

Tähelepanu juhtimine

Andmekaitse Inspeksioonile teadaolevalt esineb osades Eesti veebiteenustes turvanõrkus, mis võimaldab tuvastada, kas kasutaja on veebiteenusega seotud. Veebiteenused kasutavad kontotunnustena tihtipeale meiliaadresse. Enamlevinult on aga meiliaadressid kujul, mille abil on võimalik luua lihtne seos konkreetse inimesega. Sellisel juhul tuleb arvestada, et tegemist on isikuandmetega.

Konto tuvastatavus kujutab endast privaatsusriski ning võib viia isikuandmete kaitse rikkumiseni. Veebiteenused vastutavad nii enda tegevuse raames toimuva andmetöötluse kui ka tõhusate riskimaandamise meetmete rakendamise eest, mistõttu peame vajalikuks juhtida tähelepanu nimetatud turvanõrkusele ning selle likvideerimise vajalikkusele.

Isikuandmed ja nende kaitse tagamine

[Isikuandmete kaitse üldmääruse](#) (IKÜM) kohaselt on isikuandmed igasugune teave tuvastatud või tuvastatava inimese kohta. Isikuandmeteks võivad olla inimese nimi, isikukood, asukohateave, võrguidentifikaator või andmed, mis võimaldavad tuvastada inimest tema füüsiliste, geneetiliste, vaimsete, majanduslike, kultuuriliste või sotsiaalsete tunnuste kaudu. Seetõttu on tuvastatava inimese e-posti aadress, telefoninumber või muu unikaalne identifikaator ning fakt selle seotusest konkreetse teenusega isikuandmed.

Isikuandmete töötlemisel tuleb järgida määruses sätestatud põhimõtteid. Usaldusvääruse ja konfidentsiaalsuse põhimõtte kohustab isikuandmeid töötleva viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustamise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid. Rakendama peab asjakohaseid tehnilisi ja korralduslikke meetmeid võttes arvesse teaduse ja tehnoloogia viimast arengut, rakendamise kulusid ning töötlemise laadi, ulatust, konteksti ja eesmärke, samuti töötlemisest tulenevaid füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohte.

Isikuandmete töötlemine ja selle eest vastutav andmetöötaja

[Isikuandmete töötlemine](#) on igasugune andmetega tehtav toiming, mis võib hõlmata andmete kogumist, salvestamist, korrastamist, säilitamist, muutmist, juurdepääsu võimaldamist, avaldamist, avalikustamist, päringute teostamist, väljavõtete tegemist, kasutamist, edastamist, ristkasutamist, ühendamist, üleandmist, sulgemist, kustutamist või hävitamist sõltumata toimingute teostamise viisist või kasutatavatest vahenditest.

See tähendab, et ka e-posti ja/või kontoga seotud andmete nähtavaks tegemine veebiteenuse poolt on isikuandmete töötlemine, mis peab põhinema õiguslikul alusel ja olema kooskõlas isikuandmete kaitse põhimõtetega.

Vastutav töötleja on vastavalt üldmäärusele füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid. Olenemata sellest, kas isikuandmeid töötleb vastutav või volitatud töötleja, kohaldub kohustus tagada asjakohased meetmed mõlemale.

Veebiteenused, mis töötlevad isikuandmeid enda eesmärkidel ja vahenditega, on vastutavad andmetöötlejad üldmääruse mõistes.

Inimeste õigused isikuandmete töötlemisel

Andmekaitse Inspektsioon juhib tähelepanu inimeste õigustele, eelkõige isikute õigusele [tutvuda oma isikuandmetega](#) (artikkel 15), [õigusele isikuandmete töötlemise piiramisele](#) (artikkel 18) ning [õigusele esitada vastuväiteid](#) (artikkel 21). Kui inimene on esitanud vastava taotluse, siis tuleb andmetöötlejal sellele vastata hiljemalt ühe kuu jooksul.

Veebiteenustel tuleb aidata kaasa kasutajate privaatsuse tagamisele, andes informatsiooni selges ja lihtsas keeles ning kokkuvõtlikult, arusaadavalt ja lihtsasti kättesaadavas vormis. Juhul, kui veebiteenus ei võta kasutusele meetmeid, mis vastavad esitatud taotlusele, tuleb teatada viivitusega meetmete võtmata jätmise põhjused ning selgitada isikule võimalusi esitada järelevalveasutusele kaebus ja kasutada õiguskaitsevahendeid.

Eesti veebiteenustes konto tuvastatavus

Andmekaitse Inspektsioonile teadaolevalt on Teie veebiteenus haavatav turvariskile, mille käigus on võimalik selgitada välja, kas kindel e-posti aadress on teenuses registreeritud või mitte. Turvarisk esineb ühel või mitmel järgmistest olukordadest:

- Sisselogimisvorm;
- Parooli lähtestamise vorm;
- Konto registreerimisvorm;
- E-posti aadressi muutmise vorm;
- Konto otsing;
- MFA (mitmikautentimine) / OTP (ühekordne parool);
- Avalik API (rakendusliides).

Teateid võidakse kuvada stiilis:

„Sellise e-posti aadressiga kasutajat ei ole“;

„Selle e-posti aadressiga kontot pole olemas“;

„Sellise aadressiga konto on juba loodud“;

või mõne muu tehnilise indikatsioonina, mis võimaldab järeldada, kas isikul on konkreetsel platvormil konto või mitte.

Kuivõrd tulenevalt eeltoodust on enamikel juhtudel e-post käsitletav isikuandmetena, millel on kindel seos kindla isikuga ja selle võimalik kuvamine kõrvalistele isikutele on oluline turvarisk nii konfidentsiaalsuse, kui ka isikuandmete kaitse vaates üldisemalt, juhib Andmekaitse Inspektsioon Teie tähelepanu asjaolule, et selliselt ei ole tagatud kooskõla IKÜM-ga, mis võib viia kaugeleulatuvate tagajärgedeni nende suhtes, kes oma isikuandmed on Teile usaldanud.

Miks on oluline turvarisk likvideerida?

Andmeleketes varastatud isikuandmeid sh e-posti aadresse, on küberkurjategijatel lihtne hankida. Kui teenus paljastab lihtsal moel, et konkreetne e-posti aadress on juba kasutusel ning kurjategijal peaks mingil põhjusel olema selle aadressi suhtes kõrgendatud huvi, või tema käsutuses on näiteks ka sama e-posti aadressiga seotud võimalikud erinevad salasõnad, on tõenäosus inimese konto ülevõtmiseks suur. CAPTCHA aitab küll kaitsta automaatpäringuid tegevate veebirobotite eest, aga kui ründajal on huvi mõne konkreetse e-posti aadressi osas, saab ta alati ka käsitsi vastavad päringud teha ja robotilõksust mööda minna.

Teades, et inimene on konkreetse teenuse klient, saavad kurjategijad lihtsal viisil esineda teenusepakkuja nimel, saates inimesele õngitsuskirja, kus inimest suunatakse minema justkui autentsele veebilehele (mis tegelikult on kurjategijate poolt kloonitud) ning meelitama inimest lehel sisestama tundikke andmeid (nt maksekaardi number või SmartID PIN koodid) eesmärgiga petta välja raha.

Küberkuritegevus on Eestis saanud väga tõsiseks probleemiks. Inimestelt ja ettevõtetelt välja petetud summadest või küberrünnakutest teevad regulaarseid ülevaateid Politsei-ja Piirivalveamet ning Riigi Infosüsteemi Amet.

Isikuandmete konfidentsiaalsuse tagamine on andmekaitse üks peamisi põhimõtteid, millega teenusepakkuja nii konteksti kui laiemalt ohupilti silmas pidades peab arvestama. Alati tuleb mõelda, kas olemasolevad tehnilised lahendused ja sõnastused on piisavad, et kolmandad isikud ei saaks tuvastada inimese andmestiku seotust konkreetse e-teenusega.

Mittepiisava konfidentsiaalsuse puhul võivad realiseeruda mitmed riskid: nt sihitud küberrünnakud, andmete lekkimine, profileerimine, väljapressimine ning ahistamine. Neid riske aitavad ära hoida meetmed, mis tagavad piisava turvalisuse taseme, sh konfidentsiaalsuse.

Teenuse andmekaitseõuetega vastavusse viimine

Teenuse praegune praktika ei vasta vähemalt osaliselt andmekaitseõuetele. Näiteks uue konto loomisel (selle asemel, et juba kasutuses oleva e-posti aadressi osas veateade kuvada) saaks saata täiendava e-kirja juhistege, et registreerimisprotsess lõpule viia. Turvalisuse tagamiseks tuleks sisselogimisel kuvada näiteks üldine veateade, et kasutajanimi ja/või salasõna ei ole õige, mitte täpsustama, milline sisestatud andmetest oli vale. Oluline on hinnata ka teisi teenuse osasid, kus teated või protsessid võivad avaldada liigset infot.

Turvalisuse ja IKÜM-iga kooskõla tagamiseks peab vastutav või volitatud töötaja hindama töötlemisega seotud ohtusid ja rakendama asjaomaste ohtude leevendamiseks vajalikke meetmeid.

Käesoleva kirjaga juhib Andmekaitse Inspeksioon tähelepanu vajadusele kõrvaldada veebiteenustes esinev turvarisk, mis võimaldab konto tuvastamist, et vähendada privaatsus- ja turvariske.