07.03.2026

Justiits- ja digiministri määruse „Vastastikuse hindamise täpsemad tingimused“ 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))[1] (edaspidi *ülevõtmisseadus*). Selle seletuskirja aluseks oleva eelnõu eesmärk on võtta üle NIS2-direktiivi artikkel 19 osas, mida ei reguleerita küberturvalisuse seadusega ega muude õigusaktidega. Määrusega kehtestatakse kord, mille alusel Eesti saab osaleda Euroopa Liidu tasandil toimuvas küberturvalisuse vastastikuses hindamises. Vastastikune hindamine on mõeldud selleks, et õppida jagatud kogemustest, tugevdada vastastikust usaldust, saavutada küberturvalisuse ühtlaselt kõrge tase ning suurendada liikmesriikide küberturvalisusalast võimekust ja poliitikat, mis on vajalik NIS2-direktiivi rakendamiseks. Määruse eesmärk on võimaldada Eestil osaleda hindamises koos teiste liikmesriikidega ühistel alustel. Samuti sätestatakse, millised asutused vastutavad hindamise korraldamise eest.

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. Määruse rakendamine ei too kaasa uusi kohustusi ettevõtjatele ega elanikele ning halduskoormuse tasakaalustamise reeglit ei ole vaja rakendada. Eelnõu on seotud ennekõike Justiits- ja Digiministeeriumile või tema volitatud asutusele antud ülesande sisustamise ja asjaomase töökoormusega. Riigiasutustele võib lisanduda mõningane töökoormus juhul, kui otsustatakse osaleda Euroopa Liidu liikmesriikide vahelises vastastikuses hindamises.

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] Eelnõude infosüsteemi toimikud 24-1266 ja 25-0926. Riigikogus 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/.

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*), artikkel 19 osas, mida ei reguleerita küberturvalisuse seaduse ega muude õigusaktidega.

Eelnõu on seotud 2025.–2027. aasta koalitsioonileppe riigikaitse ja julgeoleku valdkonna eesmärgiga „tagame Eesti digiühiskonna toimepidevuse nii, et teenused on küberturvaliselt kättesaadavad igas olukorras“ ning tõhusa asjaajamise valdkonna eesmärgiga „võtame Euroopa Liidu õiguse üle Eestile sobivaimal moel ja teeme Euroopas ettepanekud sobimatute normide muutmiseks, sealhulgas ettepanek lükata edasi kestlikkusaruandluse esitamine ja muuta need vabatahtlikuks“.[2] Eelnõu väljatöötamise alus on Vabariigi Valitsuse tegevusprogrammi 2023–2027[3] ELi direktiivide valdkonna all nimetatud ülesanne „Eelnõu direktiivi (EL) 2022/2555 ülevõtmiseks (küberturvalisuse 2. direktiiv)“.

Kuna ülevõtmisseadusega suurendati halduskoormust (küberturvalisuse seaduse kohaldamisala täiendati uute subjektidega, kes peavad seaduse nõudeid täitma), nähti halduskoormuse tasakaalustamine ette Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muudatustega. Need muudatused jõustusid 1. oktoobril 2025. Kommenteeritav eelnõu ei näe ette halduskoormuse kasvu, see on seotud ennekõike Justiits- ja Digiministeeriumile või tema volitatud asutusele antud ülesande sisustamise ja asjaomase töökoormusega, mis ilmneb vaid juhul, kui Eesti otsustab osaleda vastastikuses hindamises.

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb viiest paragrahvist.

Paragrahvis 1 sätestatakse eelnõukohase määruse reguleerimis- ja kohaldamisala. **Lõike 1** kohaselt reguleerib eelnõukohane määrus Eesti Vabariigi osalemist NIS2-direktiivi artiklis 19 sätestatud vastastikuses hindamises. **Lõige 2** täpsustab määruse sisu, st sätestab, et eelnõukohases määruses täpsustatakse vastastikuses hindamises osalemise tingimusi, sealhulgas vastastikuse hindamise tegemise nõudeid, selles osalevate asutuste ülesandeid ja vastastikuses hindamises osalevaid isikuid.
Eelnõukohase määrusega on seotud ka NIS2-direktiivi põhjendused 75 ja 76:
(75) Kasutusele tuleks võtta vastastikune hindamine, et aidata õppida ühistest kogemustest, tugevdada vastastikust usaldust ja saavutada küberturvalisuse ühtlaselt kõrge tase. Vastastikune hindamine võib anda väärtuslikke teadmisi ja viia soovitusteni, mis tugevdavad üldist küberturvalisuse võimekust, luues uue funktsionaalse tee parimate tavade jagamiseks liikmesriikide vahel ning aidates tõsta liikmesriikide küberturvalisuse taset. Lisaks peaks vastastikuses hindamises võtma arvesse sarnaste mehhanismide, näiteks CSIRTide võrgustiku[4] vastastikuse hindamise süsteemi tulemusi, looma lisaväärtust ja vältima dubleerimist. Vastastikuse hindamise rakendamine ei tohiks piirata konfidentsiaalse ja salastatud teabe kaitset käsitlevate riiklike või liidu õigusaktide kohaldamist.

[2] https://valitsus.ee/valitsuse-eesmargid-ja-tegevused/valitsemise-alused/koalitsioonilepe-2025-2027
[3] https://valitsus.ee/sites/default/files/documents/2023-05/VVTP%202023-2027_26.pdf
[4] CSIRTide võrgustik on NIS2-direktiivi artikli 15 kohane võrgustik. Küberturvalisuse seaduses nimetatakse seda võrgustikku „küberintsidentide käsitlemise riiklike üksuste võrgustikuks“ või lühidalt „võrgustikuks“.

(76) Koostöörühm[5] peaks kehtestama liikmesriikide jaoks enesehindamise metoodika, mille eesmärk on hõlmata selliseid tegureid nagu küberturvalisuse riskijuhtimismeetmete ja teatamiskohustuse rakendamise tase, pädevate asutuste võimekuse tase ja ülesannete täitmise tulemuslikkus, CSIRTide[6] tegevusvõimekus, vastastikuse abi rakendamise tase, küberturvalisuse alase teabevahetuse korra rakendamise tase või konkreetsed piiriülese või valdkondadevahelise iseloomuga küsimused. Liikmesriike tuleks julgustada tegema korrapäraselt enesehindamisi ning esitama ja arutama oma enesehindamise tulemusi koostöörühmas.

Paragrahvis 2 sätestatakse vastastikuse hindamise metoodikast, korralduslikest aspektidest ja tegevusjuhenditest lähtumine.
Lõikega 1 rakendatakse NIS2-direktiivi artikli 19 lõike 1 esimese lõigu esimene lause (*[k]oostöörühm töötab 17. jaanuariks 2025 komisjoni ja ENISA[7] ning, kui see on asjakohane, CSIRTide võrgustiku[8] abiga välja vastastikuse hindamise metoodika ja korralduslikud aspektid, et õppida jagatud kogemustest, tugevdada vastastikust usaldust, saavutada küberturvalisuse ühtlaselt kõrge tase ning suurendada liikmesriikide küberturvalisuse alast võimekust ja poliitikat, mis on vajalik [NIS2-direktiivi] rakendamiseks*) ja lõike 6 kolmas lause (*[k]oostöörühm töötab koostöös komisjoni ja ENISAga välja asjakohased tegevusjuhendid, millele määratud küberturvalisuse ekspertide töömeetodid toetuvad*).
NIS2-direktiivi artikli 19 lõike 2 esimene lause näeb ette, et viidatud *metoodika sisaldab objektiivseid, mittediskrimineerivaid, õiglasi ja läbipaistvaid kriteeriume, mille alusel liikmesriigid määravad vastastikuse hindamise läbiviimiseks sobivad küberturvalisuse valdkonna eksperdid*.
Kõnealuses paragrahvis viidatud vastastikuse hindamise metoodika leiab NIS2-direktiivi artiklis 14 nimetatud koostöörühma veebilehelt.[9]

Lõikes 2 sätestatakse vastastikuse hindamise tingimused. Lõige koosneb viiest punktist.
Punktiga 1 võetakse üle NIS2-direktiivi artikli 19 lõike 6 esimene lause (*[v]astastikune hindamine hõlmab kohapealseid või virtuaalseid külastusi ja teabevahetust väljaspool tegevuskohta*). Kommenteeritavasse punkti on tegevuskoha juurde lisatud sõna „hinnatavat“, et oleks selgem seos, mida tegevuskoha all mõeldakse – tegemist on hinnatava tegevuskohaga.
Punktiga 2 võetakse üle NIS2-direktiivi artikli 19 lõike 6 neljas lause (*[v]astastikuses hindamises saadavat teavet kasutatakse üksnes hindamise eesmärgil*).
Punktiga 3 võetakse üle NIS2-direktiivi artikli 19 lõige 7 (*[l]iikmesriigis juba vastastikku hinnatud aspektid ei kuulu kõnealuses liikmesriigis enam vastastikusele hindamisele kahe aasta jooksul pärast vastastikuse hindamise lõppemist, välja arvatud juhul, kui seda taotleb liikmesriik või nii lepitakse kokku pärast koostöörühma ettepanekut*). Hinnatavate aspektide kohta vt eelnõu § 4 lõike 1 punkt 4. Kommenteeritava punktiga määratakse kindlaks üldreegel, et hinnatud aspekte kõnealuses riigis kahe aasta jooksul pärast vastastikuse hindamise lõppemist enam uuesti vastastikku ei hinnata. Riigi all on mõeldud nii Eesti Vabariiki või muud Euroopa Liidu liikmesriiki, kelle suhtes toimus vastastikune hindamine. Sellele üldreeglile on erisused: 1) kui Eesti Vabariigi suhtes tehtud vastastikuse hindamise puhul Eesti soovib mingit

[5] NIS2-direktiivi artikkel 14 reguleerib koostöörühma tegevust. Küberturvalisuse seaduses nimetatakse seda koostöörühma „artiklis 14 nimetatud koostöörühmaks“ või lühidalt „koostöörühmaks“.
[6] NIS2-direktiivi artikkel 10 reguleerib küberintsidentidele reageerimise üksuste ehk CSIRTide tegevust. Küberturvalisuse seaduses nimetatakse neid „küberintsidentide käsitlemise üksusteks“.
[7] ENISA on Euroopa Liidu Küberturvalisuse Ameti rahvusvaheline lühend.
[8] CSIRTide võrgustik on NIS2-direktiivi artikli 15 kohane võrgustik. Küberturvalisuse seaduses nimetatakse seda „küberintsidentide käsitlemise riiklike üksuste võrgustikuks“ või lühidalt „võrgustikuks“.
[9] https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group – täpsemalt: https://ec.europa.eu/newsroom/dae/redirection/document/121656.

aspekti uuesti hindamist; või 2) kui uuesti hindamine lepitakse kokku pärast NIS2-direktiivi artiklis 14 nimetatud koostöörühma ettepanekut.
Punktiga 4 võetakse üle NIS2-direktiivi artikli 19 lõike 9 esimene lause (*[v]astastikuses hindamises osalevad küberturvalisuse eksperdid koostavad aruanded vastastikuse hindamise tulemuste ja järelduste kohta*) ja lõike 9 teine lause (*[l]iikmesriigid, keda vastastikku hinnatakse, võivad esitada märkusi neid käsitlevate aruannete kavandite kohta ning sellised märkused lisatakse aruannetele*). Eesti Vabariigi õigus teha märkusi on sätestatud eelnõu § 4 lõike 1 punktis 8.
Punktiga 5 võetakse üle NIS2-direktiivi artikli 19 lõike 9 kolmas lause (*[a]ruanded sisaldavad soovitusi vastastikuse hindamisega hõlmatud aspektide parandamiseks*). Vastastikuse hindamise tulemuste ja järelduste kohta võib koostada ühe või mitu aruannet. See sõltub konkreetse vastastikuse hindamise käigus kokku lepitud tegevustest ja ülesannetest.

Paragrahviga 3 võetakse üle NIS2-direktiivi artikli 19 lõike 1 esimese lõigu kolmas lause (*[v]astastikuse hindamise viivad läbi küberturvalisuse valdkonna eksperdid*). Selle kohta vt ka eelnõu § 2 lõike 1 selgitust.

Paragrahviga 4 sätestatakse vastastikuses hindamises osalevad asutused ja nende ülesanded.
Lõikega 1 nähakse ette, et vastastikuses hindamises osaleb Justiits- ja Digiministeerium, sh kehtestatakse tema vastastikuse hindamisega seotud ülesanded. Lõige näeb ette, et ministeeriumil on võimalik oma ülesandeid ka edasi volitada – näiteks ministeeriumi haldusala asutusele, nagu Riigi Infosüsteemi Amet. Lõige koosneb kümnest punktist.
Punktiga 1 võetakse üle NIS2-direktiivi artikli 19 lõike 1 esimese lõigu neljas lause (*[k]überturvalisuse eksperdid määravad vähemalt kaks liikmesriiki, mis on muud liikmesriigid kui see, mida hinnatakse*). **Punktiga 2** võetakse üle NIS2-direktiivi artikli 19 lõike 8 esimene lause (*[l]iikmesriigid tagavad, et määratud küberturvalisuse ekspertidega seotud huvide konflikti oht tehakse enne vastastikuse hindamise algust teatavaks teistele liikmesriikidele, koostöörühmale, komisjonile ja ENISA-le*[10]). **Punktiga 3** võetakse üle NIS2-direktiivi artikli 19 lõike 8 teine lause (*[l]iikmesriik, keda vastastikku hinnatakse, võib esitada vastuväiteid konkreetsete küberturvalisuse ekspertide määramisele piisavalt põhjendatud juhtudel, millest on teatatud määravale liikmesriigile*).
Punkt 4 on seotud NIS2-direktiivi artikli 19 lõike 1 teise lõigu rakendamisega ning sama artikli lõigete 3 ja 4 ülevõtmisega.
NIS2-direktiivi artikli 19 lõike 1 teine lõik sätestab järgmist:
Vastastikuse hindamise raames hinnatakse vähemalt ühte järgmistest aspektidest:
a) artiklites 21 ja 23 sätestatud küberturvalisuse riskijuhtimismeetmete ja teatamiskohustuse rakendamise tase;[11]
b) võimekuse tase, sealhulgas olemasolevad rahalised, tehnilised ja inimressursid, ning pädevate asutuste ülesannete täitmise tõhusus;
c) CSIRTide[12] *tegevusvõimekus;*
d) artiklis 37 osutatud vastastikuse abi rakendamise tase;[13]
e) artiklis 29 osutatud küberturvalisuse alase teabevahetuse kokkulepete rakendamise tase;[14]
f) piiriülese või valdkonnaülese iseloomuga eriküsimused.

[10] ENISA on Euroopa Liidu Küberturvalisuse Ameti rahvusvaheline lühend.
[11] Nimetatud artiklid on ennekõike üle võetud küberturvalisuse seaduse §-dega 7, 8 ja 12, sh seal viidatud määrustega.
[12] NIS2-direktiivi artikkel 10 reguleerib küberintsidentidele reageerimise üksuste ehk CSIRTide tegevust. Küberturvalisuse seaduses nimetatakse neid „küberintsidentide käsitlemise üksusteks".
[13] Nimetatud artikkel on ennekõike üle võetud küberturvalisuse seaduse §-ga 17^3.
[14] Nimetatud artikkel on ennekõike üle võetud küberturvalisuse seaduse §-ga 17^5.

NIS2-direktiivi artikli 19 lõiked 3 ja 4 sätestavad järgmist:
3. Liikmesriigid võivad määrata kindlaks lõike 1 punktis f osutatud eriküsimused vastastikuseks hindamiseks.
4. Enne lõikes 1 osutatud vastastikuse hindamise alustamist teatavad liikmesriigid osalevatele liikmesriikidele selle ulatuse, sealhulgas lõike 3 kohaselt kindlaks määratud eriküsimused.
Punktiga 5 võetakse üle NIS2-direktiivi artikli 19 lõike 5 esimene lause (*[e]nne vastastikuse hindamise algust võib liikmesriik teha vaatlusaluste aspektide enesehindamise ja esitada selle määratud küberturvalisuse ekspertidele*). **Punktiga 6** võetakse üle NIS2-direktiivi artikli 19 lõike 6 teine lause (*[k]ooskõlas hea koostöö põhimõttega esitab liikmesriik, keda vastastikku hinnatakse, määratud küberturvalisuse ekspertidele hindamiseks vajaliku teabe .. .*). Selle punktiga seoses vt ka eelnõu § 4 lõige 2. **Punkt 7** on seotud NIS2-direktiivi artikli 19 lõike 7 rakendamisega (mis võetakse üle eelnõu § 2 lõike 2 punktiga 3), et oleks selge, kes Eesti puhul vastava taotluse teeb. **Punktiga 8** võetakse üle NIS2-direktiivi artikli 19 lõike 9 teine lause (*[l]iikmesriigid, keda vastastikku hinnatakse, võivad esitada märkusi neid käsitlevate aruannete kavandite kohta .. .*). **Punktiga 9** võetakse üle NIS2-direktiivi artikli 19 lõike 9 neljas lause (*[a]ruanded esitatakse koostöörühmale ja CSIRTide võrgustikule,*[15] *kui see on asjakohane.*). **Punktiga 10** võetakse üle NIS2-direktiivi artikli 19 lõike 9 viies lause (*[l]iikmesriik, keda vastastikku hinnatakse, võib otsustada teha oma aruande või selle toimetatud versiooni üldsusele kättesaadavaks*).
Kommenteeritavas lõikes või selle selgitustes mainitud metoodika kohta vt eelnõu § 2 lõike 1 selgitust.

Lõige 2 on seotud NIS2-direktiivi artikli 19 lõike 6 teise lause (*[k]ooskõlas hea koostöö põhimõttega esitab liikmesriik, keda vastastikku hinnatakse, määratud küberturvalisuse ekspertidele hindamiseks vajaliku teabe, ilma et see piiraks konfidentsiaalse või salastatud teabe kaitset või riigi põhifunktsioonide, näiteks riigi julgeoleku kaitset käsitleva liikmesriikide või liidu õiguse kohaldamist*) ülevõtmise ja rakendamisega. Selle kohta vt ka eelnõu § 4 lõike 1 punkt 6.

Paragrahviga 5 nähakse ette määruse jõustumise aeg, milleks on 1. aprill 2026 (vt seletuskirja punkt 6).

Määrusele lisatakse normitehniline märkus NIS2-direktiivi kohta.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõus järgitakse NIS2-direktiivi. Eelnõu vastab NIS2-direktiivile ning kuna direktiiv võeti ennekõike üle ülevõtmisseadusega, on selle seaduseelnõu materjalide juures ka NIS2-direktiivi ja ülevõtmisseaduse vastavustabel. Siinkohal esitatakse need NIS2-direktiivi artikli 19 sätted, mis on seotud kõnesoleva eelnõuga:
1) lõike 1 esimese lõigu esimene lause = see on seotud eelnõu § 2 lõikega 1;
2) lõike 1 esimese lõigu teine lause = ei võeta üle kõnesoleva eelnõuga, vaid on üle võetud küberturvalisuse seaduse § 17^6 lõikega 1;
3) lõike 1 esimese lõigu kolmas lause = eelnõu § 3, kuid see on seotud ka § 2 lõikega 1;
4) lõike 1 esimese lõigu neljas lause = eelnõu § 4 lõike 1 punkt 1;
5) lõike 1 teine lõik = see on seotud eelnõu § 4 lõike 1 punktiga 4;
6) lõike 2 esimene lause = ei ole vaja üle võtta, kuid see on seotud eelnõu § 4 lõike 1 punktiga 1;

[15] CSIRTide võrgustik on NIS2-direktiivi artikli 15 kohane võrgustik. Küberturvalisuse seaduses nimetatakse seda „küberintsidentide käsitlemise riiklike üksuste võrgustikuks“ või lühidalt „võrgustikuks“.

7) lõike 2 teine lause = ei ole vaja üle võtta;
8) lõige 3 = eelnõu § 4 lõike 1 punkt 4;
9) lõige 4 = eelnõu § 4 lõike 1 punkt 4;
10) lõike 5 esimene lause = eelnõu § 4 lõike 1 punkt 5;
11) lõike 5 teine lause = ei ole vaja üle võtta;
12) lõike 6 esimene lause = eelnõu § 2 lõike 2 punkt 1;
13) lõike 6 teine lause = eelnõu § 4 lõike 1 punkt 6 ja lõige 2;
14) lõike 6 kolmas lause = see on seotud eelnõu § 2 lõikega 1;
15) lõike 6 neljas lause = eelnõu § 2 lõike 2 punkt 2;
16) lõike 6 viies lause = ei võeta üle kõnesoleva eelnõuga, vaid on üle võetud küberturvalisuse seaduse § 17^6 lõikega 2;
17) lõige 7 = eelnõu § 2 lõike 2 punkt 3, kuid see on seotud ka § 4 lõike 1 punktiga 7;
18) lõike 8 esimene lause = eelnõu § 4 lõike 1 punkt 2;
19) lõike 8 teine lause = eelnõu § 4 lõike 1 punkt 3;
20) lõike 9 esimene lause = eelnõu § 2 lõike 2 punkt 4;
21) lõike 9 teine lause = eelnõu § 2 lõike 2 punktid 4 ja § 4 lõike 1 punkt 8;
22) lõike 9 kolmas lause = eelnõu § 2 lõike 2 punkt 5;
23) lõike 9 neljas lause = eelnõu § 2 lõike 2 punkt 9;
24) lõike 9 viies lause = eelnõu § 2 lõike 2 punkt 10.
Iga muudatuse juures on võrreldud muudetava sätte vastavust Euroopa Liidu õigusele, vajaduse korral on toodud ka võimalikud sõnastusalternatiivid.
Sätete puhul, mis sõnastatakse teisiti kui NIS2-direktiivis, 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

Vastastikuses hindamises osalemine on vabatahtlik. Seetõttu sõltuvad vastastikuse hindamisega seotud ülesanded ja nende maht ennekõike asjaolust, kas Eesti soovib üldse NIS2-direktiiviga ette nähtud vastastikuses hindamises osaleda.
Määruse rakendamisel võib olla otsene mõju üksnes riigiasutuste töökorraldusele, kuna Justiits- ja Digiministeeriumile (vajadusel koostöös Riigi Infosüsteemi Ameti kui ka muude asutuste küberturvalisuse valdkonna ekspertidega) võivad lisanduda vastastikuse hindamise ettevalmistamise, koordineerimise, eksperdi määramise, teabe edastamise ja aruandlusega seotud ülesanded. Tegemist on hindamisega, mis võib tuua ettevalmistamise ja läbiviimise perioodidel kaasa täiendava töökoormuse.
Määruse rakendamisel võib olla kaudne mõju riigi julgeolekule, siseturvalisusele ja ettevõtluskeskkonnale. Hindamise käigus tehtavad soovitused võivad aidata suurendada küberturvalisuse taset, toetades seeläbi teenuste toimepidevust. Kuigi määrus ei kehtesta ettevõtjatele uusi kohustusi, võib kujunev praktika mõjutada järelevalve ühtlustumist ja nõuete rakendamist. Samuti toetab määrus Eesti osalemist Euroopa Liidu küberturvalisuse alases koostöös ning aitab kaasa turvalise ja usaldusväärse digikeskkonna arengule.
Muudes valdkondades eelnõu olulist mõju ei avalda, mistõttu pole mõju sihtrühmade kaupa käsitletud.

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

Eelnõukohase määrusega seotud tegevusi ja kulusid on üldistatult hinnatud ülevõtmisseaduse eelnõu seletuskirjas (vt seletuskirja punkti 7 sissejuhatus), mistõttu selle tulemusi siin ei korrata.[16]
Justiits- ja Digiministeeriumile ja teistele kaasatud osapooltele tekkivad võimalikud tegevused ja kulud sõltuvad Eesti otsusest osaleda vastastikuses hindamises.

6. Määruse jõustumine

Määrus jõustub 1. aprillil 2026. Jõustumisaja määramisel on lähtutud kuupäevast, mis jätaks piisavalt aega eelnõu avalikuks kooskõlastamiseks.

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 määruse eelnõuga kavandatavate nõuete kohta. Asjaomase tagasiside leiab ülevõtmisseaduse eelnõu dokumentide juurest.

Eelnõu esitatakse eelnõude infosüsteemi kaudu kooskõlastamiseks Riigikantseleile ja Rahandusministeeriumile.

Eelnõu saadetakse arvamuse avaldamiseks Riigi Infosüsteemi Ametile.

[16] Vt altviidet nr 1.