



ANDMEKAITSE INSPEKTSIOON

Lp juhatuse liikmed
My Fitness AS
myfitness@myfitness.ee
andmekaitse@myfitness.ee

Meie 11.04.2025 nr 2.2-10/25/978-2

Tähelepanu juhtimine

Andmekaitse Inspeksioon (AKI) sai märgukirja seoses My Fitness AS-i spordiklubi liikmeid ja töötajaid koondava andmebaasiga. Seetõttu juhime My Fitness AS-i tähelepanu isikuandmete kaitse nõuetele.

Isikuandmete kaitse peamised nõuded tulenevad [Euroopa Parlamendi ja nõukogu määrusest \(EL\) 2016/679](#) (isikuandmete kaitse üldmäärus ehk IKÜM), isikuandmete kaitse seadusest ning vastavatest eriseadustest. Isikuandmete töötlemisel tuleb tagada isikuandmete töötlemise põhimõtete järgimine.

1. Seaduslikkus, õiglus ja läbipaistvus.

Isikuandmeteks on igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta. Tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada.

Igasugune isikuandmete töötlemine peab olema seaduslik ja täielikult kooskõlas isikuandmete kaitse nõuetega. Seega peab isikuandmete töötlemiseks esinema vähemalt üks IKÜM art 6 lg-s 1 toodud õiguslik alus (eriliigiliste isikuandmete puhul IKÜM art 9 lg 2). Isikuandmete töötlemine peab olema õiglane, s.t et isikuandmeid käsitletakse viisil, mida inimene võib mõistlikult eeldada ning andmeid ei tohi töödelda viisil, mis on andmesubjektile põhjendamatult kahjulik, ootamatu või eksitav.

Lisaks peab isikuandmete töötlemine olema läbipaistev. Selleks peab kogu isikuandmete töötlemisega seotud teave olema andmesubjektile, antud juhul nii töötajatele kui ka klientidele, lihtsalt kättesaadav, arusaadav ning selgelt sõnastatud.

2. Eesmärgipärasus, minimaalsus, õigsus

Isikuandmete töötlemine peab alati olema seotud kindla eesmärgiga ja andmeid tuleb koguda nii vähe kui võimalik teatud eesmärgi saavutamiseks. Igaks juhuks andmete kogumine on ebaseaduslik. Isikuandmeid ei tohi hiljem kasutada uuel eesmärgil, mis on algse eesmärgiga vastuolus.

Selleks, et hinnata, kas andmete kogumine ja säilitamine vastab eesmärgi piirangu ning võimalikult väheste andmete põhimõttele, tuleb:

- 1) tuua välja kõik andmete töötlemise eesmärgid, dokumenteerida ja teavitada nendest andmekaitsetingimustes;
- 2) veenduda, et nimetatud eesmärkide täitmiseks on tegelikult töödeldavad isikuandmed vajalikud, piisavad ja asjakohased.

Isikuandmete õigsus tähendab seda, et andmed on aja- ja asjakohased. Näiteks, kui klient teavitab oma kontaktandmete muutumisest, siis andmeid uuendatakse vastavalt või kui klient on keeldunud otseturustusest, siis süsteemis ei märgita tema kohta pakkumiste saamiseks nõusolekut.

3. Säilitamise piirang

Isikuandmetele tuleb määrata kindel säilitustähtaeg ja säilitamiseks peab olema konkreetne põhjus. Säilitustähtaja lõpus tuleb andmed kustutada, välja arvatud juhul, kui on selge põhjendus nende pikemaks säilitamiseks. Isikuandmeid ei tohi igaks juhuks lõputult säilitada.

4. Usaldusväärsus ja konfidentsiaalsus

Isikuandmete töötleja peab tagama, et andmed hoitakse kättesaamatult kolmandate isikute eest, et ei oleks volitamata ligipääse, juhuslikku kaotamist, hävimist või kahjustumist. Isikuandmete kaitsmiseks peavad olema rakendatud asjakohesed ja tõhusad turvameetmed.

Selleks, et oleks võimalik tagantjärele kontrollida, kes, millal ja kelle isikuandmeid on vaadanud/kasutanud/muutnud, peab olema loodud logimissüsteem. AKI hinnangul on logimine ainuke võimalik viis, mis võimaldab kontrollida seda, kas isikuandmeid on töödeldud eesmärgipäraselt. Ettevõtte peab suutma seejuures tagada, et andmebaasi ligipääs on isikutel, kellel selleks on töökohustustest tulenevalt vajadus. Volitamata isikutele andmebaasi juurdepääs tuleb piirata. Näiteks töötaja, kellel on andmebaasi töökohustustest tulenevalt ligipääs, peaks hea seisma, et arvuti juurest ka lühiajaliselt lahkudes volitamata isikud süsteemile ligi ei pääseks. Uudishimust andmetega tutvumine ei ole konfidentsiaalsuse põhimõttega kooskõlas.

5. Vastutus

Isikuandmete vastutav töötleja – ettevõtte, kes on määranud isikuandmete töötlemise eesmärgid ja vahendid – on kohustatud järgima IKÜM art-s 5 kehtestatud isikuandmete töötlemise põhimõtteid. Lisaks põhimõtete järgimisele peab vastutav töötleja olema võimeline ka põhimõtete täitmist tõendama.

Kokkuvõte

Palume My Fitness AS-l hoolikalt läbi mõelda oma isikuandmete töötlemise vastavus andmekaitse nõuetele, sh kas isikuandmete töötlemiseks (andmete kogumisel, säilitamisel, kasutamisel jm) on olemas õiguslik alus ja kas konkreetsete andmete töötlemine on ilmtingimata vajalik ja eesmärgipärane. Andmetele tuleb määrata säilitamistähtaeg. Andmebaasi kasutamist tuleb logida ja piirata juurdepääsu isikutele, kellel selleks volitust ei ole. Rakendada tuleb tehnilisi ja korralduslikke meetmeid turvalisuse tagamiseks.

Rohkem infot isikuandmete töötlemise nõuete kohta leiab [Isikuandmete töötleja üldjuhendist](#).

Käesolevale tähelepanu juhtimisele AKI vastust ei oota, kuid selgitame, et AKI võib igal ajal ette teatamata kontrollida¹ isikuandmete töötlemise õiguspärasust ja rikkumise korral alatatada järelevalvemenetluse.

Lugupidamisega

Kirsika Lääts

jurist

peadirektori volitusel

¹ Isikuandmete kaitse seaduse § 57 koosmõjus korrakaitse seaduse §-de 50 ja 51 alusel.