



Margo Külaots
Gren Eesti AS
info.eesti@gren.com

01.10.2024 nr 8-1/22-0115/241583

VÄLJAVÕTE

ETTEKIRJUTUS

Ettekirjutuse teinud haldusorgan	Riigi Infosüsteemi Amet
Haldusorgani esindaja	järelevalve osakonna juhtivekspert XXXXXXXXX
Ettekirjutuse tegemise aeg ja koht	01.10.2024, Tallinn
Ettekirjutuse adressaat	Gren Eesti AS (registrikood 12114252) Niidu tn 24 80047 Pärnu, Pärnumaa Telefon: +372 4477210 info.eesti@gren.com
Adressaadi esindajad	Margo Külaots Juhatuse liige

I Resolutsioon:

Võtnud aluseks korrakaitseaduse (edaspidi KoRS) § 28 lg 1 ja küberturvalisuse seaduse §-id 7 ja 8 ning hinnanud riikliku järelevalvemenetluse käigus välja selgitatud asjaolusid teen kohustusliku ettekirjutuse:

1. XXXXXXXXXXX XXXXXXXXXXX XXXXXXXXXXX XXXXXXXXXXX
XXXXXXXXXXXX XXXXX:
 - 1.1 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX;
 - 1.2 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX;
 - 1.3 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXX;

5. **XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX.**

Märkus: Dokumenteerimine ei eelda ilmtingimata paberdokumendi olemasolu, võib kasutada ka vastavat elektroonilist halduskeskkonda. Dokumenteerimise põhieesmärgiks on tagada süsteemi/protsessi kohta käiva igakülgse ja ajakohase teabe olemasolu ning asjaosalistele kiire ja lihtne ligipääs sellele teabele.

Määrán ettekirjutuse täitmise tähtajaks 30.09.2025.

Ettekirjutuse täitmisest tuleb Gren Eesti AS-l hiljemalt selleks tähtajaks Riigi Infosüsteemi Ametit teavitada e-posti aadressil jvo@ria.ee, esitades ettekirjutuse täitmist kinnitavad tõendid ja ajakohase teabe.

II Vaidlustamisviide:

Isikul, kes leiab, et ettekirjutusega rikutakse tema õigusi, on 30 kalendripäeva jooksul arvates sellise asjaolu teadaaamisest õigus esitada vaie Riigi Infosüsteemi Ameti peadirektorile (Pärnu mnt 139a, 15169 Tallinn, e-post info@ria.ee) haldusmenetluse seaduses sätestatud korras või kaebus Tallinna Halduskohtusse (Tallinna Kohtumaja, Pärnu mnt 7, 15082 Tallinn, e-post tlnhktallinn.menetlus@kohus.ee) halduskohtumenetluse seadustikus sätestatud korras. Ettekirjutuse vaidlustamine ei peata ettekirjutuse täitmist ega sunnivahendi rakendamist, kui Riigi Infosüsteemi Amet või kohus ei otsusta teisiti.

III Sunniraha hoiatus:

Kui ettekirjutus jäetakse määratud tähtajaks täitmata või täidetakse osaliselt, määrab Riigi Infosüsteemi Amet Gren Eesti AS-le KüTS § 17¹ alusel sunniraha alljärgnevalt:

- ettekirjutuse resolutsiooni punkti 1 mittetäitmise eest – 4500 eurot;
- ettekirjutuse resolutsiooni punkti 2 mittetäitmise eest – 2000 eurot;
- ettekirjutuse resolutsiooni punkti 3 mittetäitmise eest – 1500 eurot;
- ettekirjutuse resolutsiooni punkti 4 mittetäitmise eest – 5000 eurot;
- ettekirjutuse resolutsiooni punkti 5 mittetäitmise eest – 1000 eurot.

Juhul, kui Gren Eesti AS ei täida ettekirjutust määratud tähtajaks ja ei tasu vabatahtlikult sunniraha, edastatakse ettekirjutus kohtutäiturile täitemenetluse alustamiseks. Sellisel juhul lisanduvad sunnirahale kohtutäituri tasu ja muud täitekulud. **Asendustäitmise ja sunniraha seaduse (ATSS) § 2 lõike 2 kohaselt võib sunniraha rakendada korduvalt kuni ettekirjutusega taotletava eesmärgi saavutamiseni.**

Sunniraha vabatahtlikul tasumisel märkida selgituseks „RIA riiklik järelevalve asjas nr 8-1/24-0115 sunniraha“ ja viitenumbriks 2800045496.

Sunniraha tuleb tasuda Rahandusministeeriumi pangakontole alljärgnevalt:

SEB Pank EE891010220034796011 (BIC/SWIFT: EEUHEE2X)
Swedbank EE932200221023778606 (BIC/SWIFT: HABAEE2X)
LHV Pank EE777700771003813400 (BIC/SWIFT: LHVBE22)
Luminor Bank EE701700017001577198 (BIC/SWIFT: NDEAEE2X)

IV Faktilised asjaolud ja menetluskäik:

Riigi Infosüsteemi Amet (edaspidi RIA) algatas 03.04.2024 saadetud järelepärimisega (8-1/24-0115/24555) Gren Eesti AS (edaspidi GE) suhtes riikliku järelevalvemenetluse, mille eesmärk on kontrollida GE poolt küberturvalisuse seaduse (edaspidi KüTS) §-des 7 ja 8 sätestatud nõuete täitmist.

Järelevalvemenetluse läbiviimisel kontrolliti nõuetekohast täitmist järgmiste tegevuste osas:

- 1.1 alalist organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete rakendamist küberintsidentide ennetamiseks, lahendamiseks, leevendamiseks (asjakohaste infoturbealaste tegevuste korraldamine, sh infoturvet korraldavate organisatsiooniliste dokumentide (strateegia, korrad, poliitika, juhised jm) olemasolu ja nende rakendamine);
- 1.2 võrgu- ja infosüsteemi riskianalüüsi olemasolu ja riskide haldamist;
- 1.3 küberintsidentide käsitlemist ja teavitamist.

RIA küsis välja asjassepuutuvad dokumendid, analüüsis neid ning viis läbi kohapealse kontrolli, mille käigus intervjueris ning täpsustas tehnilisi aspekte GE vastava valdkonna eest vastutavate esindajatega. Kohapealne kontroll toimus 30.04.2024 ning serveriruumide külastus 22.05.2024 (kontrollakt asjas nr 8-1/24-0115/241222, allkirjastatud menetleja ja GE esindaja poolt 23.07.2024).

Järelevalvemenetluse käigus tuvastatud asjaolud põhinevad RIA-le esitatud dokumentide analüüsil ning GE valdkonna eest vastutavate esindajate ütlustel.

V Järelevalvemenetluse käigus tuvastatud asjaolud

XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXX.

XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX.

XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX.

XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXX.

XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXX.

VI Ärakuulamisõiguse andmine

26.08.2024 edastas RIA GE-le teavituse eelseisvast ettekirjutusest ning andis võimaluse oma arvamuse ja vastuväidete esitamiseks (nr 8-1/24-0115/241394 „Teavituse eelseisvast ettekirjutusest ja ärakuulamisõiguse andmine“). GE edastas RIA-le oma vastuse 09.09.2024 (nr 2024-33-01-032) märkides, et RIA seisukohtadele vastuväiteid GE-l ei ole.

VII Lõppjärelendus

KüTS § 7 ja § 8 ning nende sätete alusel kehtestatud määruste kohaselt on GE kohustatud:

- rakendama alaliselt organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid küberintsidendi ennetamiseks, küberintsidendi lahendamiseks või teenuse toimepidevusele või süsteemi turvalisusele avalduva mõju ennetamiseks ja leevendamiseks;
- korraldama ning kinnitama nõuete ja ajakohase riskihalduse protsessi, sh koostama võrgu- ja infosüsteemi riskianalüüsi võrgu- ja süsteemi turvalisust ja teenuse toimepidevust mõjutavate ning küberintsidendi tekkimist põhjustavate riskide järjepidevaks haldamiseks;
- tagama dokumenteeritud süsteemi riskianalüüsi, turvaeeskirjade ja turvameetmete rakendamise kirjelduse olemasolu ja ajakohasuse;
- tagama süsteemi turvalisust ohustava tegevuse või tarkvara tuvastamiseks süsteemi seire ja edastama teavet süsteemi turvalisust ohustava tegevuse või tarkvara kohta Riigi Infosüsteemi Ametile (CERT.EE);
- võtma kasutusele abinõud küberintsidendi mõju ja leviku vähendamiseks, sealhulgas vajaduse korral piirama süsteemi kasutamist või juurdepääsu süsteemile;
- ülaltoodud kohustuste täitmisel lähtuma Eesti infoturbestandardist (E-ITS) või ISO/IEC 27001 raamistikust.

XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXX XXXXXXX.

Ülaltoodut arvestades leiab RIA, et kohustusliku ettekirjutuse tegemine antud asjas on vajalik ja mõödapääsmatu esinevate puuduste kõrvaldamiseks. Ettekirjutusega nõutud tegevused on loetletud käesoleva dokumendi resolutiivosas.

IX Ettekirjutuse saatmine ja üle andmine:

Ettekirjutus edastatakse GE-le krüpteeritult ettevõtte esindaja (hr Margo Külaots) sertifikaatidega ettevõtte üldisele e-posti aadressile:
info.eesti@gren.com.

(allkirjastatud digitaalselt)

XXXXX XXXXX
Küberturvalisuse keskuse NSCS-EE
Järelevalve osakonna juhtivekspert
peadirektori volitusel
Tel: XXXXXXXX XXXXXXXX@ria.ee