



ANDMEKAITSE INSPEKTSIOON

Lp Elis Vija
Fondia Eesti OÜ

Elis.Vija@fondia.com

Teie 09.02.2026

Meie 25.02.2026 nr 2.2-9/26/523-2

Vastus selgitustaotlusele

Andmekaitse Inspektsioon (AKI) sai Teie pöördumise seisukoha saamiseks töötajate positsioneerimisseadmete kasutamise andmekaitsealase kvalifikatsiooni kohta.

Vastan tekkinud küsimustele info pinnalt, mille olete esitanud ja vastavalt küsimuste esitamise järjekorras.

a) *Kas kirjeldatud tehnilise lahenduse korral, kus tag'i unikaalset ID-d ei seostata konkreetse töötajaga ning süsteem ei võimalda füüsilisi isikuid tuvastada, on tegemist isikuandmetega GDPR artikli 4 punkti 1 tähenduses ning sellest tulenevalt ka isikuandmete töötlemisega GDPR artikli 4 punkti 2 ja isikuandmete kaitse seaduse tähenduses, või on tegemist anonüümsete andmetega, mis jäävad andmekaitse regulatsioonide kohaldamisalast välja?*

Kirjeldatud tehnilise lahenduse puhul näib, et tegu võib olla pseudonümiseeritud andmetega, mis loetakse isikuandmeteks, kui teatud eeldused on täidetud. [Isikuandmete kaitse üldmääruse](#) (IKÜM) järgi on pseudonümiseerimine isikuandmete töötlemine sellisel viisil, et isikuandmeid ei saa enam täiendavat teavet kasutamata seostada konkreetse andmesubjektiga, tingimusel et sellist täiendavat teavet hoitakse eraldi ja andmete tuvastatud või tuvastatava füüsilise isikuga seostamise vältimise tagamiseks võetakse tehnilisi ja korralduslikke meetmeid.

Euroopa Andmekaitsekoostöökoostöö suuniste kohaselt pseudonüümistatud andmeid, mida saab täiendada teabe abil seostada füüsilise isikuga, tuleb pidada tuvastatava füüsilise isiku kohta käivaks teabeks ning seega isikuandmeteks. See väide kehtib ka juhul, kui pseudonüümistatud andmed ja täiendavat teavet ei ole sama isiku valduses. Kui pseudonüümistatud andmeid ja täiendavat teavet on võimalik omavahel kombineerida, arvestades vahendeid, mida vastutav töötleja või muu isik võib mõistlikult kasutada, siis on pseudonüümistatud andmed isikuandmed. Isegi kui kogu pseudonüümistamise teostanud vastutava töötleja säilitatud täiendavat teavet on kustutatud, muutuvad pseudonüümistatud andmed anonüümseks üksnes juhul, kui anonüümisuse tingimused on täidetud (vt. [Euroopa Andmekaitsekoostöökoostöö suunised](#) punkt 22).

Täiendavat teavet hõlmab teavet, mida säilitatakse pseudonüümiseerimise protsessi osana, et tagada sama andmesubjekti eri isikuandmete järjepidev pseudonüümiseerimine, ning teavet, mida hoitakse pseudonüümiseerimise hilisemaks tagasipööramiseks. Selline täiendavat teavet võib koosneda tabelitest, mis seostavad pseudonüümise neid asendavate tuvastamist võimaldavate tunnustega. See võib hõlmata ka krüptograafilisi võtmeid (vt Euroopa Andmekaitsekoostöökoostöö suunised punkt 20).

b) Milliseid tehnilisi ja organisatsioonilisi meetmeid peaks täiendavalt rakendama, et tagada andmete anonüümsus ja vältida isikuandmete töötlemisega seotud riske?

Praeguse AKI praktika kohaselt, mis põhineb Euroopa Andmekaitseõukogu suunistel, käsitletakse pseudonümiseeritud andmeid isikuandmetena seni, kuni taasidentifitseerimine on võimalik. Seega, meetmed peaksid aitama kaasa tagada anonüümsus viisil, et taasidentifitseerimine/tagasipööramine ei ole võimalik.

Juhul, kui tegemist on pseudonümiseeritud isikuandmetega, siis selliste andmete töötlemine peab vastama IKÜM-le, sealhulgas artikli 5 kohastele seaduslikkuse, läbipaistvuse ja konfidentsiaalsuse põhimõtetele ning artikli 6 nõuetele. Vastutavad töötlejad peavad tagama asjakohase turvalisuse taseme, rakendades täiendavaid tehnilisi ja korralduslikke meetmeid. Samuti peavad vastutavad töötlejad tagama läbipaistvuse ning võimaldama andmesubjektidel kasutada IKÜM-i III peatükis sätestatud õigusi, välja arvatud juhul, kui kohaldub artikli 11 lõikes 2 ja artikli 12 lõikes 2 sätestatud erand.

Täpsemalt on võimalik isikuandmete definitsiooni kohta lugeda ka AKI [korduma kippuvate küsimuste](#) rubriigist.

Loodan, et selgitustest on abi.

Lugupidamisega

Gunnar Gabriel Einlo
Jurist
peadirektori volitusel