21.09.2026

Justiits- ja digiministri määruse „Sihipärase turvaauditi korraldamise täpsemad tingimused ja kord“ eelnõu SELETUSKIRI

1. Sissejuhatus

1.1. Sisukokkuvõte

Küberturvalisuse 2. direktiiv ehk NIS2-direktiiv võeti suuremas osas üle küberturvalisuse seaduse ja teiste seaduste muutmise seadusega (küberturvalisuse 2. direktiivi ülevõtmine (eelnõu nr 739 SE)) (edaspidi *ülevõtmisseadus*). Kommenteeritava eelnõuga kavandatakse üle võtta NIS2-direktiivi artikli 32 lõike 2 esimese lõigu punkt b ja kolmas lõik ning artikli 33 lõike 2 punkt b ja kolmas lõik osas, mida ei reguleerita küberturvalisuse seadusega ega muude õigusaktidega.
Viidatud artiklite kohaselt teeb auditit sõltumatu organ või NIS2-direktiivi artikli 8 kohane pädev asutus, selle tulemused tehakse pädevale asutusele kättesaadavaks, ning sõltumatu organi tehtava sihipärase turvaauditi kulud tasub auditeeritav üksus, välja arvatud igakülgselt põhjendatud juhtudel, kui pädev asutus otsustab teisti. Eelnõukohase määruse tähenduses on pädev asutus Riigi Infosüsteemi Amet.

Eelnõukohase määrusega sätestatakse sihipärase turvaauditi korraldamise täpsemad tingimused ja kord, sealhulgas põhjendatud juhud, millal Riigi Infosüsteemi Amet hüvitab teenuseosutajale sihipärase turvaauditi kulu. Samuti sätestatakse mainitud kulu hüvitamise kord. Määruse eesmärk on toetada küberturvalisuse taseme parandamist, kehtestades sihipäraste turvaauditite korraldamise ja auditikulude hüvitamise korra. Sihipärane turvaaudit aitab suurendada turvalisust ja tagada ühiskonna toimimise seisukohast kriitiliste teenuste toimepidavust.

Teenuseosutajatele (auditeeritavatele asutustele ja ettevõtjatele) tähendab määrus teatavat kulu hüvitamise protsessiga kaasnevat täiendavat töö- või halduskoormust. Teisalt on puudutatud isikute ring väike – sihipärane turvaaudit on järelevalve meede, mida pädev asutus kasutab vajaduse korral, mitte igas järelevalveprotsessis ning hüvitist saavad taotleda vaid piiratud hulk üksuseid. Seetõttu on määrusega kaasnev täiendav halduskoormus piiratud. Riigi Infosüsteemi Ametile toob määrus kaasa olemasoleva järelevalveülesande täpsustamise koos teatava töökoormusega. Kuna ülevõtmisseadus suurendas halduskoormust (küberturvalisuse seaduse kohaldamisala täiendati uute subjektidega, kes peavad seaduse nõudeid täitma), tasakaalustati seda halduskoormuse tõusu Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muudatustega. Need muudatused jõustusid 1. oktoobril 2025. See tasakaalustus kehtib ka nende kõnesoleva määruse kohaldamisalasse kuuluvate teenuseosutajate halduskoormuse kohta, kes soovivad esitada kulu hüvitamise taotluse. Eelnõukohase määrusega kaasnevat lisanduvat halduskoormust tasakaalustavad nimetatud muudatused, millega vähendati teenuseosutajate regulatiivset koormust.

1.2. Eelnõu ettevalmistaja

Eelnõu ja seletuskirja on koostanud Justiits- ja Digiministeeriumi riikliku küberturvalisuse talituse küberturvalisuse õigusnõunik Raavo Palu (raavo.palu@justdigi.ee). Eelnõu ja seletuskirja on keeleliselt toimetanud sama ministeeriumi õiguspoliitika osakonna õigusloome korralduse talituse toimetaja Merike Koppel (merike.koppel@justdigi.ee).

1.3. Märkused

Eelnõu on seotud küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõuga nr 739 SE.[1]

Eelnõukohase määrusega võetakse üle Euroopa Parlamendi ja nõukogu 14. detsembri 2022. a direktiivi (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152) (edaspidi ka *NIS2-direktiiv*), artikli 32 lõike 2 esimese lõigu punkt b ja kolmas lõik ning artikli 33 lõike 2 punkt b ja kolmas lõik.

Eelnõu on seotud 2025.–2027. aasta koalitsioonileppe riigikaitse ja julgeoleku valdkonna eesmärgiga „[tagada] Eesti digiühiskonna [toimepidevus] nii, et teenused on küberturvaliselt kättesaadavad igas olukorras“ ning tõhusa asjaajamise valdkonna eesmärgiga „[võtta] Euroopa Liidu [õigus] üle Eestile sobivaimal moel ja [teha] Euroopas ettepanekud sobimatute normide muutmiseks, sealhulgas ettepanek lükata edasi [kestlikkusaruannete] esitamine ja muuta need vabatahtlikuks“.[2] Eelnõu väljatöötamise alus on Vabariigi Valitsuse tegevusprogrammi 2023–2027 ELi direktiivide valdkonna all nimetatud ülesanne „Eelnõu direktiivi (EL) 2022/2555 ülevõtmiseks (küberturvalisuse 2. direktiiv)“.

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb neljast paragrahvist.

Paragrahviga 1 sätestatakse reguleerimis- ja kohaldamisala.
Lõige 1 sätestab, et määrusega reguleeritakse sihipärase turvaauditi korraldamist, mida võidakse kasutada riikliku ja haldusjärelevalve menetluses. Termin „sihipärane turvaaudit“ on defineeritud küberturvalisuse seaduse § 2 punktis 26 kui „võrgu- ja infosüsteemi andmike ja toimingute sõltumatu läbivaatus ning uurimine, et kontrollida võrgu- ja infosüsteemi turvameetmete adekvaatsust ning vastavust kehtivale infoturvapoliitikale ja tööprotseduuridele, avastada turvarikkeid ning soovitada võimalikke järelduvaid meetme-, poliitika- ja protseduurimuudatusi“. Riigikogus menetletava eelnõuga[3] kavandatakse asendada selles punktis kasutatud termin „sihipärane turvaaudit“ terminiga „turvaaudit“, kuid selle sisu ei muutu.

[1] Eelnõude infosüsteemi toimikud 24-1266 ja 25-0926. Riigikogu menetluses olnud eelnõu: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/4429a2b9-e6e2-41cf-991d-f6955c6c4a69/kuberturvalisuse-seaduse-ja-teiste-seaduste-muutmise-seadus-kuberturvalisuse-2.-direktiivi-ulevotmine/.
[2] https://valitsus.ee/valitsuse-eesmargid-ja-tegevused/valitsemise-alused/koalitsioonilepe-2025-2027
[3] Küberturvalisuse seaduse muutmise seadus (eelnõu 897 SE): https://www.riigikogu.ee/tegevus/eelnoud/eelnou/35bbbf88-078f-4da1-a87f-0bde32b0129f/kuberturvalisuse-seaduse-muutmise-seadus/.

Lõike 2 kohaselt sätestatakse määruses sihipärase turvaauditi korraldamise täpsemad tingimused ja kord, sealhulgas põhjendatud juhud, mille puhul Riigi Infosüsteemi Amet hüvitab teenuseosutajale sihipärase turvaauditi kulu. Samuti sätestatakse eelnõukohases määruses selle kulu hüvitamise kord.
Kommenteeritav paragrahv põhineb ülevõtmisseaduse kohases küberturvalisuse seaduses ette nähtud volitusnormidel – vt selle seaduse § 16 lõike 1^1 punkt 2 ja lõige 1^2 ning § 17 lõike 1^1 punkt 2 ja lõige 1^2:
§ 16. Riikliku järelevalve erisused
(1^1) Riigi Infosüsteemi Ametil on riikliku järelevalve ülesannete täitmisel õigus teha: ..
2) teenuseosutaja suhtes sihipäraseid turvaauditeid, mis põhinevad Riigi Infosüsteemi Ameti või auditeeritava teenuseosutaja tehtud riskihindamisel või muul kättesaadaval riskiteabel ning mille kulu kannab muudel kui käesoleva paragrahvi lõike 1^2 alusel kehtestatud määruses nimetatud juhtudel teenuseosutaja; ..
(1^2) Käesoleva paragrahvi lõike 1^1 punktis 2 nimetatud sihipärase turvaauditi korraldamise täpsemad tingimused ja korra, sealhulgas loetelu olukordadest, mille puhul Riigi Infosüsteemi Amet hüvitab teenuseosutajale turvaauditi kulu, ning turvaauditi kulu hüvitamise korra sätestab riikliku küberturvalisuse valdkonna eest vastutav minister määrusega.
§ 17. Haldusjärelevalve meetmed
(1^1) Riigi Infosüsteemi Ametil on haldusjärelevalve ülesannete täitmisel õigus teha: ..
2) teenuseosutaja suhtes sihipäraseid turvaauditeid, mis põhinevad Riigi Infosüsteemi Ameti või auditeeritava teenuseosutaja tehtud riskihindamisel või muul kättesaadaval riskiteabel ning mille kulu kannab muudel kui käesoleva paragrahvi lõike 1^2 alusel kehtestatud määruses nimetatud juhtudel teenuseosutaja; ..
(1^2) Käesoleva paragrahvi lõike 1^1 punktis 2 nimetatud sihipärase turvaauditi korraldamise täpsemad tingimused ja korra, sealhulgas loetelu olukordadest, mille puhul Riigi Infosüsteemi Amet hüvitab teenuseosutajale turvaauditi kulu, ning turvaauditi kulu hüvitamise korra sätestab riikliku küberturvalisuse valdkonna eest vastutav minister määrusega.

Paragrahvis 2 sätestatakse sihipärase turvaauditi korraldamise täpsemad tingimused ja kord.

Lõige 1 sätestab sihipärase turvaauditi korraldamise üldised tingimused. Üksusel on kohustus läbida sihipärane turvaaudit, kui selle näeb järelevalve menetluse raames ette Riigi Infosüsteemi Amet oma haldusaktiga. Haldusaktis määratakse seejuures kindlaks auditi käsitlusala. Vastav haldusakt tehakse teenuseosutajale teatavaks.

Lõikes 2 sätestatakse, et sihipärast turvaauditit teeb teenuseosutajaväline sõltumatu isik.
Sellega võetakse üle ka NIS2-direktiivi artikli 32 lõike 2 esimese lõigu punkt b (*[l]iikmesriigid tagavad, et pädevatel asutustel on elutähtsate üksustega seotud järelevalveülesannete täitmisel nende üksuste suhtes vähemalt järgmised õigused: .. b) teha korrapäraseid ja sihipäraseid turvaauditeid, mida teeb sõltumatu organ või pädev asutus*) ja artikli 33 lõike 2 esimese lõigu punkt b (*(l)iikmesriigid tagavad, et pädevatel asutustel on oluliste üksustega seotud järelevalveülesannete täitmisel kõnealuste üksuste suhtes vähemalt järgmised õigused: .. b) teha sihipäraseid turvaauditeid, mida teeb sõltumatu organ või pädev asutus*). Eelviidatud NIS2-direktiivi sätetes on pädevat asutust ja sõltumatut organit nimetatud justkui alternatiividena. Küberturvalisuse seaduses on käsitletud pädeva asutuse (Riigi Infosüsteemi Amet – vt küberturvalisuse seaduse § 16 lõike 1^1 sissejuhatav lauseosa ja 17 lõike 1^1 sissejuhatav lauseosa) tehtavat sihipärast turvaauditit, mille puhul ei ole ette nähtud hüvitamise kohustust. Eelnõukohase määrusega reguleeritakse olukord, mil sihipärast turvaauditit teeb NIS2-direktiivi artikli 32 lõike 2 ja artikli 33 lõike 2 tähenduses „sõltumatu organ“, mille puhul jääb auditiga seotud kulu üldjuhul teenuseosutaja kanda.

Eelnõukohases määruses võetakse termini „sõltumatu organ“ asemel kasutusele termin „teenuseosutajaväline sõltumatu isik“ ja selle lühendtermin „audiitor“.
Sõltumatu isik tähendab teenuseosutajast sõltumatut isikut. Audiitor ei ole teenuseosutajast sõltumatu, kui ta on teenuseosutaja kasutatava võrgu- ja infosüsteemi arendaja või väljatöötaja. Samuti ei peeta sõltumatuks isikut, kes nõustab teenuseosutajat küberturvalisuse meetmete rakendamisel. Sihipärane audit sarnaneb oma olemuselt teenuseosutaja suhtes tehtava välise auditiga. Seetõttu on sätestatud, et tegemist on teenuseosutajavälise isikuga. Isiku all on mõeldud füüsilist või juriidilist isikut.
Audiitoril peab auditi tegemise ajal olema kehtiv rahvusvaheliselt tunnustatud infosüsteemide audiitori kutsetunnistus või tehnilist kvalifikatsiooni tõendav muu dokument. Viidatud kutsetunnistuse all on mõeldud üht järgmist kehtivat kutsetunnistust: 1) ülemaailmse IT-professionaale ühendava organisatsiooni ISACA välja antud infosüsteemide audiitori (ingl *Certified Information Systems Auditor*, lühend *CISA*) kutsetunnistus; 2) kvaliteediinstituudi (ingl *Chartered Quality Institute*) rahvusvahelise kutsetunnistusega audiitorite registri (ingl *International Register of Certificated Auditor*s, lühend *IRCA*) välja antud infoturbe halduse süsteemide ISO/IEC 27001 kohase sertifitseerimisskeemi põhine juhtivaudiitori kutsetunnistus; 3) ametialase hindamise ja kutsetunnistuste andmise nõukogu PECB välja antud infoturbe halduse süsteemide ISO/IEC 27001 kohase sertifitseerimisskeemi põhine juhtivaudiitori kutsetunnistus. Audiitoril võib olla ka muu tehnilist kvalifikatsiooni tõendav dokument, kui auditit teeb tehniline ekspert, kellel on auditi käsitlusalale vastav tehniline kvalifikatsioon või töökogemus. See isik võib teha sihipärast turvaauditit, kui auditi käsitlusala võib olla väga kitsas ja/või väga spetsiifiline ning kompetents ette nähtud asjaolusid auditeerida võib olla just tehnilisel eksperdil.

Lõikega 3 võetakse üle NIS2-direktiivi artikli 32 lõike 2 esimese lõigu punkt b (*[l]iikmesriigid tagavad, et pädevatel asutustel on elutähtsate üksustega seotud järelevalveülesannete täitmisel nende üksuste suhtes vähemalt järgmised õigused: .. b) teha korrapäraseid ja sihipäraseid turvaauditeid, mida teeb sõltumatu organ või pädev asutus*). Kuigi sihipäraseid turvaauditeid tuleb teha ka oluliste üksuste suhtes (vt NIS2-direktiivi artikli 33 lõike 2 esimese lõigu punkt b), on direktiivis siiski ainult üliolulistе üksuste puhul märgitud, et need auditid peavad olema regulaarsed (ingl *regular*). Eelnõukohases määruses kasutatakse selle sätestamiseks sõna „korduvalt“. Kommenteeritavas punktis on kasutatud sõnastust „võib .. ette näha“, et tagada paindlikkus nii teenuseosutaja kui ka Riigi Infosüsteemi Ameti jaoks.

Lõikega 4 sätestatakse teenuseosutaja kohustus kooskõlastada audiitorivalik Riigi Infosüsteemi Ametiga. Sätte eesmärgiks on tagada, et sihipärast turvaauditit teeb selleks pädev isik ning teenuseosutaja ei satuks olukorda, kus audit ei vasta nõuetele audiitori puuduliku kompetentsi tõttu. Auditeeritavale teenuseosutajale jäetakse vabadus valida audiitor eeldusel, et ta vastab määruses sätestatud tingimustele (vt sama paragrahvi lõike 2 selgitusi).
Nõuetele vastavust kontrollib Riigi Infosüsteemi Amet enne sihipärase turvaauditi tegemist. Auditeeritav teenuseosutaja esitab ametile välja valitud audiitori nime ja lõikes 2 ette nähtud dokumendi. Selleks dokumendiks on sõltuvalt sihipärase turvaauditi käsitlusala spetsiifikast kas vastava audiitori kutsetunnistus või tehnilist kvalifikatsiooni tõendav muu dokument. Teenuseosutaja esitab Riigi Infosüsteemi Ametile enne auditeerimise teenuse osutamise lepingu sõlmimist kas ühe või mitu dokumenti (sõltuvalt konkreetse audiitori pädevuse tõendamise vajadusest).
Auditeeritav teenuseosutaja sõlmib valitud audiitoriga auditeerimislepingu vaid juhul, kui valitud audiitori kohta esitatud kutsetunnistus või kvalifikatsiooni tõendav muu dokument võimaldab veenduda, et audiitor on kvalifitseeritud tegema ettekirjutuses sätestatud käsitusalaga auditit. Kui selles ollakse veendunud, teeb Riigi Infosüsteemi Amet positiivse

otsuse. Vastava otsuse tegemiseks on aega kuni kümme tööpäeva. Kui teenuseosutaja sõlmib lepingu enne vastava kinnituse saamist, riskib ta võimalusega, et Riigi Infosüsteemi Amet ei aktsepteeri sihipärase turvaauditi tulemusi haldusakti täitmise kontrollimisel, sest auditit pole teinud nõuetele vastav isik. Samuti ei ole auditeeritaval teenuseosutajal sellisel juhul võimalik taotleda sihipärase turvaauditi kulu hüvitamist, kuna eelnõukohase määruse § 3 lõige 6 näeb ette, et kulude hüvitamist saab taotleda vaid juhul, kui sihipärane turvaaudit vastab §-s 2 sätestatud tingimustele.

Lõikega 5 võetakse üle NIS2-direktiivi artikli 32 lõike 2 kolmanda lõigu esimene lause (*[s]ihipärase turvaauditi tulemused tehakse kättesaadavaks pädevale asutusele*) ja artikli 33 lõike 2 kolmanda lõigu esimene lause (*[s]ihipärase turvaauditi tulemused tehakse pädevale asutusele kättesaadavaks*). Kommenteeritava lõikega nähakse ette kohustus teha auditi tulemused Riigi Infosüsteemi Ametile teatavaks ilma viivituseta, kuid hiljemalt viie tööpäeva pärast. Sätte eesmärk on vältida järelevalvemenetluse põhjendamatut venimist, kuna teenuseosutaja ei edasta sihipärase turvaauditi tulemusi Riigi Infosüsteemi Ametile.

Lõige 6 sätestab, et sihipärase turvaauditi kulu arvestus peab olema arusaadav, õige, üksikasjalik ja järjepidev. Kommenteeritava lõike tulemusena peab olema arusaadav, mis laadi kulu on tekkinud, kantud kulu arvestus peab olema õige ning kirja pandud piisava detailsusega, st olema üksikasjalik ja järjepidev. Säte rajaneb kohtuekspertiisiseaduse[4] § 37 lõikel 2.

Paragrahvis 3 sätestatakse teenuseosutaja kulu hüvitamise tingimused.

Lõikes 1 sätestatakse üldreegel, mille kohaselt kannab sihipärase turvaauditi kulu auditeeritav teenuseosutaja. Säte on kooskõlas NIS2-direktiivi artikli 32 lõike 2 kolmanda lõigu teise lause (*[s]õltumatu organi poolt läbi viidava sihipärase turvaauditi kulud tasub auditeeritud üksus, välja arvatud igakülgselt põhjendatud juhtudel, kui pädev asutus otsustab teisiti*) ja artikli 33 lõike 2 kolmanda lõigu teise lausega (*[s]õltumatu organi poolt läbi viidava sihipärase turvaauditi kulud tasub auditeeritud üksus, välja arvatud igakülgselt põhjendatud juhtudel, kui pädev asutus otsustab teisiti*).

Lõikes 2 sätestatakse põhjendatud juhud, millal Riigi Infosüsteemi Amet hüvitab teenuseosutajale sõltumatu organisatsiooni tehtud sihipärase turvaauditi kulu. Tegemist on erandiga lõikes 1 sätestatud üldreeglist. Säte on kooskõlas NIS2-direktiivi artikli 32 lõike 2 kolmanda lõigu teise lause (*[s]õltumatu organi poolt läbi viidava sihipärase turvaauditi kulud tasub auditeeritud üksus, välja arvatud igakülgselt põhjendatud juhtudel, kui pädev asutus otsustab teisiti*) ja artikli 33 lõike 2 kolmanda lõigu teise lausega (*[s]õltumatu organi poolt läbi viidava sihipärase turvaauditi kulud tasub auditeeritud üksus, välja arvatud igakülgselt põhjendatud juhtudel, kui pädev asutus otsustab teisiti*).
Sihipärase turvaauditi kulu hüvitamist saavad taotleda lõikes 3 nimetatud teenuseosutajad kahel alternatiivsel alusel: 1) teenuseosutaja tõendab, et ta ei ole võimeline sihipärase turvaauditi kulu ise kandma; või 2) varasem sihipärane turvaaudit tehti viimase 12 kuu jooksul ning selle käigus tuvastatud puudused on uue sihipärase turvaauditi määramise ajaks kõrvaldatud. Esimesel juhul saab kulu hüvitamist taotleda, kui teenuseosutaja on sellises majanduslikus olukorras, et sihipärase turvaauditi tegemise kulu kandmine takistaks oluliselt auditi tulemusel esitatud soovituste elluviimist või järelevalve käigus tuvastatud puuduste kõrvaldamist. Teine alternatiiv on samuti suunatud majandusliku koorma vähendamisele. Kui auditeeritav teenuseosutaja peab lühikese ajavahemiku jooksul korduvalt kandma auditeerimise kulu, võib see mõjuda

[4] Kohtuekspertiisiseadus (RT I, 14.03.2025, 11). https://www.riigiteataja.ee/akt/114032025011

negatiivselt teenuseosutaja majanduslikule võimekusele võtta meetmeid infoturbe parandamiseks. Seega kui teenuseosutaja on täitnud oma kohustused kõrvaldada varasema auditi käigus ilmnenud puudused ning varasem audit tehti viimase 12 kuu jooksul, saab teenuseosutaja samuti taotleda kulude hüvitamist. Vt ka eelnõukohase määruse § 2 lõiget 6.

Lõikes 3 sätestatakse üksuste loetelu, kellel on õigus hüvitist taotleda. Teenuseosutajate loetelu on koostatud ajendatuna Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (edaspidi *määrus nr 121*) § 3 lõikest 2^1 ja § 4 lõikest 4, st eesmärk on lähtuda põhimõtteliselt samadest alustest, mille puhul ei tule teenuseosutajal järgida Eesti infoturbestandardit, sh ka välisauditi läbimise nõuet.
Punkti 1 kohaselt on hüvitise taotlemise õigus teenuseosutajal, kes on väiksem kui keskmise suurusega ettevõtja vastavalt komisjoni soovitusele 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratluse kohta.[5] Ülevõtmisseaduse eelnõu seletuskirjas on küberturvalisuse seaduse § 3 sissejuhatava lauseosa puhul selgitatud eelnimetatud soovituse olemust ja sisu, sh ka seda, kuidas tehakse kindlaks, kas tegemist on keskmise suurusega ettevõtjaga (töötajate arv ja finantsnäitajate arvutamine). Seetõttu seda siin üle ei korrata. Muudatuses ei mainita mikroettevõtjaid,[6] kuid kuna mikroettevõtjale kehtestatud nõuded mahuvad eelviidatud Euroopa Komisjoni soovituse piiridesse (st nad on väiksemad kui keskmise suurusega ettevõtjad), siis kohaldub kommenteeritav punkt ka mikroettevõtja suhtes.
Punktis 2 sätestatakse, et hüvitist saab taotleda teenuseosutajast 1) valla või linna ametiasutus; 2) valla või linna ametiasutuse hallatav asutus; 3) osavalla või linnaosa ametiasutus või hallatav asutus või 4) kohaliku omavalitsuse üksuste ühisamet või -asutus. See punkt rajaneb määruse nr 121 § 4 lõike 4 punktil 2.
Punktis 3 sätestatakse, et hüvitist saab taotleda teenuseosutajast kohaliku omavalitsuse üksuste liit. See punkt rajaneb määruse nr 121 § 3 lõike 2^1 punktil 4, kuid kommenteeritavasse punkti ei ole lisatud ühe kriteeriumina töötajate arvu (50 töötajat). Kohaliku omavalitsuse korralduse seaduse[7] §-de 63–63^4 kohaselt võib moodustada kolme liiki kohaliku omavalitsuse üksuste liite: maakonna omavalitsusüksuste liit, piirkondlik omavalitsusüksuste liit ja üleriigiline omavalitsusüksuste liit. Üleriigilisi liite võib olla vaid üks. Praegu on selleks Eesti Linnade ja Valdade Liit.
Punktis 4 sätestatakse, et hüvitist saab taotleda teenuseosutajast riigimuuseum. See punkt rajaneb määruse nr 121 § 4 lõike 4 punktil 2.
Punktis 5 sätestatakse, et hüvitist saab taotleda teenuseosutajast põhikool või gümnaasium ehk riigikool, kes tegutseb Haridus- ja Teadusministeeriumi hallatava asutusena. Põhikooli- ja gümnaasiumiseaduse[8] § 1 lõike 2 kohaselt reguleerib seadus valla või linna ametiasutuse hallatava asutusena tegutsevate koolide (edaspidi *munitsipaalkool*) ning Haridus- ja Teadusministeeriumi hallatava asutusena tegutsevate koolide (edaspidi *riigikool*) tegevust. Munitsipaalkooli pidajaks on vald või linn. Riigikooli pidajaks on riik. Eraõigusliku juriidilise isiku asutusena tegutsevale koolile (edaspidi *erakool*) kohaldatakse põhikooli- ja gümnaasiumiseadust niivõrd, kuivõrd erakooliseadus ei sätesta teisiti.
Punkides 6 ja 7 nimetatakse eraldi Eesti Lastekirjanduse Keskust ja Võru Instituuti. Nende punktide puhul on võetud eeskuju määruse nr 121 § 4 lõike 4 punktidest 5 ja 6.

---

[5] Komisjoni 6. mai 2003. aasta soovitus 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratluse kohta (ELT L 124. 20.05.2003, lk 36–41). https://eur-lex.europa.eu/eli/reco/2003/361/oj/eng
[6] Mikroettevõtja on ettevõtja, mis annab tööd kuni 10 inimesele ning mille käibe (määratud ajavahemikul saadud raha) või bilansi (ettevõtte varade ja kohustuste aruanne) maht ei ületa 2 miljonit eurot. https://eur-lex.europa.eu/ET/legal-content/summary/micro-small-and-medium-sized-enterprises-definition-and-scope.html
[7] Kohaliku omavalitsuse korralduse seadus (RT I, 10.02.2026, 13). https://www.riigiteataja.ee/et/akt/110022026013
[8] Põhikooli– ja gümnaasiumiseadus (RT I, 09.07.2026, 17). https://www.riigiteataja.ee/et/akt/109072026017

Lõikega 4 tagatakse selgus selles, et sama paragrahvi lõike 3 punktis 1 nimetatud teenuseosutaja puhul ei kohaldata tema töötajate arvu, aastabilansimahu ja aastakäibe kindlakstegemisel komisjoni soovituse 2003/361/EÜ lisa artikli 3 lõiget 4. Kuigi NIS2-direktiivi artikli 2 lõike 1 teine lõik võeti üle ülevõtmisseaduse kohase küberturvalisuse seaduse § 3 lõikega 6, siis kõnesoleva lõikega täpsustatakse, et selle seaduse sättes olev nõue kohaldub ka sihipärase turvaauditi kulu hüvitamisel.
Komisjoni soovituse 2003/361/EÜ lisa artikli 3 lõige 4 kehtestab üldreegli, mille kohaselt ei ole ettevõtja väike ega keskmise suurusega, kui 25% või rohkemat tema kapitalist või hääleõigusest kontrollivad otseselt või kaudselt, ühiselt või üksikult, üks või mitu avaliku sektori organisatsiooni (ingl *controlling public body*). Vt selle kohta ka nimetatud soovituse põhjendus 13:
(13) Vältimaks kunstlikku vahetegemist liikmesriigi erinevate avalik-õiguslike asutuste vahel ja arvestades vajadust õiguskindluse järele, peetakse vajalikuks kinnitada, et VKE ei ole ettevõte, mille kapitalist või hääleõigustest 25% või enam kontrollib avalik-õiguslik asutus.
NIS2-direktiivi artikli 2 lõike 1 teine lõik täpsustab, et viidatud soovituse artikli 3 lõiget 4 ei arvestata NIS2-direktiivi puhul. Kuna küberturvalisuse seadusesse lisati sama nõue, siis selguse huvides lisatakse sarnane nõue ka kõnesolevasse sihipärase turvaauditi määrusesse. Seega on eelnõukohase määruse kohaselt võimalik teenuseosutajat pidada väike- või keskmise suurusega ettevõtjaks, kui seda kontrollib (osaliselt) avaliku sektori organisatsioon, aga ainult siis, kui kommenteeritava paragrahvi lõike 1 punktis 4 nimetatud tingimused (töötajate arv ja finantsnäitajad) on täidetud. NIS2-direktiiv ei näe ette nõudeid selle kohta, kuidas teha kindlaks töötajate arv ja finantsnäitajad avaliku sektori organisatsioonide puhul. Need organisatsioonid kuuluvad NIS2-direktiivi artikli 2 lõike 2 punkti f kohaselt NIS2-direktiivi kohaldamisalasse, olenemata üksuse suurusest. Soovitus 2003/361/EÜ ei ole mõeldud reguleerima seda, kuidas toimida kontrolli omavate avaliku sektori organisatsioonidega, ega sisalda selgeid reegleid selle kohta. Selle soovituse reeglite järgimine kontrolli omavate avaliku sektori organisatsioonide puhul (tuvastamaks nende seost partner- ja sidusettevõtjatega väike- või keskmise suurusega ettevõtjate puhul) tekitaks Euroopa Liidu liikmesriikide seas killustatust ja õiguslikku segadust. Seetõttu ei tule kommenteeritava lõike kohaselt ettevõtjate töötajate arvu ja finantsnäitajate väljaselgitamisel eraldiseisva kontrolli omava avaliku sektori üksuse töötajate arvu ja finantsnäitajaid arvesse võtta. Vt lisaks ülevõtmisseaduse § 3 selgitusi soovituse 2003/361/EÜ kohta.

Lõikes 5 sätestatakse lisareegel teenuseosutaja töötajate arvu, aastakäibe ja aastabilansimahu arvestamise kohta partner- ja sidusettevõtjate puhul. Sellise reegli loomise võimalusele viitab NIS2-direktiivi põhjendus 16, mis on sõnastatud järgmiselt:
(16) Vältimaks seda, et üksusi, millel on partnerettevõtjad või mis on sidusettevõtjad, peetaks elutähtsateks[9] või olulisteks üksusteks, kui see oleks ebaproportsionaalne, on liikmesriikidel võimalik soovituse 2003/361/EÜ lisa artikli 6 lõike 2 kohaldamisel võtta arvesse üksuse oma partneritest või sidusettevõtjatest sõltumatuse määra. Eelkõige on liikmesriikidel võimalik võtta arvesse asjaolu, et üksus on oma partner- või sidusettevõtjatest sõltumatu teenuste osutamisel kasutatavate võrgu- ja infosüsteemide osas, ja teenuste osas, mida üksus osutab. /.../.
Arvestades NIS2-direktiivi ülevõtmise aluseks võetud üldpõhimõtet, et riigisiseselt ei sätestata NIS2-direktiivis ette nähtud miinimumnõuetest rangemaid nõudeid, on kommenteeritavasse lõikesse lisatud NIS2-direktiivi põhjenduses 16 sätestatud võimalus jätta partner- ja sidusettevõtjate töötajate arv ning käive või bilansimaht arvestamata. Sellega tagatakse sarnaste õigusnormide kohaldamine ülevõtmisseaduse kohases küberturvalisuse seaduses kui ka sama seaduse alusel kehtestatud määrustes sätestatud olukordades, st töötajate arvu ja finantsnäitajate

[9] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulisteks“.

arvutamiseks. Kommenteeritavas lõikes ette nähtud välistuse rakendamine on võimalik, kui teenuseosutajal on otsustav mõju enda infotehnoloogiasüsteemide toimimise üle. Teisisõnu, kui ta on enda IT-lahenduste korraldamisel sõltumatu. Selline sõltumatus infotehnoloogiasüsteemide toimimise üle otsustamisel on olemas eelkõige siis, kui teenuseosutaja saab omal vastutusel teha põhilisi otsuseid infotehnoloogiasüsteemide, selle komponentide ja protsesside üle. Kui teenuseosutaja on selliste otsuste tegemisel vaba, siis ei arvestata tema töötajate arvu ning käibe- või bilansinäitajate kindlakstegemisel partner- või sidusettevõtja töötajate arvu, käivet ega bilansimahtu. Kõnealuse välistuse kohaldamine ei tule aga kõne alla juhul, kui IT-lahendusi rakendatakse terves kontsernis ühetaoliselt, näiteks otsustab kõik IT-süsteemidega seotud küsimused emaettevõtja.

Lõikes 6 sätestatakse, et § 2 lõikes 1 nimetatud sihipärase turvaauditi kulu hüvitatakse vaid juhul, kui samas paragrahvis ette nähtud tingimused on täidetud. Kokkuvõtvalt hüvitatakse teenuseosutajale tema kantud kulu täielikult või osaliselt, kui on täidetud järgmised tingimused:

- sihipärane turvaaudit on tehtud eelnõukohase määruse § 2 lõikes 1 nimetatud haldusakti alusel;
- Riigi Infosüsteemi Amet on audiitori sobivuse kinnitanud eelnõukohase määruse § 2 lõikes 4 nimetatud otsusega;
- kulu arvestus vastab eelnõukohase määruse § 2 lõikele 6;
- esineb vähemalt üks eelnõukohase määruse § 3 lõikes 2 nimetatud alus;
- teenuseosutaja on nimetatud eelnõukohase määruse § 3 lõikes 3;
- sihipärase turvaauditi tulemused on tehtud Riigi Infosüsteemi Ametile kättesaadavaks;
- teenuseosutaja on esitanud Riigi Infosüsteemi Ametile kulu hüvitamise taotluse (vt järgmise paragrahvi selgitust).

Paragrahvis 4 sätestatakse teenuseosutaja kulu hüvitamise kord.

Lõikes 1 sätestatakse, et kulu hüvitamise aluseks on teenuseosutaja taotlus, millele tuleb lisada ka andmed eelnõukohase määruse §-des 2 ja 3 sätestatud nõuete täitmise kohta. Sellega tagatakse, et teenuseosutaja ise taotleb aktiivselt oma kulu hüvitamist. Kõnesoleva punkti sõnastamisel on võetud eeskuju tsiviilkohtumenetluse seadustiku[10] § 160 lõikest 1.
Eelnõukohase määruse § 3 lõike 2 esimest alternatiivi ehk oma majanduslikku olukorda saab teenuseosutaja tõendada, esitades asjakohased dokumendid. Viimase 12 kuu jooksul sihipärase turvaauditi läbimise tõendina piisab, kui esitatakse varasem sihipärase turvaauditi aruanne või viidatakse selle esitamisele Riigi Infosüsteemi Ametile. Lisaks on aga vaja esitada tõendid selle kohta, et aruandes toodud puudused on kõrvaldatud ning sobivad tõendid sõltuvad puudustest, mida kõrvaldati.
Paragrahvi 3 lõike 3 kohta käiv kinnitus on vajalik selleks, et veenduda selles, et teenuseosutajal on õigus hüvitist saada. Selle lõike esimese punkti (st kas tegemist on mikro- või väikeettevõtjaga) puhul on esitatud kinnitusele vastavust võimalik kontrollida e-äriregistri vahendusel, kasutades majandusaasta aruandeid ja avaandmeid. Seda kontrolli teostatakse, lähtudes komisjoni soovituse 2003/361/EÜ lisa artikli 4 lõikes 2 ette nähtud võrdlusperioodist (vaadeldav aasta ja kaks sellele eelnenud aastat).
Taotlusele tuleb lisada ka sihipärase turvaauditi kuludokumendid kulude kohta auditi etappide kaupa.

Lõikes 2 sätestatakse teenuseosutaja kohustus esitada Riigi Infosüsteemi Ametile sihipärase turvaauditi kulu tõendavad lisadokumendid ja anda selgitusi. See kohustus tekib juhul, kus

[10] Tsiviilkohtumenetluse seadustik (RT I, 20.06.2026, 21). https://www.riigiteataja.ee/et/akt/120062026021

teenuseosutaja taotlusele lisatud dokumendid ja selgitused ei ole olnud piisavad ning on tekkinud vajadus lisadokumentide või -selgituste järele. Seega oleneb selle lõike kohaldumine asjaolust, kas amet vajab lisadokumente või -selgitusi. Kõnesolev lõige rajaneb kohtuekspertiisiseaduse § 43 lõikel 3.

Lõikes 3 sätestatakse, et Riigi Infosüsteemi Amet teeb hüvitamisele kuuluva summa kindlaks, lähtudes esitatud dokumentidest ja tehtud kulutuste põhjendatusest. Seeläbi kontrollib amet esitatud kuludokumendi või -dokumentide sisu. Sellega tagatakse, et hüvitatav kulu on asjakohane ja seotud sihipärase turvaauditiga. Näiteks ei hüvitata kulu, mis on seotud sihipärase turvaauditi käigus tuvastatud puuduse kõrvaldamisega (näiteks uuendamata jäetud litsentsi asendamine uue litsentsiga). Samuti ei hüvitata auditi kulu õigeaegselt tasumata jätmisest tulenenud viiviseid ja leppetrahve. Lisaks on põhjendatuse arvestamise alusena nimetatud samaväärse auditi turuhind. Riigi Infosüsteemi Ametil on sellest lähtuvalt õigus vähendada hüvitatavat summat, kui auditi hind on selle käsitlusala arvestades selgelt üle turuhinna.

Lõikes 4 sätestatakse kulu osalise hüvitamise alused. Riigi Infosüsteemi Amet võib otsustada kulu hüvitada osaliselt, kui sihipärase turvaauditi käsitlusala on laiem kui haldusaktis määratud käsitlusala. Juhul kui teenuseosutaja soovib lasta sihipärase turvaauditi raames auditeerida ka haldusakti käsitlusala väliseid aspekte, võib ta seda teha, kuid ette nähtud käsitlusala ületava osa kulu ei hüvitata. Teiseks on alust kulu hüvitada vaid osaliselt, kui Riigi Infosüsteemi Ameti hinnangul ei ole auditi kulud piisavalt dokumenteeritud ning on kahtlus, et kulu ei ole käsitlusala arvestades põhjendatud. Kolmandaks on osaline hüvitamine põhjendatud juhul, kui Riigi Infosüsteemi Ameti hinnangul ületab auditi hind oluliselt samaväärse auditi turuhinda. Nimetatud tingimus on kooskõlas ka kommenteeritava paragrahvi lõike 3 esimeses lauses sätestatuga.

Lõikes 5 määratakse kindlaks kulu hüvitamise nõude esitamise tähtaeg (kolm kuud). See tähtaeg hakkab kulgema päevast, mil sihipärase turvaauditi tulemused tehakse Riigi Infosüsteemi Ametile kättesaadavaks. Kui ametile tehakse sihipärase turvaauditi tulemused kättesaadavaks, teavitab amet teenuseosutajat eelmainitud tähtajast ja tähtaja möödumise tagajärgedest. Peamine tagajärg on, et teenuseosutajale ei hüvitata sihipärase turvaauditiga seotud kulu. Vt ka kommenteeritava paragrahvi lõike 6 selgitust. Kõnesolev lõige rajaneb tsiviilkohtumenetluse seadustiku § 160 lõikel 2.

Lõikes 6 sätestatakse, et teenuseosutaja võib nõuda tähtaja ennistamist, kui tal ei olnud võimalik tähtajast mõjuval põhjusel kinni pidada. Sel juhul peab teenuseosutaja selgitama, miks tal ei olnud võimalik taotlust tähtajal esitada. Samas tuleb arvestada, et tähtaja ennistamise taotluse võib esitada kümne tööpäeva jooksul takistuse kõrvaldamisest ja tähtaja ennistamise tingimuste põhistamisest arvates. Kõnesolev lõige rajaneb tsiviilkohtumenetluse seadustiku § 160 lõikel 4.

Lõikes 7 sätestatakse teenuseosutaja kulu hüvitamise nõudeõiguse lõppemise tähtaeg (kuus kuud), mis kehtib ka juhul, kui teenuseosutaja taotleb tähtaja ennistamist. Sellega tagatakse, et kulu hüvitamise nõude esitamiseks on lõplik tähtaeg. Nõue tekib siis, kui Riigi Infosüsteemi Ametile on sihipärase turvaauditi tulemused kättesaadavaks tehtud. Kõnesolev lõige rajaneb tsiviilkohtumenetluse seadustiku § 160 lõikel 5, kuid erinevuseks on tähtaja pikkus.

Lõikes 8 sätestatakse tähtaeg, mille jooksul peab Riigi Infosüsteemi Amet otsustama kulu täieliku või osalise hüvitamise. Seda tuleb teha 20 tööpäeva jooksul alates 1) puudusteta taotluse esitamisest; või 2) kui kommenteeritava paragrahvi lõike 2 kohaselt on küsitud lisadokumente

või -selgitusi. Kui amet jätab tähtaja järgimata, ei tähenda see siiski kulu hüvitamise otsuse vaikimisi andmist, kuivõrd see läheks vastuollu sihipärase turvaauditiga seotud kulu hüvitamise korra mõttega. Sellises olukorras on teenuseosutajal haldusmenetluse ja halduskohtumenetluse seadustikust tulenevad õiguskaitsevahendid vaide ja/või kaebuse esitamiseks.

Lõikega 9 määratakse kindlaks, mis tähtaja jooksul Riigi Infosüsteemi Amet kannab hüvitamisele kuuluva summa üle teenuseosutaja nimetatud pangakontole. Lõige rajaneb kohtuekspertiisiseaduse § 43 lõikel 5.

Määrusele lisatakse normitehniline märkus NIS2-direktiivi kohta.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu järgib NIS2-direktiivi. Eelnõu vastab NIS2-direktiivile ning kuna direktiiv võeti ennekõike üle ülevõtmisseadusega, on selle seaduseelnõu materjalide hulgas ka NIS2-direktiivi ja ülevõtmisseaduse vastavustabel. Siinkohal esitatakse need sätted, mis on seotud kommenteeritava eelnõuga:
1) artikli 32 lõike 2 esimese lõigu punkt b = määruse § 2 lõiked 2 ja 3;
2) artikli 32 lõike 2 kolmanda lõigu esimene lause = määruse § 2 lõige 5;
3) artikli 32 lõike 2 kolmanda lõigu teine lause = määruse § 3 lõiked 1–3 ja 6;
4) artikli 33 lõike 2 esimese lõigu punkt b = määruse § 2 lõike 1 punkt 2;
5) artikli 33 lõike 2 kolmanda lõigu esimene lause = määruse § 2 lõige 5;
6) artikli 33 lõike 2 kolmanda lõigu teine lause = määruse § 3 lõiked 1–3 ja 6.
Iga muudatuse juures on hinnatud muudetava sätte vastavust Euroopa Liidu õigusele, vajaduse korral on toodud ka võimalikud sõnastusalternatiivid.
Kehtiva õiguse suhtes kohaldub ka NIS2-direktiivi artikkel 5, mis näeb ette järgmist: *[NIS2-direktiiv] ei takista liikmesriike tarbijate kaitseks vastu võtmast või kehtima jätmast sätteid, millega tagatakse kõrgem küberturvalisuse tase, tingimusel et sellised sätted on kooskõlas liikmesriikide kohustustega, mis on sätestatud liidu õiguses.*

4. Määruse mõjud

Määrusega luuakse sihipärase turvaauditi korraldamise ning auditikulu hüvitamise tingimused ja kord olukorras, kus auditi läbimise kohustus nähakse ette haldusaktiga. Määrusega kehtestatakse nõuded audiitori sõltumatusele ja pädevusele, audiitori kooskõlastamisele Riigi Infosüsteemi Ametiga, auditi tulemuste esitamisele ning auditikulu hüvitamise taotlemisele ja menetlemisele. Muudatused mõjutavad eelkõige teenuseosutajaid ja Riigi Infosüsteemi Ametit. Mõju avaldub majanduskeskkonnas ja riigivalitsemises. Muudatuste eesmärk on toetada võrgu- ja infosüsteemide turvalisust ning ühiskonna toimimiseks oluliste teenuste toimepidevust, mistõttu võib määrusel olla kaudne positiivne mõju küberturvalisusele ja seeläbi riigi julgeolekule.

4.1. Teenuseosutajad

Mõjuvaldkonnad: majanduskeskkond ja riigivalitsemine

Mõju sihtrühm: teenuseosutajatest ettevõtjad ja avaliku sektori üksused, kelle suhtes Riigi Infosüsteemi Amet teeb ettekirjutuse läbida sihipärane turvaaudit(vastavalt kas riikliku järelevalve menetluses või haldusjärelevalve menetluses), sealhulgas need teenuseosutajad, kellel on õigus taotleda auditikulu hüvitamist. Sel põhjusel hinnatakse nii ettevõtjaid kui ka

avaliku sektori üksuseid ühe sihtrühmana koos, mitte eraldi. Ülevõtmisseaduse seletuskirjas[11] on analüüsitud, kui mitut üksust ülevõtmisseadus mõjutab. Kõnesoleva eelnõuga seotud mõjud võivad avalduda neile kõigile – seda tingimusel, et konkreetse üksuse suhtes kohaldatakse haldusaktiga ette nähtud sihipärast turvaauditit. Sihtrühma täpset suurust ei ole võimalik ette prognoosida, sest sihipärase turvaauditi kohaldamine sõltub Riigi Infosüsteemi Ameti kaalutlusotsusest.

Avalduv mõju ja mõju olulisus:
Sihipärase turvaauditi kui ühe järelevalvemeetme kasutamine on ette nähtud küberturvalisuse seaduses (vt § 16 lg 1^1 punkt 2 ja § 17 lõike 1^1 punkt 2). Tegemist on Riigi Infosüsteemi Ametile antud volitusega, mitte kohustusega vastavat järelevalvemeedet kasutada. Kõnesolev eelnõu ei mõjuta otseselt selle järelevalvemeetme kohaldumist, sealhulgas seda, kas ja millal otsustatakse seda kasutada. Selle meetme kohaldamisel kehtib diskretsiooniõigus, millele kohalduvad haldusmenetluse seaduse nõuded, sh riikliku järelevalve menetluse puhul ka korrakaitseseaduses ette nähtud nõuded. Selle diskretsiooniõiguse kasutamise käigus määratakse haldusaktiga kindlaks sihipärase turvaauditi käsitlusala, st selle küsimused ja teemad, mida audiitor vaatab läbi ja uurib. On keeruline hinnata, kui suured kulud võivad teenuseosutajale tekkida ning millises ulatuses need kulud võidakse hüvitada – see sõltubki paljuski auditi käsitlusalast. Nende kriteeriumitega omakorda tagatakse, et Riigi Infosüsteemi Amet ei kasutaks seda järelevalvemeedet teenuseosutajate suhtes ülemäära tihti. Seda enam, et ametile on antud volitus prioriseerida oma järelevalveülesandeid, arvestades riski- või ohuprognoosipõhist lähenemisviisi (küberturvalisuse seaduse § 14 lõike 6 punkt 1). See prioriseerimine on paljuski seotud ameti enda järelevalveressursside olemasolu ja nende kasutamisega järelevalvemenetlustes.
Eelnõukohase määruse mõju avaldub üksnes järgmistel juhtudel:
1) Riigi Infosüsteemi Amet on otsustanud sihipärast turvaauditit kui järelevalvemeedet kohaldada, kasutades selleks teenuseosutajavälist sõltumatut isikut ehk audiitorit;
2) sihipärase turvaauditi käigus tekib teenuseosutajale kulu;
3) teenuseosutajal on õigus tekkinud kulu eest hüvitist saada (eelnõukohase määruse § 3 lõiked 2 ja 3).

Kõnesoleva eelnõukohase määruse puhul avaldab kõige suuremat mõju kolmas tingimus. Sellest johtuvalt peab õigustatud teenuseosutaja esitama kulu hüvitamise taotluse ja selleks peavad olema ka täidetud eelnõukohase määruse § 4 lõikes 1 ette nähtud tingimused. Taotluse esitamine toob kaasa teatava töö- või halduskoormuse taotluse esitajale. Eeldatavasti on suurim koormus seotud kulu põhjendamise ja tõendamisega. Selle pärast ongi eelnõukohase määruse § 2 lõikega 6 ette nähtud, et sihipärase turvaauditi kulu arvestus peab olema arusaadav, õige, üksikasjalik ja järjepidev ning § 4 lõike 1 punktis 3 on sätestatud nõue, et kuludokumentides peab kajastuma kulu auditi etappide kaupa. Kuna eelnõukohase määruse järgi kasutatakse sihipärase turvaauditi tegemiseks audiitorit, on taotluse esitaja töö- või halduskoormust võimalik vähendada näiteks sellega, et selle audiitori või muu pädeva isiku töö kohta koostatud arve vastab eelnõukohase määruse § 2 lõikele 6 ja § 4 lõike 1 punktile 3.

Järeldus mõju olulisuse kohta: eelnõukohase määruse mõju on seotud kulu hüvitamise taotlemisega kaasneva töö- ja halduskoormusega. Neid kulusid tekitavat järelevalvemeedet (sihipärast turvaauditit) kasutatakse ühe teenuseosutaja suhtes eeldatavasti harva, seega esineb asjaomase töö- või halduskoormusega seotud mõju samuti harva ning ebasoovitavate mõjude avaldumise risk on ka väike.

[11] Vt allviide nr 1, lk-d 163–164.

4.2. Riigi Infosüsteemi Amet

Mõjuvaldkond: riigivalitsemine

Mõju sihtrühm: Riigi Infosüsteemi Amet

Avalduv mõju ja mõju olulisus: eelnõukohane määrus avaldab mõju Riigi Infosüsteemi Ameti töökoormusele, mis on seotud õigustatud teenuseosutajate esitatud kulu hüvitamise taotluste kontrollimise ja maksete tegemisega. See toob kaasa täiendava töökoormuse, sh dokumentide kontrollimise, kulude põhjendatuse hindamise ja väljamaksete tegemise. Teatav mõju avaldub ka teenuseosutaja välja valitud auditi tegija sobilikkuse hindamisega (vt eelnõukohase määruse § 2 lõige 4).
Lisaks avaldub otsene rahaline mõju Riigi Infosüsteemi Ameti eelarvevahenditele seoses määratavate sihipäraste auditite kulu hüvitamisega. Kuna tegemist on uue meetmega, ei ole määruse eelnõu ettevalmistamise ajal Riigi Infosüsteemi Ameti eelarves vastavaid vahendeid ette nähtud. Seega on määrusega kehtestatava korra rakendamise eelduseks täiendavate eelarve vahendite ette nägemine Riigi Infosüsteemi Ametile.
Mõju ulatus sõltub sellest, mil määral ja kui tihti tekib vajadus järelevalve raames sihipärast turvaauditit kasutada ning kui suurel osal neist teenuseosutajatest, kelle suhtes seda meedet kasutatakse, on õigus kulu hüvitamist taotleda ja kui sageli otsustatakse auditikulu osaliselt või täielikult hüvitada.

Järeldus mõju olulisuse kohta:
Mõju töökoormusele on alguses, esimeste sihipärase turvaauditi määramiste ja vastavate kulu hüvitamise taotluste puhul suurem, kuna vastavad protseduurid ei ole veel välja kujunenud, need on vaja välja töötada ja õigustatud teenuseosutajale teatavaks teha. Samas muutub see hiljem igapäevase tööprotsessi osaks. Seetõttu on muudatuse ebasoovitav mõju töökoormusele pikemas perspektiivis väike.
Mõju olulisust rahalistele vahenditele on keeruline hinnata, sest mõju ulatus sõltub sellest, mil määral ja kui tihti tekib vajadus järelevalve raames sihipärast turvaauditit kasutada ning kui suurel osal neist teenuseosutajatest, kelle suhtes seda meedet kasutatakse, on õigus kulu hüvitamist taotleda ja kui sageli otsustatakse auditikulu osaliselt või täielikult hüvitada.

5. Määruse rakendamisega seotud tegevused, vajalikud kulud ja määruse rakendamise eeldatavad tulud

Eelnõukohase määruse rakendamisega ei planeerita tulu.

Riigi Infosüsteemi Ameti kui järelevalveasutuse tegevusi ja kulusid on hinnatud ka ülevõtmisseaduse eelnõu seletuskirjas[12] (vt seletuskirja punkt 7.2), mistõttu selle tulemusi tervikuna siin ei korrata.
Eelnõu määrusena jõustumise korral peab Riigi Infosüsteemi Amet välja töötama kulu hüvitamise taotluste hindamise ja kulu hüvitamise summa ülekandmise protseduurid. Amet saab ka välja töötada kulu hüvitamise taotluse vormi, mis on abiks teenuseosutajale, kes esitab kulu hüvitamise taotluse.
Mõju Riigi Infosüsteemi Ameti eelarvele on keeruline hinnata, kuna see sõltubki ennekõike asjaolust, kui tihti amet haldusaktiga ette nähtavat sihipärast turvaauditit kui järelevalvemeedet

[12] Vt allviide nr 1.

kasutab. Seetõttu tuleb eelnõukohase määrusega seotud ressursse kavandada eelarve planeerimise käigus.

6. Määruse jõustumine

Määrus jõustub üldises korras, kuna tegemist on ülevõtmisseadusest tuleneva rakendusaktiga. Jõustumisaeg on piisav määruse rakendamisega seotud eeltoimingute tegemiseks ja määruse nõuetega tutvumiseks.

7. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Enne eelnõu koostamist toimusid kaasamised seoses NIS2-direktiivi ülevõtmisega. Nende käigus sai anda tagasisidet muu hulgas ka kommenteeritava eelnõuga kavandatavate nõuete kohta. Asjaomase tagasiside leiab ülevõtmisseaduse eelnõu dokumentide juurest.

Eelnõu esitati eelnõude infosüsteemi kaudu kooskõlastamiseks ministeeriumitele, Riigikantseleile ning Eesti Linnade ja Valdade Liidule.

Eelnõu saadeti arvamuse avaldamiseks Riigikogu Kantseleile, Riigikontrollile, Vabariigi Presidendi Kantseleile, Õiguskantsleri Kantseleile, Andmekaitse Inspektsioonile, Eesti Pangale, Riigi Infosüsteemi Ametile, Riigi Info- ja Kommunikatsioonitehnoloogia Keskusele, Registrite ja Infosüsteemide Keskusele, Riigiside Sihtasutusele, Eesti Interneti Sihtasutusele, Finantsinspektsioonile, Eesti Pangaliidule, Eesti Haiglate Liidule, Eesti Arstide Liidule, Eesti Perearstide Seltsile, Eesti Vee-ettevõtete Liidule, Eesti Kiirabi Liidule, Eesti Ravimihulgimüüjate Liidule, Ravimitootjate Liidule, Eesti Proviisorapteekide Liidule, Eesti Apteekrite Liidule, Eesti Elektritööstuse Liidule, Eesti Jõujaamade ja Kaugkütte Ühingule, Eesti Gaasiliidule, Eesti Transpordikütuste Ühingule, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule, Eesti Infosüsteemide Audiitorite Ühingule, Eesti Kaubandus-Tööstuskojale, Eesti Põllumajandus-Kaubanduskojale, Eesti Toiduainetööstuse Liidule ja Eesti Kaupmeeste Liidule.