ANDMEKAITSE INSPEKTSIOON

Lp Jüri Mets
Mjproduction MTÜ
jurimets@mail.ru

14.01.2025 nr 2.1-1/24/1088-2692-10

Tähelepanu juhtimine

Andmekaitse Inspektsioon sai kaebuse, mille kohaselt on MJproduction MTÜ lisanud kaebaja kohta käiva pildi oma veebilehele aadressil https://mjproduction.ee/. Kaebaja soovis tema andmete kustutamist, kuid ei saanud Teiega ühendust.

Saatsin kaebuse saamise järgselt Teile pöördumise edastamise vastamiseks, millele lubasite koheselt ka vastata. Kuivõrd tähtaegselt vastust ei laekunud edastasin Teile meeldetuletuse, misjärel andsite teada, et Teie server kukkus kokku ning kõik kirjad, sh inspektsiooni pöördumine, läksid kaduma. Probleemi põhjustas kõvaketas, mis põles läbi ja andmed ei olnud varundatud.

Kinnitasite, et andmed ei ole lekkinud, sest server sisaldas vaid mjproduction.ee lõpuga e-kirju ning et kliendiandmete jaoks on Teil kasutusel eraldi server.

Esmalt selgitan, et isikuandmed on isikuandmete kaitse üldmääruse (IKÜM) kohaselt igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta, keda saab otseselt või kaudselt tuvastada, eelkõige selliste tunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal (artikkel 4 p 1).

Seega, ka ettevõtte e-kirjad võivad sisaldada isikuandmeid. Näiteks kliendi nimi ja e-mail või telefoni number. Samuti võivad tööalased e-kirjad sisaldada ka töötajate isikuandmeid. Paljudel juhtudel kasutavad töötajad töö e-posti isiklikuks otstarbeks mugavuse, aja kokkuhoiu ja turvalisuse tõttu (töö e-posti loetakse reeglina iga päev või lausa terve päeva jooksul, mistõttu pole vaja erapostkasti pidevalt sisse logida, et kontrollida, ega pole uusi kirju tulnud). Isegi, kui töötaja ei kasuta e-posti aadressi isiklikuks otstarbeks, peab tööandja siiski arvestama, et sinna võivad paratamatult sattuda isikliku sisuga kirjad, sest kunagi ei saa 100% välistada sissetulevaid erakirju, kolleegide kirjad üksteisele võivad olla eraviisilise sisuga ning kirjad võivad olla eraviisilise sisuga ka ainult osaliselt.

Samuti selgitan, et isikuandmete töötlemiseks peab olema õiguslik alus – kas isiku nõusolek või muu seadusest tulenev alus (artiklid 5 ja 6). Isikuandmete töötlemine peab vastama põhimõtetele, mis nõuavad andmete seaduslikku, ausat ja läbipaistvat töötlemist, eesmärgipärast kogumist, minimaalsuse, täpsuse, säilitamise piirangute ja turvalisuse tagamist (IKÜM artikkel 5 lg 1). Andmetöötleja on kohustatud järgima neid põhimõtteid igas isikuandmete töötlemise etapis.

Täpsemalt saab isikuandmete töötlemist puudutavate nõuete ja kohustuste kohta lugeda Andmekaitse Inspektsiooni isikuandmete töötleja üldjuhendist.

Erineva tõenäosuse ja tõsidusega ohud füüsiliste isikute õigustele ja vabadustele võivad tuleneda isikuandmete töötlemisest selle põhimõtte vastaselt. Andmesubjektid võivad jääda ilma oma õigustest ja vabadustest või kontrollist oma isikuandmete üle. Füüsiliste isikute õiguste ja vabaduste kaitsmine isikuandmete töötlemisel eeldab asjakohaste tehniliste ja korralduslike meetmete võtmist, et tagada IKÜM-i nõuete täitmine[1].

Vastavalt IKÜM artikkel 4 lg 1 p-le 12 on isikuandmetega seotud rikkumine turvanõuete rikkumine, mis põhjustab edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu. Näiteks võivad sellised rikkumised olla õigustamatu isikuandmete avaldamine (nt süsteemis või kodulehel isikuandmete avaldamine) või küberründe tagajärjel hävitatud või lekkinud andmed.

Intsidendiga on ka tegemist siis, kui toimub turvaintsident, mille tõttu ei ole isikuandmed teatud aja jooksul kättesaadavad või lähevad kaotsi, kuna andmetele juurdepääsu puudumine võib märkimisväärselt mõjutada füüsiliste isikute õigusi ja vabadusi. Selguse huvides olgu öeldud, et kui isikuandmed ei ole kättesaadavad kavandatud süsteemihoolduse tõttu, ei ole see turvanõuete rikkumine.

Eelnevast selgitusest tulenevalt juhin tähelepanu, et võtaksite vastu vajalikud meetmed (nt koolitada töötajaid isikuandmete seotud rikkumiste tuvastamisel ja kirjeldamisel või vajadusel täiendada sisedokumente) IKÜM nõuete täitmiseks.[2]

Vastavalt IKÜM artikkel 33 lg-le 5 on vastutaval andmetöötlejal isikuandmete seotud rikkumise korral kohustus intsident dokumenteerida. Rikkumiste dokumenteerimine on seotud IKÜM artikli 5 lg-s 2 sätestatud vastutuse põhimõttega. Kuivõrd andmetöötleja peab kõik rikkumised dokumenteerima, on soovituslik pidada sisemist registrit rikkumiste kohta. Registri ülesehitus on iga andmetöötleja enda otsustada, kuid teatavad elemendid peavad siiski olemas olema, näiteks IKÜM artikli 33 lg-s 5 on sätestatud, et kirjas peavad olema rikkumise põhjused, toimunu kirjeldus, mõjutatud isikuandmed ja võetud parandusmeetmed.

IKÜM 33 ja 34 nõuete paremaks täitmiseks oleks hea, kui andmetöötleja oleks sisemistes kordades või juhendites reguleerinud intsidentide haldamise protsessi, millega on kehtestatud kord, mida järgida pärast rikkumise avastamist, sealhulgas juhised selle kohta, kuidas intsidendi ulatust piirata, seda ohjata ja andmed taastada ning kuidas ohtu hinnata ja rikkumisest teatada.

Juhul, kui intsidendi tagajärjel kujutab rikkumine endast tõenäoliselt ohtu füüsiliste isikute õigustele ja vabadustele, tuleb põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul pärast sellest teada saamist teavitada Andmekaitse Inspektsiooni (artikkel 33) ning andmesubjekte (artikkel 34).

Eeltoodust tulenevalt juhin tähelepanu, et Teil tuleb edaspidi intsidendi järgselt koheselt veenduda, et isikuandmed ei oleks puudutatud ning vajadusel teavitada Andmekaitse Inspektsiooni ja/või andmesubjekte.

Samuti tuleb tagada, et isikuandmete töötlemisel on IKÜM-is sätestatud reeglid täidetud.

Käesolevale tähelepanu juhtimisele inspektsioon vastust ei oota.

[1] Vt ka IKÜM art 25 ja 32.
[2] Täiendavalt soovitan tutvuda ka Euroopa Andmekaitsenõukogu suunistega 9/2022, mis käsitlevad isikuandmetega seotud rikkumisest teatamist isikuandmete kaitse üldmääruse alusel. (Versioon 2.0, vastu võetud 28. märtsil 2023)

Lugupidamisega

(allkirjastatud digitaalselt)

Kirsika Kuutma
jurist
peadirektori volitusel