Outlook

Re: Küsimus GDPR'i ja emaili aadresside kohta

From Eleri Karu - AKI <eleri.karu@aki.ee>
Date Mon 2025-12-15 13:42
To Ingmar | Adfinity <ingmar@adfinity.ee>

Tere!

Pöördusite Andmekaitse Inspektsiooni (AKI) poole seoses konto olemasolu tuvastatavuse turvanõrkuse kohta. On igati tervitatav, et pikaajalise kogemusega süsteemiarendajad tunnevad huvi andmekaitse ja turvalisuse kokkupuutepunktide vastu.

Esmalt selgitan et AKI ei saa selgitustaotlusele vastates anda konkreetsele juhtumile siduvat õiguslikku hinnangut, see on võimalik ainult järelevalvemenetluses. Seetõttu annan Teile järgnevalt üldised selgitused. Lisaks märgin ka märgukirjale ja selgitustaotlusele vastamist reguleerib märgukirjale ja selgitustaotlusele vastamise ning kollektiivse pöördumise esitamise seadus (edaspidi MSVS). Sellest tulenevalt on AKI-l kohustus anda õigusalaseid selgitusi inspektsiooni tegevuse aluseks olevate õigusaktide ja asutuse pädevuse kohta. Õigusalaste selgituste andmine ei tähenda õigusabi andmist.

Andmekaitse reeglid ehk isikuandmete kaitse nõuded[1] kohalduvad isikuandmetele. Isikuandmed on igasugune teave, mille abil on võimalik otseselt või kaudselt tuvastada füüsiline isik. Näiteks on isikuandmed nimi, isikukood, e-posti aadress, asukohateave, võrguidentifikaator. [2]

Teie tõstatatud konflikt kasutajamugavuse (UX) ja privaatsuse/turvalisuse vahel on praktikas üks sagedasemaid arutelukohti. AKI vaates on lähtepunktiks põhimõte: e-posti aadress on enamasti isikuanne ning teave selle kohta, kas konkreetne isik on mingi teenuse kasutaja või mitte, on teave, mille avaldamiseks peab olema õiguslik alus. Veebivormil suvalisele pärijale selle info kuvamine ei ole üldjuhul põhjendatud ega turvaline.

Toon välja ka mõju inimesele ehk miks on konto olemasolu tuvastatavus reaalne oht:

- Spetsiifiline õngitsus e. harpuunimine (*spearfishing*): Teadmine, et inimene on konkreetse teenuse (nt panga, terviseportaali või tutvumisäpi) klient, võimaldab kurjategijatel luua väga usaldusväärseid ja personaalseid pettusekirju, mille ohvriks langemise tõenäosus on suur. Ja me teame, et Eestis on see trend olenemata aastaajast kõrge.
- Kui ründaja teab, et konto kindlasti eksisteerib, saab ta kontsentreerida oma ründed (*credential stuffing* või *password spraying*) just sellele e-posti aadressile. See vähendab ründaja jaoks avastamise riski ja suurendab sisselogimise õnnestumise tõenäosust.
- Leke võib paljastada tundlikke seoseid (nt liikmelisus spetsiifilisel platvormil), mis riivab isiku privaatsust ja võib äärmuslikul juhul viia sotsiaalse häbimärgistamise või väljapressimiseni.

Seega, kui Teie arendatud süsteem ütleb registreerimisel "See e-mail on juba kasutusel", olete Te ründaja jaoks teinud ära esimese sammu luurest – sihtmärgi valideerimise.

Samuti ei ole selline käsitlus vaid Eesti eripära ja selline lähenemine on rahvusvaheline standard. Lisaks IKÜM-i nõuetele[3] leiab selle turvanõrkusega seotud viiteid ka küberturvalisuse standarditest. Nii OWASP ASVS kui ka NIST juhised rõhutavad, et autentimise ja parooli taastamise vastused peavad olema ühtsed. Veateated ei tohi avalikustada tundlikku infot ning küberhügieeni vaatest loetakse ainuüksi kasutajakonto olemasolu kinnitamist tundlikuks infoks.

Arendaja kohustus on tagada, et kõrvalised isikud ei saaks süsteemist välja pärida andmeid, milleks neil õigust pole. Mõistan Teie muret kasutajamugavuse pärast. Siiski, andmekaitse ja -turbe põhimõte on, et mugavus ei tohi tulla turvalisuse arvelt.

Mõned üldised soovitused veebilehe arendajatele:

- Kui avalik veateade veebilehel ("See e-mail on juba kasutusel") on turvarisk, siis tuleb info edastada kanalisse, millele on ligipääs ainult konto omanikul – ehk e-postkasti.
- Veebileht annab neutraalse vastuse, süsteem saadab teavituse e-mailile. See tagab, et info konto olemasolust jõuab vaid õige isikuni.
- Teie toodud näide mitme e-mailiga inimesest on asjakohane. Siin on lahenduseks selgitav tekst kasutajaliideses (nt "Proovi vajadusel ka teisi aadresse"), mitte andmebaasi sisu avalikustamine veateate kaudu.

Saade keskendus lihtsale sisselogimisele ja registreerimisele, kuid probleem on tegelikult laiem ja vaatama peab tervikpilti. Leke võib toimuda ka avaliku API kaudu (mis tagastab erinevaid veakoode, mida UI võib-olla ei näita, aga mida ründaja näeb), parooli taastamise protsessis või mitmikautentimises (MFA). Samuti ei saa me ette kirjutada kõiki võimalikke lahendusi, sest iga süsteem on erinev.

Tänane hea tava on aga liikunud suunas, kus veebivormid on n.ö tummad ehk ei reeda infot ja tegelik infovahetus toimub kontrollitud kanalites (e-post vms kanal). See võib tunduda esmapilgul kasutajale sammu võrra tülikam, kuid see on vajalik samm, et meie e-posti aadressid ei oleks avalikud sihtmärgid küberkurjategijatele.

Loodan, et minu selgitustest oli abi.

Lugupidamisega

Eleri Karu
Andmeturbe ekspert
Eleri.karu@aki.ee

ERAELU KAITSE JA RIIGI LÄBIPAISTVUSE EEST
Tatari 39 | 10134 Tallinn | Eesti
LinkedIn | YouTube

ANDMEKAITSE INSPEKTSIOON

[1] Isikuandmete kaitse nõuded tulevad eelkõige Euroopa Parlamendi ja nõukogu määrusest (EL) 2016/679 (isikuandmete kaitse üldmäärus ehk IKÜM).
[2] IKÜM art 4 p 1.

[3] IKÜM artikkel 5 lõige 1 punkt f (terviklikkus ja konfidentsiaalsus), artikkel 25 (lõimitud ja vaikimisi andmekaitse ja artikkel 32 (töötlemise turvalisus).

From: Ingmar | Adfinity <ingmar@adfinity.ee>
Sent: Thursday, December 11, 2025 17:43
To: Eleri Karu - AKI <eleri.karu@aki.ee>
Subject: Küsimus GDPR'i ja emaili aadresside kohta

> **Tähelepanu!** Tegemist on välisvõrgust saabunud kirjaga.
> Tundmatu saatja korral palume linke ja faile mitte avada.

Tere!

Eile juhiti minu tähelepanu Pealtnägijas esinenud loo osas, kus veebilehtedel emaili järgi kasutaja tuvastamist nimetati “turvanõrkuseks”.
Olles ise 20+ aastat tegelenud süsteemide arendamisega (kaasa arvatud veebilehed), siis sain aru küll mõttest, kuid samas ühtegi lahendust välja ei toodud.

Murekohad jaotaks loo põhjal kaheks – uudiskirjaga liitumised ja veebilehe kontod:

1) Uudiskirjaga liitumise puhul on asi võrdlemisi lihtne – olenemata olukorrast anda kasutajale üks üldine vastus (a’la “täname uudiskirjaga liitumast”). Kuna uudiskirjaga liitumine on üldiselt eraldi süsteem, siis ei tähenda see jällegi konkreetset konto olemasolu ja keegi või liituda sellega ka 10 aastat tagasi.

2) Veebilehe kontodega läheb nüüd keerulisemaks – kui emaili alusel kasutaja tuvastamine läheb vastuollu GDPR’iga, siis milline on lahendus?

Kontode kasutamisega seoses on veebilehtel lisa funktsionaalsus:

* **Sisselogimine** – siin võimalik anda vea korral üldine vastus, seega asi lahendatud.

* **Parooli taastamine** - siin on võimalik anda jällegi üldine vastus (a’la “juhul kui selle emailiga kasutaja on süsteemis olemas, saate emaili koos lingiga”). Küll aga tekitab see kohe probleemi, kus paljudel on mitu emaili (näiteks töö, personaalne, peale abielu uue nimega jne) ning kuidas õige email üles leida? Kõik ühe kaupa läbi proovida ja loota, et äkki mingi meili peale tuleb kiri?

* **Registreerimine** - täna praktiliselt kõik veebilehed kasutavad kasutaja tuvastamise emaili aadressi ja parooli.
Kui süsteemis on juba kasutaja olemas selle emailiga, siis on hea tava anda sellest ka kasutajale teada (ehk ta saab aru, et ilmselt on tal juba konto olemas ja proovib seejärel hoopis sisse logida). Emailiga sisselogimiseks peaks emaili aadress olema süsteemis unikaalne – kontrollitakse ju selle ja parooli kattuvust. Siin ei ole kasu ka sellest, kui anda üldist veateadet – näiteks “nende andmetega ei ole võimalik registreerida”. See on kasutaja jaoks väga segadust tekitav ning esimene mõte sellise üldise teavituse peale tuleb see, et sait on katki.
Kuna tavaliselt küsitakse registreerimiseks ainult emaili ja parooli, siis igasugune veateade annab siin märku sellest, et kasutaja selle emailiga on olemas.
Ei näe, et sama emailiga mitu korda registreerimise võimalus pakuks ka lahendust – tekitab süsteemides palju segadust, kuna tekivad mitmed kontod sama emailiga ning lööb sassi ka muu funktsionaalsuse nagu parooli taastamine, tellimuste ajalugu jne. Samuti ei saa kasutaja siis enam aru, millist kontot ta hetkel kasutab.

Kuidas see “turvanõrkus” registreerimise etapis siis lahendada?

Kui registreerimise pool jätta nüüd “parandamata”, siis pole ju otseselt mõtet ka teistel “parandustel”.
Täpsemad veateated on täna mõeldud ikkagi kasutaja sõbralikkuse eesmärgil ja “parandused” siin teeksid kasutajate jaoks lihtsalt elu keerulisemaks.

Kui suur “turvanõrkus” või GDPR rikkumine täna üksnes emaili alusel konto olemasolu tuvastamine on?

Ma julgeks väita, et sellisel viisil on täna praktiliselt kõikidel lehtedel konto olemasolu tuvastatav, millel on võimalus endale konto luua emaili alusel.
Samuti võttes ette näiteks Google’i konto loomise – kui selle aadressiga on konto olemas, siis tuleb veateade.
Pealtnägijas toodi välja Circle K ja kuidas peaministri emailiga on seal konto olemas – teoorias aitab küll inimest profileerida aga praktikas ma kahtlen, et sellest reaalset kasu on. Täna on konto loomine praktiliselt iga tellimuse või liikmelisuse programmi aluseks. Kui nüüd äkki peaministril on konto ka Alexelas, Nestes, Terminalis või mujal, siis võib ju ainult oletada, et äkki ta sõidab autoga või on kunagi autot omanud?
Ühtlasi paljud veebilehed ei nõua emaili kinnitust registreerimisel ja konto jääb sinna alles praktiliselt igaveseks – seega võib tegelikult iga inimene luua konto kuhugi veebilehele ilma reaalset ligipääsu sellele omamata. Sama kehtib ka uudiskirjadega liitumisel – see küll ei ole ilus aga sisestada võib ju üks kõik kelle emaili.

Kas seda loetakse nüüd GDPR’i rikkumiseks praegu ainult Eestis või ka mujal maailmas?
Mis on need täpsemad punktid / lõigud millest siin lähtutakse?

Best wishes / Parimate soovidega,

Ingmar Haak
AdFinity OÜ
+372 510 1230