



ANDMEKAITSE INSPEKTSIOON

Lp Mihkel Männamaa
info@hours.ee
Hours OÜ

27.03.2026 nr 2.2-10/26/657-2

Tähelepanu juhtimine

Andmekaitse Inspeksioon (AKI) sai märgukirja, milles on juhitud tähelepanu, et Hours OÜ töötajate jälgimise tarkvara¹ ei vasta isikuandmete kaitse nõuetele.

Juhime Teie tähelepanu asjaolule, et töötaja arvestuse, töötajate jälgimise, asukohapõhise monitooringu ning personalihalduse funktsionaalsust pakkuv tarkvara töötleb oma olemuselt ulatuslikku hulka isikuandmeid, sealhulgas potentsiaalselt ka eriliiki andmeid. Sellise teenuse arendamisel ja pakkumisel on oluline tagada vastavus isikuandmete kaitse nõuetele.

Alljärgnevalt toome välja peamised aspektid, mida Teie ettevõtte peaks teenuse kujundamisel ja pakkumisel silmas pidama:

1. Isikuandmete töötlemisele kehtestatud nõuded on reguleeritud isikuandmete kaitse üldmääruses (IKÜM)², isikuandmete kaitse seaduses ning vastavates eriseadustes. IKÜM aluspõhimõteteks on andmete seaduslik, aus ja läbipaistev töötlemine, eesmärgipärane kogumine, minimaalne andmete töötlemine, andmete täpsus ning säilitamise piirang ja andmete töötlemise turvalisus (IKÜM art 5 lg 1). Andmetöötleja on kohustatud järgima neid põhimõtteid igas isikuandmete töötlemise etapis. Töötlemise õiguspärasuse eest vastutab ja on võimeline selle täitmist tõendama isikuandmete vastutav töötleja (IKÜM art 5 lg 2).
2. IKÜM artikkel 4 lõike 1 kohaselt on isikuandmeteks igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta. Tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada. Töötajate jälgimise tarkvara abil võidakse töödelda töötajate isikuandmed sh nt töötaja nime, kontaktandmeid, töötaja arvestuse andmed, sh asukoha andmeid, logisid jm, töötaja andmeid (sh eriliiki) sisaldavad ka personalidokumendid.
3. Vastavalt IKÜM art 5 lg 1 punktile a peab isikuandmete töötlemine olema seaduslik, õiglane ja andmesubjektile läbipaistev. Töötlemine on seaduslik juhul, kui selleks on vähemalt üks IKÜM art 6 lõikes 1 toodud õiguslik alus. Olukorras, kus tegemist on eriliiki isikuandmete (sh nt terviseandmete) töötlemisega, peab lisaks artiklile 6 esinema ka üks artiklis 9 sätestatud eranditest ning muul juhul on eriliiki andmete töötlemine keelatud. Töösuhetes töödeldakse töötaja isikuandmeid erinevatel õiguslikel alustel – kõige sagedamini lepingu täitmiseks, tööandjale seadusest tulenevate kohustuste täitmiseks ning olenevalt konkreetsetest tööprotsessidest ka

¹ Stressivaba töötajaarvestus - Hours

² Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta ([isikuandmete kaitse üldmäärus](#))

õigustatud huvi alusel. Tööaja arvestuse pidamise kohustus on tööandjale pandud töölepingu seadusega³, kuid seadus ei sätesta täpset viisi, kuidas seda teha. Seetõttu võib tööandja valida sobiva meetodi tingimusel, et see vastab IKÜM-i nõuetele.

4. Töötajate jälgimise õiguspärasus eeldab, et isikuandmete töötlemine vastab IKÜM-i põhimõtetele, sealhulgas eesmärgipärasusele, vajalikkusele, proportsionaalsusele ja andmete minimaalsusele. Praktikast tähendab see, et tööandja võib koguda üksnes selliseid andmeid ja sellises ulatuses, mis on töökorralduslike eesmärkide saavutamiseks vältimatult vajalikud. Tarkvara funktsioonid, mis hõlmavad ekraanisalvestusi, klaviatuurivajutuste salvestamist või jälgimist, reaalaajas tegevusmonitooringut, asukohajälgimist või tööprotsesside detailset analüüsi, ületavad tavapärase töötajate kontrollimise mõistlikke piire ning kujutavad endast ebaproportsionaalset sekkumist töötaja eraellu. Selline ulatuslik jälgimine ei ole üldjuhul õigustatud ning ei vasta IKÜM-i nõuetele.
5. Hours OÜ veebilehel nähtava tarkvara kirjelduse põhjal eeldab tarkvara kasutamine ulatuslikku töötajate monitoorimist, sealhulgas töötajate tegevuste ja tööprotsesside detailset jälgimist. Selline lähenemine on oma olemuselt problemaatiline, kuna see ei vasta andmete minimaalsuse, eesmärgipärasuse ega proportsionaalsuse põhimõtetele ja võib viia olukorrani, kus tööandja teostab töötajate üle õigusvastast ja ebaproportsionaalset kontrolli ning võib kaasa tuua IKÜM-i rikkumise, mille eest vastutavad nii tarkvara kasutajad kui ka teenuse pakkujad, kes võimaldavad või soodustavad õigusvastast töötlemist.

Seega peaks Teie pakutava teenuse disain toetama põhimõtet, et kogutakse ainult neid andmeid, mis on konkreetse eesmärgi täitmiseks vältimatult vajalikud, nt asukohapõhine jälgimine ei tohi toimuda väljaspool tööülesannete täitmise aega, funktsioonid ei tohi võimaldada varjatud või põhjendamatut jälgimist. Lisaks peaks olema rakendatud vaikimisi privaatsussõbralikke seadeid (nn lõimitud- ja vaikimisi andmekaitse), mis tähendab, et eraelu kaitse on organisatoorsesse ja infotehnoloogilistesse vahenditesse n-ö sisse kirjutatud.⁴ Tarkvara peab võimaldama määrata erinevatele andmekategooriatele säilitustähtajad ja kustutada või anonüümida andmed automaatselt pärast tähtaja möödumist. Kui tarkvara võimaldab töödelda biomeetrilisi või terviseandmeid, tuleb tagada kõrgendatud turvanõuded ja nt võimalus selliste funktsioonide kasutamine tööandja poolt välja lülitada.

6. IKÜM-i kohaselt⁵ on mõistetel „vastutav töötleja“, „kaasvastutav töötleja“ ja „volitatud töötleja“ keskne tähendus, kuna nende kaudu määratakse kindlaks, kes vastutab andmekaitse n-ö täitmise eest ning millised on töötaja praktilised võimalused oma õigusi kasutada. Isikuandmete töötlemisel eristatakse andmetöötlejate rolle vastavalt sellele, kes määrab kindlaks töötlemise eesmärgid ja vahendid ning kes kannab üldist vastutust isikuandmete kaitse nõuete täitmise eest.

Vastutav töötleja vastutab isikuandmete töötlemise põhimõtete järgimise eest ning määrab kindlaks, millisel eesmärgil ja milliste vahenditega isikuandmeid töödeldakse.

³ TLS § 28 lg 2 punkt 4

⁴ Vt AKI koostatud Isikuandmete töötleja üldjuhend, 2. ptk, lk 11.

⁵ IKÜM art 4 p-d 7-8

Vastutav töötleja vastutab nii enda kui ka tema nimel tegutsevate osapoolte poolt teostatava isikuandmete töötlemise eest.⁶

Volitatud töötleja töötleb isikuandmeid vastutava töötleja nimel ja üksnes viimase dokumenteeritud juhiste alusel.⁷ Kui volitatud töötleja hakkab ise määrama isikuandmete töötlemise eesmäärke või vahendeid, loetakse ta selle töötlemistoimingu ulatuses vastutavaks töötlejaks. Seetõttu peab vastutav töötleja volitatud töötleja valimisel olema hoolsuskohustuse kohaselt veendunud, et viimane suudab tagada piisavad tehnilised ja korralduslikud meetmed isikuandmete kaitseks. Töötlemise volitus peab olema vormistatud kirjalikult lepingu või Euroopa Liidu või liikmesriigi õiguse kohase siduva õigusakti alusel. Andmetöötlusleping reguleerib vastutava ja volitatud töötleja omavahelise suhte ning rollijaotuse, mistõttu peab lepingus olema üksikasjalikult kirjeldatud töötlemise sisu ja kestus, töötlemise laad ja eesmärk, töödeldavate isikuandmete liigid, andmesubjektide kategooriad ning poolte õigused ja kohustused.⁸ Kui vastutav töötleja kasutab isikuandmete töötlemisel vahendusteenust (nt personalitarkvara), tuleb sõlmida andmetöötlust reguleeriv leping, mis vastab IKÜM artikli 28 nõuetele.

Euroopa Andmekaitsekoostöögruppi on oma suunises 07/2020 rõhutanud, et vastutava ja volitatud töötleja mõisted on funktsionaalsed – rollid tuleb määrata tegeliku tegevuse ja faktiliste asjaolude põhjal, mitte üksnes lepingulise kokkuleppe alusel. Seega ei ole rollide jaotus läbiräägitav, vaid tuleneb sellest, kes tegelikkuses kontrollib töötlemise eesmäärke ja vahendeid.⁹

Teenusepakkuja on vastutav töötleja eelkõige juhul, kui:

- ta määrab kindlaks andmetöötluse eesmärgid või vahendid,
- tarkvara arhitektuur või ärimudel eeldab andmete kogumist viisil, mida tööandja ei kontrolli,
- ta kasutab kogutud andmeid omaenda eesmärkidel (nt analüütika, teenuse täiustamine, profiilianalüüs).

Sellisel juhul lasub teenusepakkujal otsene vastutus IKÜM-i nõuete täitmise eest, sealhulgas töötlemise õigusliku aluse olemasolu, läbipaistvuse tagamine, andmesubjektide õiguste võimaldamine, turvanõuete rakendamine jm nõuete täitmine.

Teenusepakkuja saab olla volitatud töötleja üksnes juhul, kui:

- ta töötleb andmeid rangelt tööandja dokumenteeritud juhiste alusel,
- tal puudub iseseisev otsustusõigus andmete kasutamise üle,
- ta ei kasuta andmeid kõrvaleesmärkidel.

Sellisel juhul peab teenusepakkuja tagama volitatud töötleja lepingu olemasolu (IKÜM art 28), töötlemise piiritlemise üksnes tööandja juhistega ning rakendama töötlemise iseloomule vastavaid turvameetmeid. Kui tarkvara kirjeldusest ei nähtu selget rollijaotust ega vastutuse piire, kujutab see endast iseenesest IKÜM-i rikkumise riski.

⁶ IKÜM art 4 p 7

⁷ IKÜM art 4 p 8

⁸ Andmetöötluslepingu elemendid on loetletud IKÜM artiklis 28.

⁹ Euroopa Andmekaitsekoostöögruppi. [Suunised 07/2020 vastutava töötleja ja volitatud töötleja mõistete kohta isikuandmete kaitse üldmääruses](#), ver 2.0. 07.07.2021, p 12, lk 9.

Eeltoodust tulenevalt on oluline, et teenuse kasutajate ja teenusepakkuja vahel oleks selgelt määratletud, millises rollis pooled tegutsevad (vastutav või volitatud töötleja) ning milline on andmetöötluse ulatus, eesmärgid ja tingimused. Selleks tuleb sõlmida IKÜM-i artiklile 28 vastav andmetöötlusleping ning tagada, et kõik andmetöötluses osalevad osapooled järgivad andmekaitseõudeid.

7. IKÜM-st tuleneb ka nõue, et vastutav töötleja ja volitatud töötleja peavad isikuandmete töötlemisel riske hindama, seda eelkõige seoses kohustusega töödelda isikuandmeid turvaliselt. Nimelt tuleks isikuandmeid töödelda viisil, mis tagab nende turvalisuse, sealhulgas kaitse loata või ebaseadusliku töötlemise ning juhusliku kaotsimineku, hävimise või kahju eest. Selleks peaksid vastutavad töötlejad ja volitatud töötlejad võtma asjakohaseid tehnilisi ja korralduslikke meetmeid, et kaitsta isikuandmeid võimalike ohtude eest. Neid meetmeid tuleks hinnata, võttes arvesse teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning töötlemise laadi, ulatust, konteksti ja eesmäärke, samuti töötlemisest üksikisikute õigustele tekkivaid erineva tõenäosuse ja suurusega ohte.¹⁰

IKÜM artikkel 32 kohustab rakendama turvameetmeid, mis vastavad töötlemise riskitasemele. Töötajate jälgimise tarkvara puhul on riskitase kõrge, kuna töödeldakse potentsiaalselt väga tundlikku teavet, suurt andmemahtu ning automatiseeritud jälgimisinfot.

Teenusepakkujal peab olema seega rakendatud vähemalt:

- juurdepääsukontrollid ja logimine,
- andmete pseudonüümimise või anonüümimise võimalus,
- andmete säilitustähtaegade rangelt piiratud määratlemine,
- regulaarne turvatestimine ja haavatavuste hindamine,
- mehhanismid andmesubjektide õiguste (ligipääs, kustutamine, piiramine) tagamiseks.

Kui tarkvara ei võimalda neid meetmeid rakendada, ei ole teenus IKÜM-iga kooskõlas.

Kokkuvõttes palume Teil hinnata oma teenuse vastavust kehtivatele andmekaitseõuetele ning vajadusel viia toode ja mh ka selle turunduspraktikad kooskõlla IKÜM-i põhimõtetega. Arvestades töötajate jälgimise ja asukohapõhise monitooringu tundlikkust, on üldtoodud nõuete täitmine oluline nii Teie ettevõtte kui ka teenuse kasutajate õiguspärase tegevuse tagamiseks. Palume Teil hinnata oma teenuse vastavust nimetatud põhimõtetele ning vajadusel rakendada täiendavaid meetmeid.

Vajaduse korral soovitame konsulteerida õigusnõustajaga, et tagada teenuse õiguspärane ja vastutustundlik pakkumine. Kõige olulisema, mida isikuandmete töötleja peab teadma, leiab ka AKI veebilehelt [isikuandmete töötleja üldjuhendist](#).

Eelnevast tulenevalt palume Teil:

- 1. hinnata tarkvara vastavust IKÜM-i nõuetele,**
- 2. tagada, et tarkvara funktsionaalsus ei eelda ebaproportsionaalset töötajate jälgimist,**
- 3. määratleda selgelt oma roll andmetöötluses (vastutav või volitatud töötleja),**

¹⁰ IKÜM art 5 lg 1 p f, art-d 25 ja 32.

- 4. rakendada nõuetekohased turvameetmed,**
- 5. korrigeerida turundus- ja müügimaterjale, et need ei soodustaks õigusvastast isikuandmete töötlemist.**

Käesolevale tähelepanu juhtimisele inspeksioon vastust ei oota, kuid selgitame, et inspeksioon võib igal ajal ette teatamata kontrollida¹¹ andmetöötluse õiguspärasust. Rikkumise korral võib inspeksioon algatada järelevalvemenetluse.

Lugupidamisega

(allkirjastatud digitaalselt)

Mari-Liis Uprus
jurist
peadirektori volitusel

¹¹ Isikuandmete kaitse seaduse § 57 koosmõjus korrakaitse seaduse §-de 50 ja 51 alusel