ANDMEKAITSE INSPEKTSIOON

Teie 06.01.2026

Meie 26.01.2026

Vastus selgitustaotlusele

Andmekaitse Inspektsioon (AKI) sai Teie selgitustaotluse näotuvastuse teel tööaja registreerimise kohta. Kirjeldate, et kasutatav seade ei kogu ega talleta biomeetrilisi andmeid, vaid genereerib näost juhuslike punktide põhjal tekstirea, millest ei ole võimalik töötaja nägu taastada. Seetõttu leiate, et seadmes ei ole hoiustatud ka biomeetrilisi andmeid ja „näoandmete" lekkimisoht puudub. Küsite, kas sellise töötlemise puhul on vajalik töötajatelt võtta luba biomeetriliste andmete töötlemiseks.

Esmalt selgitan, et AKI ei saa selgitustaotlusele vastates anda konkreetset siduvat õiguslikku hinnangut, see on võimalik ainult järelevalvemenetluses. Seetõttu annan Teile üldised selgitused esitatud teabe põhjal.

Igasuguseks isikuandmete töötlemiseks (sh andmete vaatamine, kogumine, säilitamine jne) peab lähtuvalt isikuandmete kaitse üldmääruse[1] (IKÜM) artiklist 6 esinema õiguslik alus. Olukorras, kus tegemist on eriliigiliste isikuandmete (sh biomeetriliste andmete) töötlemisega, peab lisaks artiklile 6 esinema ka üks artiklis 9 sätestatud eranditest ning muul juhul on eriliigiliste andmete töötlemine keelatud.

Teie kirjeldatud lahenduse keskmes on küsimus, kas tööaja arvestamiseks kasutatav näotuvastussüsteem töötleb biomeetrilisi andmeid ning kas selliseks töötlemiseks on vaja töötajatelt eriliiki andmete töötlemise erandit (nt nõusolekut).

IKÜM defineerib biomeetriliste andmetena konkreetse tehnilise töötlemise abil saadavaid isikuandmeid isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad konkreetset füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist, näiteks näokujutis ja sõrmejälgede andmed (art 4 punkt 14). Seega on andmed IKÜM-i mõistes biomeetrilised ainult siis, kui need:

1) seostuvad kellegi füüsiliste, füsioloogiliste või käitumuslike omadustega (nt viis, kuidas keegi kirjutab, kõndimis- või liikumisviis, inimese hääl, sõrmejäljed, silmaiirise muster, nägu või näo mõõtmed ja proportsioonid, veenimuster jm),
2) on saadud konkreetse tehnilise töötlemise abil (nt spetsiaalse tarkvaraga kõne helisalvestise analüüsist tuvastatakse selliseid inimese omadusi nagu toon, kõrgus, aktsent ja intonatsioon) ja
3) võimaldavad andmesubjekti ainulaadset tuvastamist.[2]

[1] Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679.

[2] Loe lähemalt: 1) Artikkel 29 andmekaitse töörühma (WP29) arvamus 3/2012 biomeetriliste tehnoloogiate arengu kohta (WP193). Vastu võetud 27.04.2012 (edaspidi: *WP29 biomeetria arvamus 2012*). Lk 3-4, punkt 2.; 2) Euroopa

Esimese ja teise tingimuse puhul eeldab toorandmete, s.o inimese füüsiliste, füsioloogiliste ja käitumuslike omaduste töötlemine nende mõõtmist. Seejuures ei ole määrav, milliste konkreetsete tehniliste võtetega need omadused tuletatakse.

Kolmanda tingimuse osas on oluline rõhutada, et inimesest tehtud video- või fotosalvestist ei saa pelgalt selle olemasolu tõttu lugeda IKÜM-i art 9 tähenduses automaatselt biomeetrilisteks andmeteks. Biomeetriliseks muutub selline salvestis (või sellest saadud näopilt) üksnes siis, kui seda töödeldakse spetsiaalselt tehniliste vahenditega selleks, et füüsilist isikut tuvastada.[3]

Asjaolu, et seade *"salvestab näo suvalistest punktidest saadud tekstirea"* ehk räsi väärtused ega võimalda nägu tagasi "rekonstrueerida", ei muuda töödeldavate andmete õiguslikku olemust. Biomeetrilisi andmeid saab talletada ja töödelda eri esitlusvormides. Teie kirjeldatud näotuvastusprotsessi kulgemisest nähtub, et biomeetriliste andmete – antud juhul näo – toorvormist põhielementide eraldamise teel loob ja talletab süsteem unikaalse räsi väärtusena biomeetrilise malli, mille abil võrreldakse igakordsel registreerimisel, kas inimese biomeetriline mall on süsteemis kasutus- või ligipääsuõigusega seotud. Seega töötleb süsteem nii biomeetrilisi toorandmeid kui neist loodud unikaalset biomeetrilist malli.

Andmekaitse töörühma[4] selgituste kohaselt ongi biomeetriline mall töötlemata näoandmetest (nt näomõõtmised kujutiselt) välja võetud põhiomaduste esitus, mille loomine peaks olema ühesuunaline – mallist ei tohiks olla võimalik toorandmeid taastada. See, et malli alusel ei saa nägu tagasi luua, ei muuda malli mitte-biomeetriliseks. Vastupidi, malle kasutataksegi tuvastamiseks, võrreldes uut mõõtmist varem salvestatud malliga.[5]

Järelikult töötleb Teie kirjeldatud lahendus biomeetrilisi isikuandmeid ka siis, kui talletatakse üksnes näost tuletatud „tekstirida" ehk mall. Ning kuna eesmärk on töötaja kordumatu tuvastamine tööaja registreerimiseks, kuulub töötlemine IKÜM artikli 9 kohaldamisalasse.

Kuna biomeetriline andmetöötlus ei ole lubatud lepingu täitmise eesmärgil ning kehtiv seadus ei anna tööandjale õigust töödelda töötaja biomeetrilisi andmeid tööaja arvestuseks või ligipääsukontrolliks, saab selline töötlemine toimuda ainult töötaja nõusolekul. Nõusolek peab olema vabatahtlik, konkreetne, teadlik ja ühemõtteline ning selle olemasolu tõendamise kohustus lasub tööandjal. Enne nõusoleku andmist tuleb töötajat teavitada õigusest nõusolek igal ajal tagasi võtta.[6]

Juhin tähelepanu, et töösuhetes on üldiselt nõusoleku alusele tuginemine problemaatiline poolte vahel valitseva võimude tasakaalutuse tõttu, kuna töötaja on alluvussuhtes. Seetõttu peab tööandja eriliigiliste isikuandmete töötlemisel olema eriti hoolikas ning tagama, et biomeetriliste andmete kasutamine oleks tegelikult vabatahtlik. Töötajal peab olema reaalne võimalus otsustada, kas ta soovib kasutada tööaja arvestuseks biomeetrilist tuvastust, ning alati peab olema olemas alternatiivne, mitte-biomeetriline tööaja registreerimise viis (nt kiipkaart, *PIN*-kood või muu elektrooniline võti).[7] Kui alternatiiv puudub või seda ei ole võimalik töötajal tegelikult kasutada, ei saa nõusolekut pidada vabatahtlikuks. Samuti peab töötajal olema võimalus igal ajal loobuda biomeetrilise tuvastuse kasutamisest.

Nõusoleku tingimustest põhjalikumalt saab lugeda siit Nõusolek | Andmekaitse Inspektsioon.

Andmekaitsenõukogu suunised 3/2019 isikuandmete töötlemise kohta videoseadmetes. Versioon 2.0 Vastu võetud 29.01.2020 (edaspidi: *EAKN videovalve suunised 2019*). Lk 18, p-d 74-77.

[3] IKÜM põhjenduspunkt 51.

[4] Artikkel 29 andmekaitse töörühm on enne IKÜMi jõustumist kohaldatud andmekaitsedirektiivi (95/46/EÜ) kohaselt Euroopa Liidu liikmesriikidele eksperdinõuannete andmise nõuandev organ, mida asendab alates 25.05.2018 Euroopa Andmekaitsenõukogu.

[5] 1) WP29 biomeetria arvamus 2012, lk 3-6, punkt 2.; 2) EAKN videovalve suunised 2019, lk 19, p 82.

[6] IKÜM art 4 punkt 11, artikkel 7 ja põhjenduspunkt 32.

[7] 1) WP29 biomeetria arvamus 2012, lk 10-12, p 3.1.1; 2) EAKN videovalve suunised 2019, lk 20, p 86.

Lisaks nõuab näotuvastuse kasutuselevõtt sellega kaasneva mõju hindamist töötajate isikuandmete kaitsele. Andmekaitsealane mõjuhinnang on kohustuslik olukordades, kus andmetöötlusega kaasneb tõenäoliselt suur oht inimeste õigustele ja vabadustele (IKÜM art 35). Andmekaitse töörühma suuniste kohaselt on mõju hindamine tavaliselt nõutud siis, kui täidetud on mitmed suure ohu kriteeriumid. Näotuvastusega tööajaarvestus vastab neist vähemalt järgmistele: (1) töötajad kuuluvad haavatavate andmesubjektide hulka tulenevalt tööandja ja töötaja ebavõrdsest võimusuhtest; (2) andmetöötluseks kasutatakse uuenduslikku tehnoloogiat (näitena tuuakse välja näotuvastus autentimiseks); (3) sõltuvalt asjaoludest võib esineda ka süstemaatilise jälgimise elemente.[8]

Seega tuleb enne biomeetrilise töötlemise alustamist tööandjal koostada IKÜM artikli 35 kohane andmekaitsealane mõjuhinnang. Seda tuleb teha ka juhul, kui töötlemise õiguslikuks aluseks on töötaja nõusolek.

Mõjuhinnangust täpsemalt saab lugeda AKI kodulehe rubriigist Mõjuhinnang | Andmekaitse Inspektsioon.

Loodan, et minu selgitustest on abi.

Lugupidamisega

Jekaterina Aader
jurist
peadirektori volitusel

[8] 1) Artikli 29 alusel asutatud andmekaitse töörühma suunised, mis käsitlevad andmekaitsealast mõjuhinnangut ja selle kindlaksmääramist, kas isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht“ vastavalt määrusele (EL) 2016/679 (WP 248 rev. 01). Saadaval eestikeelne versioon. Vastu võetud 4. aprillil 2017. Viimati muudetud ja muudatused vastu võetud 4. oktoobril 2017. Lk 11-12, kriteeriumid 3, 7-8; 2) IKÜM põhjenduspunktid