus on volitatud töötlejal üksnes jälitustoimingutega seotud ja seaduses sätestatud pädevuse raames ja ülesannete täitmiseks.

(3) Paragrahvis 12 sätestatud järelevalve teostamise korras on õigus kontrollida kannete ja andmetöötluse vastavust seaduses sätestatud pädevusele ja ülesannetele ning käesolevas lõikes sätestatud juurdepääsu korral vastavust selle eesmärgile. Järelevalvet teostaval ametnikul ei ole juurdepääsu käimasoleva kriminaalmenetluse jälitustoiminguid käsitlevale teabele, kui andmetele juurdepääs ohustab kriminaalmenetluse või jälitustoimingu eesmärki.

§ 10. Juurdepääs infosüsteemi sisestatud andmetele

(1) Infosüsteemi sisestatud andmetele võimaldatakse juurdepääs riigisaladuse ja salastatud välisteabe seaduses ja kriminaalmenetluse seadustikus sätestatud tingimustel isikule või asutusele, kellel on selleks seadusest tulenev õigus. Loa andmise infosüsteemi sisestatud andmetele juurdepääsuks otsustab prokurör.

(2) Juurdepääs andmetele võimaldatakse juurdepääsuõiguse andmisega või väljavõttena infosüsteemist.

(3) Juurdepääsu võimaldamiseks peab isik või asutus esitama prokuratuurile kirjaliku taotluse, milles tuleb esitada vähemalt järgmised andmed:
1) taotluse esitaja nimi või nimetus;
2) isiku- või registrikood;
3) taotluse allkirjastaja ees- ja perekonnanimi;
4) taotluse esitaja ametikoht, kui taotlejaks on juriidiline isik või ametiasutus;
5) juurdepääsuõiguse taotlemise vajaduse põhjendus ning viide andmete saamise aluseks olevale õigusnormile;
6) selle isiku ees- ja perekonnanimi, isikukood ning ameti- või töökoht, kellele juurdepääsuõigust taotletakse;
7) juurdepääsu kestus;
8) isiku riigisaladusele juurdepääsu loa tase;
9) nende andmete kirjeldus või loetelu, millele juurdepääsu õigust taotletakse;
10) soovitav andmetele juurdepääsu viis.

(4) Prokuratuur otsustab juurdepääsuõiguse andmise või sellest keeldumise ning juurdepääsuõiguse andmise ulatuse ja viisi 30 päeva jooksul nõuetekohase taotluse saamisest arvates.

§ 11. Juurdepääs infosüsteemile statistiliste andmete kogumise eesmärgil

(1) Infosüsteemi sisestatud andmetele võib prokuratuuri loal saada juurdepääsu käesolevas paragrahvis nimetatud tingimustel statistiliste andmete kogumise eesmärgil vastutava töötleja töötaja. Loa saamiseks esitab isik kirjaliku põhistatud taotluse.

(2) Statistiliste andmete kogumise eesmärgil kasutajad sisestab infosüsteemi vastutava töötleja taotlusel haldur.

(3) Statistiliste andmete kogumise eesmärgil infosüsteemile juurdepääsu õigusega kasutajatel on juurdepääs infosüsteemi andmetele, mis ei ole riigisaladus.

(4) Statistiliste andmete kogumise eesmärgil ei ole juurdepääsu jälitustoimingutega seotud ega riivatud isikute isikuandmetele, jälitustoiminguga kogutud andmetele, samuti ei ole avatavad jälitustoimingute lubade ja taotluste dokumendid.

§ 12. Volitatud töötleja teenistusalane järelevalve

(1) Volitatud töötleja teostab järelevalvet infosüsteemi eesmärgipärase pidamise, tähtaegse andmete sisestamise ja töötlemise ning põhjendatud teadmisvajaduse korral infosüsteemi andmetele juurdepääsu õiguse kasutamise üle.

(2) Volitatud töötleja juht määrab kindlaks teenistusalase järelevalve teostamiseks pädeva volitatud töötleja töötaja. Volitatud töötleja koostab kokkuvõtte eelnenud aasta jooksul teostatud teenistusalase järelevalve käigus avastatud puudustest ja nende kõrvaldamisest jooksva aasta 31. märtsiks. Kokkuvõte järelevalve tulemustest edastatakse 30 päeva jooksul vastutavale töötlejale.

(3) Volitatud töötleja on kohustatud kõrvaldama teenistusalase järelevalve teostamisel ilmnenud puudused infosüsteemi pidamisel ning võtma tarvitusele abinõud puuduste kordumise vältimiseks.

4. peatükk
TEGEVUSED INFOSÜSTEEMIS

§ 13. Infosüsteemi eelteavitused

(1) Infosüsteem edastab automatiseeritud eelteavitusi volitatud töötleja kasutaja elektronposti aadressil vastavalt volitatud töötleja pädevusele ja seadistustele infosüsteemis.

(2) Infosüsteemi eelteavitused sisaldavad informatsiooni volitatud töötleja täitmist ootavatest ülesannetest ning jälitustoiminguga seotud toimingu tähtpäeva saabumise kohta. Infosüsteemi eelteavituse edastamise aja enne tähtpäeva saabumist või ülesande täitmise kohustuse saabumist saab infosüsteemis seadistada volitatud kasutaja.

(3) Infosüsteemi sisenemisel on volitatud töötleja töölaual nähtav pädevusekohane teostamiseks edastatud ja ootel olevate tegevuste loetelu.

§ 14. Infosüsteemi kannete tegemise nõuded

(1) Volitatud töötleja vastutab andmete sisestamisel infosüsteemi sisestatavate andmete tegelikkusele vastavuse eest.

(2) Volitatud töötleja teeb pädevusekohased kanded või toimingud infosüsteemis esimesel võimalusel, järgides kriminaalmenetluse seadustiku 3^1. peatükis sätestatud tähtaegu ning arvestusega, et iga toiming või kanne infosüsteemis on seotud sellele eelneva kande või toiminguga.

(3) Kinnitatud, digiallkirjastatud või edastatud kandeid saab infosüsteemis muuta ja kustutada volitatud töötleja taotlusel ainult haldur.

(4) Kui kannet ei ole tehnilise takistuse tõttu võimalik teha lõikes 2 nimetatud tähtajal, siis tehakse see viivitamata pärast takistuse kõrvaldamist, olles takistuse ilmnemisel teavitanud kohe vastavalt § 5 lõike 2 punktile 7 haldurit.

§ 15. Infosüsteemi sisestatavad andmed

(1) Infosüsteemi sisestatakse dokumendid ja toimingute andmed, mis seonduvad kriminaalmenetluse seadustiku 3^1. peatükis sätestatud jälitustoimingute tegemisega, vastavalt §-des 16–18 sätestatud pädevusele.

(2) Infosüsteemi sisestatakse järgmised dokumendid:
1) jälitustoimingu tegemise luba;
2) jälitustoimingu tegemise taotlus;
3) jälitustoimingu tegemise loa tühistamise määrus;
4) jälitustoimingu tegemise loast keeldumise kohtumäärus;
5) jälitustoimingu tegemise pikendamise luba;
6) jälitustoimingu tegemise pikendamise taotlus;
7) jälitustoimingu tegemise pikendamisest keeldumise kohtumäärus;
8) jälitustoimingust teavitamata jätmise luba;
9) jälitustoimingust teavitamata jätmise pikendamise taotlus;
10) jälitustoimingust teavitamata jätmise pikendamisest keeldumise kohtumäärus;
11) jälitustoimingust teavitamise teade.

(3) Lõikes 2 loetletud dokumente on võimalik luua infosüsteemi täisdigitaalses keskkonnas. Võimalik on ka laadida üles varem koostatud dokumendifailid ja need infosüsteemis allkirjastada.

(4) Infosüsteemis dokumendi loomisel kasutatakse eeltäidetud andmetega dokumentide malle.

§ 16. Uurimisasutuste tegevused infosüsteemis

(1) Uurimisasutustel on õigus juurdepääsuks infosüsteemis sisalduvatele andmetele ja nende töötlemiseks muul viisil käesolevas paragrahvis sätestatud ulatuses, arvestades kriminaalmenetluse seadustiku 3^1. peatükis vaid jälitusasutustele antud pädevusest tulenevaid piiranguid.

(2) Uurimisasutuste õigus juurdepääsuks infosüsteemile ja andmetöötluseks selles on alljärgnev:
1) uurimisasutuse juht või tema poolt volitatud töötaja lisab infosüsteemi ja eemaldab sealt uurimisasutuse kasutajaid, määrab järelevalvepädevusega ametniku või ametnikud, tal on juurdepääs kõigile tema juhitava asutuse menetletavatele digitaalsetele jälitustoimikutele ning õigus andmetöötluseks ja kannete tegemiseks kõigis tema juhitava asutuse menetletavates digitaalsetes jälitustoimikutes;
2) teenistuslikku järelevalvet teostav ametnik lisab infosüsteemi ja eemaldab sealt uurimisasutuse kasutajaid, tal on juurdepääs kõigile konkreetse uurimisasutuse menetletavatele digitaalsetele jälitustoimikutele järelevalveks vajalikus mahus ning õigus andmetöötluseks ja kannete tegemiseks vaid temale nähtavaks tehtud digitaalsetes jälitustoimikutes;
3) Justiits- ja Digiministeeriumi vanglate osakonna asekantsler võib määrata vanglate osakonna järelevalvepädevusega ametniku või ametnikud, kellel on punktis 2 nimetatud pädevus lisaks vanglate osakonna menetletavatele digitaalsetele jälitustoimikutele ka vanglate menetletavates digitaalsetes jälitustoimikutes; [RT I, 30.12.2024, 1- jõust. 01.01.2025, Vabariigi Valitsuse seaduse § 105.19 lõike 12 alusel asendatud sõna „Justiitsministeerium" sõnadega „Justiits- ja Digiministeerium" vastavas käändes]
4) uurimisasutuse üksuse juht lisab infosüsteemi ja eemaldab sealt tema juhitava üksuse uurimisasutuse kasutajaid, tal on juurdepääs kõigile tema juhitava üksuse kasutajate digitaalsetele jälitustoimikutele ning õigus andmetöötluseks ja kannete tegemiseks neis;
5) uurimisasutuse menetlejal on õigus andmetöötluseks, kannete tegemiseks ning juurdepääsu andmiseks ja lõpetamiseks teisele uurimisasutuse menetlejale üksnes digitaalsete jälitustoimikute puhul, millele talle on antud juurdepääs.

(3) Uurimisasutus sisestab infosüsteemi andmed konkreetse jälitustoimingu loa alusel tehtud jälitustoimingu kohta järgmiselt:
1) viivitamata jälitustoimingu tegemise alguse kuupäeva;
2) jälitustoimingu lõpu kuupäeva hiljemalt jälitustoimingu lõpetamisel;
3) põhjenduse jälitustoimingu tegemata jätmise kohta;
4) kahe kuu jooksul pärast jälitustoimingu lõppu isikute kohta, kelle suhtes jälitustoiming tehti, ja tuvastatud isikute kohta, kelle perekonna- või eraelu puutumatust jälitustoiminguga oluliselt riivati;
5) jälitustoimingu tegemise teate koostamise ja saatmise aja ja viisi ning viite dokumendihaldussüsteemi registreerimisnumbrile;
6) jälitustoiminguga kogutud andmete andmesubjektile tutvustamise aja ja koha.

(4) Lõike 3 punktis 4 nimetatud isikute kohta sisestatakse infosüsteemi isiku ees- ja perekonnanimi ning isikukood.

(5) Jälitustoimingu tegemise pikendamise korral sisestab jälitusasutus lõikes 3 loetletud andmed infosüsteemi ka pikendamise loa alusel tehtud jälitustoimingu kohta.

(6) Kriminaalmenetluse seadustiku § 126^2lõigete 7 ja 8 alusel tehtud jälitustoimingute korral sisestab jälitustoimingu teinud uurimisasutus infosüsteemi käesoleva paragrahvi lõike 3 punktides 1–3 loetletud andmed ja jälitustoimingut taotlenud uurimisasutus käesoleva paragrahvi lõike 3 punktides 4–6 loetletud andmed.

§ 17. Prokuratuuri tegevused infosüsteemis

(1) Prokuratuuri õigus juurdepääsuks infosüsteemis sisalduvatele andmetele ja nende töötlemiseks on alljärgnev:
1) riigi peaprokurör või tema poolt volitatud töötaja lisab infosüsteemi ja eemaldab sealt prokuratuuri kasutajaid, volitab järelevalvepädevusega ametniku või ametnikud, tal on juurdepääs kõigile prokuratuuri menetletavatele digitaalsetele jälitustoimikutele ning õigus andmetöötluseks ja kannete tegemiseks kõigis prokuratuuri menetletavates digitaalsetes jälitustoimikutes;
2) Riigiprokuratuur lisab infosüsteemi ja eemaldab sealt prokuratuuri kasutajaid, tal on juurdepääs kõigile jälitustoimikutele järelevalve teostamiseks vajalikus mahus ning õigus andmetöötluseks ja kannete tegemiseks vaid temale nähtavaks tehtud digitaalsetes jälitustoimikutes;
3) juhtivprokurör lisab infosüsteemi ja eemaldab sealt tema juhitava ringkonnaprokuratuuri kasutajaid, tal on juurdepääs kõigile tema juhitava ringkonnaprokuratuuri kasutajate digitaalsetele jälitustoimikutele ning õigus andmetöötluseks ja kannete tegemiseks neis;
4) menetlust juhtival prokuröril on juurdepääs ainult tema enda alustatud jälitustoimikutele ja õigus andmetöötluseks neis, ta annab ja lõpetab digitaalsele jälitustoimikule juurdepääsu õiguse uurimisasutuse menetlejale ja teisele prokurörile.

(2) Prokuratuur volitatud töötlejana sisestab infosüsteemi § 15 lõikes 2 nimetatud dokumendid, mille on koostanud prokuratuur, ning otsuse selle kohta, millist isikut tuleb tehtud jälitustoimingust teavitada.

(3) Igale prokuratuuri poolt sisestatud dokumendile antakse infosüsteemis unikaalne number.

§ 18. Kohtu tegevused infosüsteemis

(1) Kohus lahendab jälitustoimingutega seoses talle infosüsteemi kaudu prokuratuuri poolt edastatud taotlused ning teostab infosüsteemis sellega seonduva andmetöötluse.

(2) Kohtunikul on õigus juurdepääsuks digitaalsele jälitustoimikule ja andmetöötluseks selles § 15 lõike 2 punktides 2, 6 ja 9 nimetatud taotluse alusel, mis on esitatud asjaomasele kohtule.

(3) Kohtu esimees sisestab infosüsteemi kasutajatena eeluurimiskohtunikud, kes on määratud tööjaotusplaaniga jälitustoiminguks luba andma. Kohtu esimehel ei ole juurdepääsu jälitustoimikutele.

(4) Kohus volitatud töötlejana sisestab infosüsteemi § 15 lõikes 2 nimetatud dokumendid, mille on koostanud kohus. Igale kohtu poolt sisestatud dokumendile antakse infosüsteemis unikaalne number.

§ 19. Digitaalse jälitustoimiku alustamine ja lõpetamine

(1) Digitaalse jälitustoimiku alustab menetlust juhtiv prokurör jälitustoimingute tegemise vajaduse tõttu.

(2) Prokurör lõpetab digitaalse jälitustoimiku, kui jälitustoimingute tegemise vajadus on lõppenud ning § 16 lõike 3 punktis 4 nimetatud isikuid on teavitatud tehtud jälitustoimingutest või on võetud vastu otsus teavitamata jätmise kohta.

(3) Lõpetatud digitaalses jälitustoimikus on prokuratuuril pädevus andmetöötluseks kriminaalmenetluse seadustiku §-des 126^{13}ja 126^{14}sätestatud korras teavitamise otsustamiseks või kohtule taotluse esitamiseks teavitamata jätmise tähtaja pikendamise loa saamiseks.

(4) Lõpetatud digitaalsele jälitustoimikule lisatakse infosüsteemis märge „Lõpetatud“.

5. peatükk
ANDMETE SÄILITAMINE JA INFOSÜSTEEMI LIKVIDEERIMINE

§ 20. Infosüsteemi sisestatud andmete säilitamine

(1) Jälitustoimingu kohta infosüsteemi sisestatud andmete säilitamisel juhindutakse kriminaalmenetluse seadustiku § 126^{12}lõigetes 2, 5 ja 8 sätestatust.

(2) Digitaalse jälitustoimiku andmed kustutatakse infosüsteemist, kui vastav jälitustoimik kuulub kriminaalmenetluse seadustiku § 126^{12}kohaselt hävitamisele.

§ 21. Infosüsteemi likvideerimine

Infosüsteemi likvideerimise otsustab Vabariigi Valitsus seaduse alusel.

6. peatükk
RAKENDUSSÄTTED

§ 22. Rakendussäte

Infosüsteemi sisestatakse alates 1. septembrist 2015. a avatud jälitustoimikutes koostatud dokumendid ja tekkinud andmed.

§ 23. Määruse jõustumine

Määrus jõustub 1. septembril 2015. a.