21. juuni 2025

Lugupeetud `MAXIMA Estonia iOS/Android` äpi vastutav andmetöötleja

Kirjutan teile andmesubjektina EL isikuandmete kaitse üldmääruse ("IKÜM") raames, seoses minu isikuandmete töötlemisega teenuses `MAXIMA Estonia iOS/Android` äpis.

Kuupäeval 2025-04-06, teavitati teid kasutajakontode loendamise turvanõrkusest (*account enumeration vulnerability*), mis **lubab selleks volitamata isikutel kinnitada, kas konkreetse meiliaadressiga kasutaja on teie teenuses registreeritud**. Tänase seisuga näib, et see turvanõrkus on lahenduseta sisse logimise vormil, parooli lähtestamise vormil, kasutaja registreerimise vormil ja meiliaadressi vahetamise vormil (vt lisatud aruannet).

Minu isikuandmeid – täpsemalt fakti, et mul on kasutaja teie veebiteenuses – töödeldakse eelnevalt mainitud vormides viisil, mis võimaldab selle avaldamist selleks volitamata isikutele. Ma ei ole teadlik ühestki IKÜM artiklis 6 kirjeldatud seaduslikust alusest, mis lubaks sellist töötlemist, ega ole andnud selget nõusolekut sellisel kujul isikuandmete töötlemiseks ja võimalikuks avaldamiseks.

Seetõttu esitan järgnevad ametlikud taotlused:

1. IKÜM artikli 15 kohaselt taotlen, et esitaksite eesmärgi, viidates IKÜM artikli 6 järgi kehtivale õiguslikule alusele, mille alusel töödeldakse minu (eelnevalt kirjeldatud) andmeid viisil, mis muudab need haavatavaks kasutajakontode loendamisele selleks volitamata isikutele (s.t., avaldades, kas minu meiliaadress on teenuses registreeritud).
2. IKÜM artikli 18 kohaselt nõuan piirangut oma isikuandmete töötlemisele viisil, mis on haavatav kasutajakontode loendamisele (st, avaldades, kas minu meiliaadress on teenuses registreeritud). Väidan, et selline isikuandmete töötlemine on ebaseaduslik. Samuti olen vastu oma isikuandmete kustutamisele.
3. IKÜM artikli 21 kohaselt esitan vastuväite minu isikuandmete igasugusele töötlemisele eesmärgiga avaldada kasutajakonto olemasolu selleks volitamata isikutele, eelkõige kui sellist töötlemist võidakse põhjendada töötleja õigustatud huvina. Selles kontekstis kaaluvad sellise huvi üles minu huvid, põhiõigused- ja vabadused isikuandmete kaitsele ja privaatsusele.

Palun vastake neile taotlustele e-posti teel ühe kuu jooksul, nagu on sätestatud IKÜM artiklis 12(3), ja täpsustage võetud meetmeid nende täitmiseks. Juhul, kui te ei suuda esitada rahuldavat vastust, mis käsitleb neid muresid ja parandab igasuguse ebaseadusliku töötlemise nõutud ajavahemiku jooksul, esitan vastavalt IKÜM artiklile 77 kaebuse asjakohasele järelvalveasutusele (Andmekaitse Inspektsioon).

Lugupidamisega

Gregor Eesmaa
isikukood: 39806170815
meiliaadress: gregoreesmaa1@gmail.com
/ allkirjastatud digitaalselt /

21st June 2025

Dear Data Controller of `MAXIMA Estonia iOS/Android` app,

I am writing to you as a data subject under the EU General Data Protection Regulation ("GDPR") regarding the processing of my personal data by `MAXIMA Estonia iOS/Android` app.

On 2025-04-06, you were notified of account enumeration security vulnerability that **allows unauthorised parties to verify whether a user with a specific email address is registered with your service**. As of today, this vulnerability appears to remain unresolved on the login form, password reset form, account registration form and email change form (see attached report).

My personal data – specifically, the fact that I hold an account with your online service – is being processed in the previously mentioned forms in a manner that allows its disclosure to any unauthorised party. I am not aware of any legal basis under GDPR Article 6 that would allow such processing, nor have I provided explicit consent for this specific form of processing and potential disclosure.

Accordingly, I make the following formal requests:

1. Pursuant to Article 15 of GDPR, I request you provide the purpose, citing a valid legal basis under GDPR Article 6, for processing my personal data (as described above) in a manner that is vulnerable to account enumeration by unauthorised parties (i.e., revealing whether my email address is registered within the service).
2. Pursuant to Article 18 of GDPR, I request the restriction of my personal data being processed in a manner vulnerable to account enumeration (i.e., revealing whether my email address is registered within the service). I contest the lawfulness of this specific processing. I also oppose erasure of my personal data.
3. Pursuant to Article 21 of GDPR, I object to any processing of my personal data for the purpose of revealing account existence to any unauthorised party, particularly where such processing might be claimed under legitimate interests. My interests, fundamental rights and freedoms to data protection and privacy override such interests in this context.

Please respond to these requests over email within the statutory time limit of one month, as per Article 12(3) of GDPR, and confirm the measures taken to comply with it. In case of failure to provide a satisfactory response, addressing these concerns and rectifying any unlawful processing within the required timeframe, I will file a formal complaint with the competent supervisory authority (Andmekaitse Inspektsioon) in accordance with Article 77 of GDPR.

Kind regards,

Gregor Eesmaa
personal code: 39806170815
email address: gregoreesmaa1@gmail.com
/ signed digitally /