ANDMEKAITSE INSPEKTSIOON

ETTEKIRJUTUS-HOIATUS
isikuandmete kaitse asjas nr. 2.2.-2/21/3026

Ettekirjutuse tegija	Andmekaitse Inspektsiooni jurist Mehis Lõhmus
Ettekirjutuse tegemise aeg ja koht	5. jaanuar 2022 Tallinn
Ettekirjutuse adressaat – isikuandmete töötleja	aadress: e-posti aadress: jetskalo@severi.ee
Isikuandmete töötleja vastutav ametiisik	Sergei Jetskalo, juhatuse liige (Severi Kaubandus OÜ)

RESOLUTSIOON: Isikuandmete kaitse seaduse § 56 lõike 1, lõike 2 punkti 8, § 58 lõike 1 ning isikuandmete kaitse üldmääruse artikli 58 lõike 1 punkti a ning arvestades sama lõike punktiga e, teeb Andmekaitse Inspektsioon Severi Kaubandus OÜ-le täitmiseks kohustusliku ettekirjutuse:

> **Vastata Andmekaitse Inspektsiooni 09.12.2021 nr 2.2.-2/21/3026 saadetud järelepärimisele ja ettepanekule**

Määrame ettekirjutuste täitmise tähtajaks **14.01.2022.a.** Ettekirjutuse täitmisest teatada hiljemalt selleks tähtajaks Andmekaitse Inspektsiooni e-posti aadressile info@aki.ee.

VAIDLUSTAMISVIIDE:

Käesoleva ettekirjutuse saab vaidlustada 30 päeva jooksul, esitades kas:
- haldusmenetluse seaduse kohase vaide Andmekaitse Inspektsioonile või
- halduskohtumenetluse seadustiku kohase kaebuse Tallinna Halduskohtusse (sel juhul ei saa enam samas asjas vaiet läbi vaadata).

Ettekirjutuse vaidlustamine ei peata selle täitmise kohustust ega täitmiseks vajalike abinõude rakendamist.

SUNNIRAHA HOIATUS:

Kui ettekirjutus on jäetud määratud tähtajaks täitmata, määrab Andmekaitse Inspektsioon ettekirjutuse adressaadile isikuandmete kaitse seaduse § 60 alusel:

sunniraha 3000 eurot.

Sunniraha võib määrata korduvalt – kuni ettekirjutus on täidetud. Kui adressaat ei tasu sunniraha, edastatakse see kohtutäiturile täitemenetluse alustamiseks. Sel juhul lisanduvad sunnirahale kohtutäituri tasu ja muud täitekulud.

FAKTILISED ASJAOLUD:

Andmekaitse Inspektsiooni menetluses on Severi Kaubandus OÜ rikkumisteade, mille kohaselt toimus Severi Kaubandus OÜ vastu küberrünnak.

Täpsustavalt on CERT-EE leidnud, et *"...paigaldatud oli Phobose lunavara. Kuna lunavara paigaldamine eeldab juurdepääsu saavutamist seadmele, siis peaks lugema seadmes olnud admed lekkinuks. Küberkurjategijad võivad hiljem ka kogutud andmete avaldamisega ähvardada ja nõuda lunaraha. Juhul, kui seadmed sisaldasid delikaatseid isikuandmeid tuleks kaaluda ka Andmekaitse Inspektsioon teavitamist."*

Seetõttu alustasime isikuandmete kaitse seaduse § 56 lg 3 punkti 8 alusel järelevalvemenetlust. Andmekaitse Inspektsioonil on õigus nõuda selgitusi ja muud teavet, sh järelevalvemenetluse läbiviimiseks vajalike dokumentide esitamist.[1]

Palusime teil täita ja esitada nõuetekohane rikkumisteate vorm ja vastata järelepärimises esitatud küsimustele. 14. oktoober 2021 esitasite täidetud rikkumisteate blanketi ja vastasite küsimustele.

Kuivõrd Andmekaitse Inspektsioon tuvastas teie esitatud vastuses puudujääke või vastuolusid, siis teostasime me 9. detsembril 2021 uue järelepärimise ning tegime ka ettepaneku.

Tõime 9. detsembri 2021 järelepärimises välja järgnevad probleemkohad:

Olete enda vastuses kirjutanud, et täpne rünnakust puudutatud isikute arv ei ole teile teada. Ometi rikkumisteates olete välja toonud, et rikkumisest puudutatud isikute arv oli 1-9. Selgitan, et rikkumisest puudutatud isikute arvu all on mõeldud täpne isikute arv kelle andmed lekkes olid. Muuhulgas olete märkinud, et andmeid lekkis 88,4 GB, mistõttu võib lekkinud isikuandmete arv olla suur.

Lisaks tõite rikkumisteates välja, et andmesubjekte teavitati andmelekkest suuliselt ja edastati järgnev informatsioon: „Meil eile õhtul toimus küberrünnaki juhtum". Jääb arusaamatuks andmesubjektide teavitamise võimalikkus, sest olete välja toonud, et rikkumisest puudutatud isikute arv on teile teadmata. Veel enam juhime teie tähelepanu asjaolule, et ülaltoodud teavitus on puudulik. Isikuandmete kaitse üldmääruse artikkel 34 lg 1 kohaselt teavitab vastutav töötleja andmesubjekti põhjendamatu viivituseta isikuandmetega seotud rikkumisest, kui isikuandmetega seotud rikkumine kujutab endast tõenäoliselt suurt ohtu füüsiliste isikute õigustele ja vabadustele. Sama artikli lg 2 sätestab, et andmesubjektile esitatud teates

[1] Selgituste küsimise õiguslik alus: haldusväliste isikute puhul vastavalt korrakaitseseaduse § 30 lõigetele 1 ja 3 koos isikuandmete kaitse üldmääruse artikkel 58 lõike 1 punktidega a, e ja f; haldusorgani puhul vastavalt Vabariigi Valitsuse seaduse § 75^2 lõike 1 punktile 1.

kirjeldatakse selges ja lihtsas keeles isikuandmetega seotud rikkumise laadi ning esitatakse vähemalt artikli 33 lõike 3 punktides b, c ja d osutatud teave ja meetmed. Antud juhul te seda teinud ei ole.

Lisaks ei ole te selgitanud andmelekke toimumise tagamaid, sh. lekkepõhjust. Selgitan, et rikkumisteate eesmärk on anda järelevalveasutusele võimalikult täpne ja selge ülevaade toimunud andmelekkest, et oleks võimalik võtta vastavad meetmed. Saime aru, et paigaldati Phobose pahavara – aga kuidas see õnnestus ja mis jäi vajaka Severi Kaubandus OÜ turvalisuse poolelt?

Muuhulgas esitasime täiendavas järelepärimises järgnevad küsimused:

1. Mis lekke põhjustas? Kuidas sai ründaja ligi andmetele?
2. Kus andmeid hoiti?
3. Millised turvameetmed olid andmete hoiustamiseks rakendatud?
4. Kui palju isikuandmeid lekkis? Palume tuua täpne arv. Kui lekkinud isikuandmete arv ei ole veel selge, siis palume põhjendada ja selgitada, kuidas kavatsetakse antud asjaolu selgeks teha.
5. Miks vahetatakse rikkumiste vältimiseks ruuter? Kuidas ruuteri vahetamine aitab edaspidiseid küberrünnakuid ära hoida? Mis põhjusel selline otsus vastu võeti?
6. Kas CERT-EE on teostanud lekke süvaanalüüsi koos soovitustega ja selle teile edastanud? Kui jah, siis palume see edastada Andmekaitse Inspektsioonile.

Lisaks eelnevale tegi Andmekaitse Inspektsioon Severi Kaubandus OÜ-le ettepaneku:

7. teha andmesubjektidele kirjalik, isikuandmete kaitse üldmäärusele vastav teavitus. Teavituse sisu osas lähtuda isikuandmete kaitse üldmääruse artiklist 34 lõikest 1 ja 2;
8. saata teavituse koopia Andmekaitse Inspektsioonile.

Kahjuks ei ole tänaseni Severi Kaubandus OÜ Andmekaitse Inspektsioonile vastanud. Järelepärimisele ja ettepanekule ootasime vastust hiljemalt 17. detsembriks.

Järelepärimises juhtis inspektsioon ka tähelepanu ettekirjutuse ja sunniraha määramisele juhul, kui inspektsiooni järelepärimisele ja ettepanekule tähtaegselt ei vastata.

ANDMEKAITSE INSPEKTSIOONI PÕHJENDUSED:

Vastavalt isikuandmete kaitse seaduse § 58 lõikele 1 ning isikuandmete kaitse üldmääruse artikkel 58 lõike 1 punktile a ning arvestades sama lõike punktiga e, on inspektsioonil õigus nõuda selgitusi ja muud teavet, sh järelevalvemenetluse läbiviimiseks vajalike dokumentide esitamist.

Võttes arvesse faktilisi asjaolusid ja asjaolu, et haldusorgani järelevalvemenetluse raames tehtud järelepärimisele vastamine on kohustuslik, kuid Severi Kaubandus OÜ ei ole inspektsiooni 9. detsembril 2021 saadetud järelepärimisele ja ettepanekule vastanud, leiab inspektsioon, et kohustusliku ettekirjutuse tegemine antud asjas on vajalik järelevalveasja

oluliste asjaolude väljaselgitamiseks ning haldusmenetluse efektiivselt, sh võimalikult kiirelt, läbi viimiseks.

Kui isikul on probleeme määratud tähtajaks inspektsioonile vastamisega, on isikul võimalik järelevalveasutusele selgitada, millised objektiivsed asjaolud olid takistuseks. Lihtsalt vastatama jätmine aga ei ole aktsepteeritav.

/allkirjastatud digitaalselt/
Mehis Lõhmus
jurist
peadirektori volitusel