ANDMEKAITSE INSPEKTSIOON

ETTEKIRJUTUS-HOIATUS
isikuandmete kaitse asjas nr. 2.2.-2/21/474

Ettekirjutuse tegija	Andmekaitse Inspektsiooni jurist Mehis Lõhmus
Ettekirjutuse tegemise aeg ja koht	30.03.2021 Tallinnas
Ettekirjutuse adressaat – isikuandmete töötleja	Living Minerals OÜ aadress: Kivila tn 18, Tallinn 13917 e-posti aadress: living.minerals@gmail.com
Isikuandmete töötleja vastutav isik	Juhatuse liige

RESOLUTSIOON: Isikuandmete kaitse seaduse (IKS) § 56 lõike 1, lõike 2 punkti 8, § 58 lõike 1 ning isikuandmete kaitse üldmääruse (IKÜM) artikli 58 lõike 2 punkdi d, artikli 13 lg 1 p c, d ja f alusel teen täitmiseks kohustusliku ettekirjutuse:

1. viia Living Minerals OÜ andmekaitsetingimused vastavusse IKÜM artiklites 12-14 sätestatud nõuetega.

Määran ettekirjutuse täitmise tähtajaks 12. aprill 2021.

Ettekirjutuse täitmisest teatage 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.

VÄÄRTEOKARISTUSE HOIATUS:
Isikuandmete kaitse üldmääruse artikli 58 lõike 2 kohase ettekirjutuse täitmata jätmise eest võidakse algatada väärteomenetlus isikuandmete kaitse seaduse § 69 tunnustel. Selle teo eest võidakse füüsilist isikut karistada rahatrahviga kuni 20 000 000 eurot ning juriidilist isikut võidakse karistada rahatrahviga kuni 20 000 000 eurot või kuni 4 protsenti tema eelmise majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem. Väärteo kohtuväline menetleja on Andmekaitse Inspektsioon.

FAKTILISED ASJAOLUD:

1. 03.02.2021 sai Andmekaitse Inspektsioon (AKI) Living Minerals OÜ teate, et toimunud on andmeleke. Nimelt oli Teie veebilehel mineralgarden.org võimalik ligi pääseda klientide isikuandmetele.
2. Kirjutasite, et olukord saadi kontrolli alla vähem kui poole tunni jooksul pärast CERT-EE teavitust. Kustutasite koheselt kättesaadava faili, deaktiveerisite pluginad ja kontrollisite üle ka veebilehe seaded, olemaks kindel, et kõik võimalikud ohud on kõrvaldatud.
3. Veebilehe haldur kommenteeris olukorda järgnevalt: *„Tegemist on antud mooduli eripäraga, mis tehtud exporte hoidis upload kataloogis, millest me ei olnud teadlikud. Upload kataloog on wordpressil alati avalik olnud vaikimisi, vastasel juhul ei kuvataks veebis ka pilte. Andmed otsingumootoris kindlasti leitavad ei olnud, seo ja webmaster blokeerivad seda vaikimisi samuti wordpress ise. Kui keegi selle leidis upload kataloogis ja alla laadis on tegemist tahtliku ründega meie lehe vastu.''*
4. Eelnevast tulenevalt alustas AKI 05.02.2021 järelevalvemenetluse.
5. Järelevalvemenetluse käigus esitas AKI 05.02.2021 järelepärimise, millele Living Minerals OÜ vastas 10.02.2021.
6. Saadud vastuste põhjal tegi AKI täiendava järelepärimise ning ettepaneku isikuandmete kaitse asjas.
7. AKI tegi ettepaneku koostada isikuandmete kaitse üldmääruse artiklitele 12-14 vastav privaatsuspoliitika, lõpetada koheselt www.bluehost.com kasutamine, kui puuduvad asjakohased kaitsemeetmed ning väljastada veebihalduri andmed.
8. 22.02.2021 vastas Living Minerals OÜ järgnevalt: *„Koostame uue privaatsuspoliitika ning anname selle valmimisest esimesel võimalusel teada; Kuna www.bluehost.com privaatsuspoliitika tagab Euroopa Liidu residentide õiguskaitse kooskõlas GDPR-ga, siis leiame, et teenusepakkujaga lepingu lõpetamiseks puudub hetkel põhjus; www.mineralgarden.org veebihaldur on Online Sysadmin OÜ.“*
9. Kuivõrd Living Minerals OÜ ei olnud pikalt pärast ettepaneku tegemist andmekaitsetingimusi uuendanud, siis tegi AKI 17.03.2021 korduva ettepaneku isikuandmete kaitse asjas.
10. Ettepanekuga soovis AKI, et Living Minerals OÜ koostaks isikuandmete kaitse üldmääruse artiklitele 12-14 vastava privaatsuspoliitika ja seda hiljemalt 25. märtsiks 2021.
11. 26.03.2021 saatis Living Minerals OÜ järgmise teate: *„Koostasime Andmekaitse*

Inspektsiooni suuniste kohaselt uue privaatsuspoliitika ning laadisime selle üles aadressile https://mineralgarden.org/privaatsuspoliitika/.“

12. AKI, olles tutvunud loodud andmekaitsetingimustega, leidis, et need ei vasta IKÜM artiklites 12-14 sätestatud nõuetele.

ISIKUANDMETE TÖÖTLEJA SELETUS:

Vastus 11.02.2021 tehtud ettepanekule

Seoses ettepanekutega:

1. Koostame uue privaatsuspoliitika ning anname selle valmimisest esimesel võimalusel teada.

Vastus 17.03.2021 korduvale ettepanekule

Koostasime Andmekaitse Inspektsiooni suuniste kohaselt uue privaatsuspoliitika ning laadisime selle üles aadressile https://mineralgarden.org/privaatsuspoliitika/.

ANDMEKAITSE INSPEKTSIOONI PÕHJENDUSED:

Isikuandmete töötlemisel tuleb lähtuda isikuandmete töötlemise põhimõtetest (vt IKÜM artikkel 5). Isikuandmete töötlemine peab olema seaduslik, õiglane ja läbipaistev. Läbipaistvuse põhimõte eeldab, et kogu isikuandmete töötlemisega (sh andmete kogumisega) seotud teave on lihtsalt kättesaadav, arusaadav ning selgelt sõnastatud. Läbipaistvuse tagamiseks on vastutaval töötlejal vajalik koostada ja avaldada oma andmekaitsetingimused. Andmekaitsetingimuste sisu reguleerivad IKÜM artiklid 12 – 14. Täpsemalt on võimalik läbipaistvuse osas lugeda ka inspektsiooni koostatud isikuandmete töötleja üldjuhendi lehekülgedelt 43 – 45 (10. peatükk. Läbipaistvus[1]).

Kontrollisime varasemalt Living Minerals OÜ andmekaitsetingimusi ning leidsime, et need ei vasta IKÜM artiklites 12-14 esitatud nõuetele.

Järgnevalt www.mineralgarden.org (Living Minerals OÜ) andmekaitsetingimuste analüüs:

1. Andmekaitsetingimuste punktis 3 olete sätestanud klientide isikuandmete töötlemise. Punkti 3.1 kohaselt võib andmetöötleja töödelda järgnevaid andmesubjekti isikuandmeid: ees- ja perekonnanimi; telefoninumber; e-posti aadress; kohaletoimetamise aadress; arvelduskonto number; maksekaardi detailid; IP-aadress.
2. Punktis 3.3 olete viidanud üldiselt IKÜM-i artiklile 6 ja öelnud, et *„isikuandmete töötlemise õiguslik alus on isikuandmete kaitse üldmääruse paragrahv 6 lg 1 p-d a,b,c ja f.“*
3. Selgitan, et isikuandmete töötlemise aluseks ei saa olla terve IKÜM-i artikkel 6. Andmesubjektide ja üldise õigusselguse huvides tuleb õiguslikule alusele viidata selgelt ja arusaadavalt. Näiteks: toote välja erinevad isikuandmete liigid, mida töötlete (ees- ja perekonnanimi, telefoninumber jne) ja iga välja toodud liigi taha kirjutate ka õigusliku aluse. Andmesubjektil peab olema arusaam sellest, millisel õiguslikul alusel

[1] Isikuandmete töötleja üldjuhend, Andmekaitse Inspektsioon – Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf (29.03.2021)

neid andmeid töödeldakse.

4. Märgin selguse huvides, et IKÜM-is on *„artiklid*“, mitte *„paragrahvid“.* Olite ilmselt ekslikult märkinud oma andmekaitsetingimuste punktis 3.3 *„paragrahv“.*
5. Isiklik soovitus (mitte kohustus) oleks 3 peatükk andmekaitsetingimustes teha tabeli kujul, mille esimeses veerus toote välja andmetüübid, teises veerus õigusliku aluse ja kolmandas veerus töötlemise eesmärgi.
6. Kujutletav näide tabelist:

Andmetüüp	Õiguslik alus	Töötlemise eesmärk
Ees- ja perekonnanimi	IKÜM artikkel 6 lg 1 p b (leping)	Kliendiga sõlmitud lepingu täitmine

7. Selgitan, et eelnevalt toodud näide ei ole kohustuslik vorm. Sellegipoolest tagab selline lähenemine arusaama sellest, kuidas ja millisel alusel ning milliseid andmeid töödeldakse.
8. Andmekaitsetingimuste punktis 3.4 olete välja toonud isikuandmete töötlemise eesmärgid ning isikuandmete säilitamise vastavalt töötlemise eesmärgile. Siinkohal soovitab AKI säilitamise tähtajad lisada ülal näidatud tabelisse neljanda veeruna. Näide:

Andmetüüp	Õiguslik alus	Töötlemise eesmärk	Säilitamise tähtaeg
Ees- ja perekonnanimi	IKÜM artikkel 6 lg 1 p b (leping)	Kliendiga sõlmitud lepingu täitmine	Lepingu lõppemiseni

9. Selgitan, et töötlemise eesmärkide sätestamisest on vähe kasu, kui pole selge, milliseid andmeid täpsemalt töödeldakse. Kui andmekaitsetingimuste punktis 3.4.1 olete sätestanud, et töötlemise eesmärk on julgeolek ja turvalisus, siis tekib küsimus, milliste andmete töötlemise eesmärk on julgeolek ja turvalisus? See pole üheselt selge ja seetõttu oleks mõistlik kasutada ülal viidatud tabelsüsteemi või muul viisil selgitada/punkte täiendada vastavate isikuandmete liikidega.
10. Täielikult on andmekaitsetingimustest puudu IKÜM artikkel 13 lg 1 punktist d tulenev teave, mis sätestab, et andmete kogumise korral andmesubjektilt, teeb vastutav töötleja andmesubjektile teatavaks teabe vastutava töötleja või kolmanda isiku õigustatud huvide kohta. Andmekaitsetingimustes pole välja toodud asjakohast kolmandate osapoolte õigustatud huvi isikuandmete töötlemisel, kuigi punktis 3.3 on see ühe töötlemise õigusliku alusena välja toodud.
11. Samuti puudub andmekaitsetingimustest teave kolmandatesse riikidesse edastatava teabe kohta. Näiteks olid teie enda kaasuse näitel lekkinud failid veebiserveris, mille teenust pakub Ameerika Ühendriikide teenusepakkuja Bluehost. IKÜM artikkel 13 lg 1 punkt f kohaselt peab andmetöötleja avalikustama teabe selle kohta, et vastutav töötleja kavatseb edastada isikuandmeid kolmandale riigile või rahvusvahelisele organisatsioonile, ning teave kaitse piisavust käsitleva komisjoni otsuse olemasolu või puudumise kohta või IKÜM artiklis 46, 47 või 49 lõike 1 teises lõigus osutatud edastamise korral viide asjakohastele või sobivatele kaitsemeetmetele ja nende koopia saamise viisile või kohale, kus need on tehtud kättesaadavaks. Praegusel juhul puudub andmesubjektidel teave andmete Ameerika Ühendriikidesse edastamise kohta, mistõttu on ülimalt oluline, et see IKÜM-ist tulenev nõue oleks täidetud.

Andmekaitsetingimuste loomise taustast

12. Pean vajalikuks selgitada, et andmekaitsetingimused ei ole lihtsalt „teen ära, siis olen seadusega kooskõlas tingimused“. Andmekaitsetingimuste loomine algab arusaamast, kust, kuidas ja kuhu andmed liiguvad. Enamasti aitab selliseid asju tuvastada andmekaitseaudit, mille tegemiseks leiab internetiavarustest piisavalt materjali[2].
13. Ilmselt Teie ettevõtte puhul audit vajalik pole, sest andmetöötlus on väiksem võrreldes mõne IT-ettevõttega. Sellegipoolest peate te teadma, kuidas, millisel õiguslikul alusel ja miks andmeid töödeldakse. See arusaam peab jõudma ka andmesubjektini ja selleks ongi andmekaitsetingimused. Nagu enne mainitud sai, siis isikuandmete töötlemine peab olema seaduslik, õiglane ja läbipaistev ning neid eesmärke aitavad andmekaitsetingimused ka täita.

Võttes arvesse faktilisi asjaolusid ja asjaolu, et andmete töötlemine endiselt käib, kuid andmesubjektidel puudub adekvaatne teave andmete töötlemise kohta, leiab AKI, et kohustusliku ettekirjutuse tegemine antud asjas on vajalik rikkumise kõrvaldamiseks.

/allkirjastatud digitaalselt/
Mehis Lõhmus
jurist
peadirektori volitusel

[2] Näiteid audititest ja nende koostamisest – Kättesaadav: https://www.aki.ee/et/inspektsioon-kontaktid/auditid (29.03.2021)