

Pr. Liisa-Ly Pakosta

justiits- ja digiminister

Justiits- ja Digiministeerium Meie 31.01.2025 nr 10/1-4

**Eesti Põllumajandus-Kaubanduskoja seisukoht küberturvalisuse seaduse ja teiste seaduste muutmise seadusele**

Eesti Põllumajandus-Kaubanduskoda (EPKK), mis koondab koos oma liikmesorganisatsioonidega üle 30 000 juriidilise ja füüsilise isiku, pöördub Teie poole, et anda tagasisidet küberturvalisuse seaduse (KüTS) ja teiste seaduste muutmise seadusele, mis keskendub küberturvalisuse NIS2 direktiivi ülevõtmisele.

NIS2 direktiivi ülevõtmise peamine eesmärk on tugevdada ettevõtjate küberturvalisuse süsteeme, hinnata turvariske ja tagada, et nende tegevus ei ohusta mitte ainult ettevõtte enda, vaid ka tarbijate ja teiste ettevõtete ja tarneahela osaliste turvalisust. See on kindlasti oluline, arvestades, et küberintsidendid on toimunud viimastel aastatel ka põllumajanduse ja toidutootmisega tegelevates ettevõtetes. Toidutootjad, kes sõltuvad suurtesti IT-süsteemidest, automatiseeritud tootmisprotsessidest või laiaulatuslikest andmevahetustest, peavad uutele nõuetele vastavalt pöörama senisest rohkem tähelepanu küberturvalisusele ja selle tagamisele, mis toob kaasa ka senisest märkimisväärselt suuremaid kulusid.

**Meie peamine mure on KüTS-i E-ITS infoturbestandardi rakendamise kohustus, mis sisaldab nõuet auditeerida riske audiitorkontrolliga ja vajadusel teha suuremahulisi ja kulukaid muudatusi protsessides.** Meile on jätkuvalt arusaamatu, milline on riski ulatus või reaalne oht riigile, kui toidusektori ettevõtjad igaüks eraldiseisvana ei rakenda küberturvalisuse seadust nõutud mahus? Tuleb märkida, et toidutootmine on enamasti mehhaniseeritud ja suures osas digitaliseeritud, kuid seadmeid saab vajadusel manuaalselt käivitada ja protsesside etappe teostada käsitsi. Seetõttu jääb arusaamatuks, miks toiduvaldkonnas tegutsev ettevõte peab kasutama just ettenähtud E-ITS-i ja ei saa ise valida sobivaid meetodeid küberturvalisuse riskidega tegelemiseks. KüTS-i määratud riskide maandamine peab olema osa ettevõtte riskianalüüsist, kus küberturvalisuse riske ja ohte hindab elutähtsa teenuse osutajast ettevõtte juht kaalutletult, võttes vastu vastavad meetmed nende maandamiseks. Eelnõu väljatöötamisel ei ole analüüsitud, kui suures ulatuses tootjad peavad oma protsesse täiendama ega ole arvestatud E-ITS-i rakendamisega kaasnevat lisainvesteeringute vajadust.

Me ei saanud 23. jaanuaril toimunud küberturvalisuse seaduse (NIS2) seminaril kinnitust, et riigil on olemas vajalik oskustugi ettevõtjatele, et aidata küberturvalisuse nõudeid täita nende tootmisspetsiifikast lähtuvalt. Küberturvalisuse seadusest tulenevad kohustused ei saa aga olla ainult ettevõtjate ülesanne. Ettevõtete küberturvalisusega seotud probleemide lahendamiseks tuleb ette näha üleriigilisi õppusi ja ettevõtjapõhiseid koolitusi. Just õppused aitavad tõhusamalt tuvastada probleemkohad nii ettevõtetes, sektoriüleselt kui ka riigi tasandil, olles tõhusam lahendus kui iga seaduse subjekti eraldi auditeerida.

**Audiitorkontrollide vajadus ja hind**

Meie arvates ei ole audiitorkontrollide vajadust ja sellega kaasnevat kulu ettevõtjatele piisavalt hinnatud. NIS2 direktiivi rakendamisest tulenev audiitorkontrolli hind sõltub mitmest tegurist nagu ettevõtte suurusest ja tehnoloogiliste protsesside keerukusest. Suuremad ettevõtted, millel on keerukamad IT-süsteemid ja rohkem töötajaid, vajavad tõenäoliselt põhjalikku ja aeganõudvat auditeerimist. Kuna enamik ettevõtteid peab auditi tegema esmakordselt, võib protsess võtta rohkem aega. Kui ettevõtte küberturvalisuse süsteemid vajavad täiendamist, võib see muuta audiitorkontrolli kallimaks. Väiksemate ettevõtete puhul võib audiitorkontrolli hind ulatuda 3000–5000 euroni, kuid suuremate ettevõtete puhul, kus süsteeme rohkem, võib hind ulatuda 15 000–50 000 euroni või enamgi.

Lisaks käesoleva eelnõu rakendamisele tahame muuhulgas pöörata tähelepanu, et viimastel aastatel on erinevate eelnõudega lisandunud teisigi audiitorkontrolli nõudeid, nt ESG aruandlus, kuid nende kumulatiivset mõju ja kulu ettevõtjatele ei ole hinnatud.

Meie hinnangul võib auditeerimist kui ühte meedet kaaluda juhul, kui teisi võimalusi turvalisuse tagamiseks ei ole ning kui see siiski vajalikuks osutub, on mõistlik teha auditeerimist aeg-ajalt, näiteks iga 3 või 5 aasta järel, mitte pidevalt.

EPKK on alati seisnud selle eest, et Eesti põllumajandus- ja toidusektoril oleks strateegiline roll toidujulgeoleku tagamisel. Toidusektor kui üks elutähtsate teenuste osutaja, lisati hädaolukorra seadusesse viimase redaktsiooniga, andes sektorile üleminekuaja seadusest tulenevate kohustuste täitmiseks. 23. jaanuaril toimunud küberturvalisuse seaduse (NIS2) muutmise tutvustusseminaril kinnitati, et ka sellele seadusele kehtib toidusektorile üleminekuperiood. Me loodame, et lubatud ülemineku aeg kehtestatakse seaduse tasandil.

Lugupidamisega

/allkirjastatud digitaalselt/

Meeli Lindsaar

Toiduvaldkonna juht

Eesti Põllumajandus-Kaubanduskoda