

Justiits- ja Digiministeerium
Suur-Ameerika 1, 10122 Tallinn
info@justdigi.ee

11.03.2026

Eesti Näitlejate Liidu täpsustavad seisukohad Euroopa Komisjoni digitaalse omnibus'i ettepanekutele. Koostatud koostöös Rahvusvahelise Näitlejate Föderatsiooniga (FIA).

Peamised probleemid:

1. Mõiste „isikuandmed“ üha subjektiivsemaks ja tehisaru arendavate ettevõtete enda tõlgenduse küsimuseks muutmine;
2. Muudatustega lubatakse tehisaru arendajatel tugineda liiga laia tähendusväljaga „õigustatud huvile“, et kasutada isikuandmeid tehisaru treenimiseks ja toimimiseks ilma isiku nõusolekuta;
3. Muudatustega võimaldatakse vabastada suur osa sensitiivsed andmed GDPRi rangematest kaitsenõuetest;
4. Lihtsustatakse tehisaru ettevõtete võimalust tagasi lükata või kitsendada isikuandmete juurdepääsutaotluste tingimusi, sealhulgas ka õigusi esindavate organisatsioonide poolt oma liikmete nimel esitatud taotluste puhul;
5. Lihtsustatakse olukordi, kus isiku seadmes (nt telefonis või sülearvutis) talletatud isikuandmeid võib ilma nõusolekuta kasutada ja töödelda;

1. ISIKUANDMED MUUTUVAD SUBJEKTIIVSEKS

Mis on „isikuandmed“, muutub täielikult subjektiivseks. Praegu loetakse andmeid isikuandmeteks, kui kedagi on nende põhjal võimalik mõistlike vahenditega tuvastada. Uue lähenemise järgi oleks andmed „isikuandmed“ ainult siis, kui konkreetne ettevõtte, kes neid kasutab, ei suuda sind tuvastada – isegi kui hilisemad andmesaajad suudaksid seda hõlpsasti teha. Teisisõnu saavad ettevõtted suures osas ise otsustada, kas GDPR kehtib nende kogutud, kasutatud või edasi antud andmete suhtes või ei. See tähendaks GDPRi rakendamise sisulist õõnestamist ja selle põhilise kaitsemehhanismi tühistamist.

Näide: tootmisettevõtte võib kasutada näitlejate häälesalvestisi või esituse tehisaru treenimiseks ja väita, et kuna nimed on eemaldatud, ei ole tegemist enam isikuandmetega. Kui samu andmeid jagatakse hiljem *casting*-platvormi või teise tehisaru ettevõttega, kes suudab näitleja hääle või liikumise järgi ära tunda, on kahju juba tehtud. GDPR ei kehtinud esimeses etapis ning esitajal puudus õigus teada, vaidlustada või kontrollida, kuidas tema andmeid kasutati.

2. UUS ÕIGUSLIK ALUS ISIKUANDMETE KASUTAMISEL TEHISARU TREENIMISEKS JA TÖÖTLEMISEKS

Tehisaru arendavad ettevõtted võivad „õigustatud huvile“ tuginedes kasutada tehisaru arendamiseks ja töös hoidmiseks isikuandmeid ilma isiku eelneva nõusolekuta. Seda piiravad

vaid ähmased tehnilised meetmed, subjektiivsed kaalutlused ja „õigus keelduda isikuandmete töötlemisest“. See õigus on aga paratamatult sisutühi, sest inimesed ei tea kunagi, kus nende andmeid kasutatakse ning isegi kui nad teaksid, peaksid nad vastu astuma väga suurtele ja mõjuvõimsatele ettevõtetele.

Näide: tehisaru ettevõtte võib koguda näitlejatest avalikult kättesaadavaid videoklippe (filmid, intervjuud, sotsiaalmeedia jne) ja kasutada neid mudeli treenimiseks, mis suudab luua näitleja svälimuse, hääle või liikumise põhjal realistliku digitaalse koopiat. Tuginedes „õigustatud huvile“ tehakse seda ilma loata ja ilma tasu maksmata, kuigi digitaalset koopiat võidakse kasutada kommertseesmärkidel.

3. LAIEM JUURDEPÄÄS TUNDLIKELE ANDMETELE

Hetkel kaitseb GDPR tundlikke andmeid (nt biomeetrilised, rassilised, terviseandmed, etniline päritolu, poliitilised vaated, seksuaalne orientatsioon, religioossed või filosoofilised veendumused, ametiühingu liikmelisus) rangelt.

Ettepanek muudab need reeglid kohaldatavaks ainult juhul, kui andmed paljastavad tundliku teabe „otseselt“. See tähendab, et täiendav kaitsekiht kaoks ning tehisaru treenimine ja andmete töötlemine oleks lubatud, kui tundlik info on „järeldatud“ või „kaudselt tuletatud“ erinevatest andmetest. See erand kehtib tingimusel, et tehisaru arendav ettevõtte ei „kavatse“ neid andmeid koguda, eemaldab need tuvastamise korral koheselt või kui see nõuab „ebaproportsionaalselt suurt pingutust“, tagab, et andmeid ei saa väljundis kasutada, avaldada ega kolmandatele isikutele kättesaadavaks teha.

Praktikas tähendab see, et tehisaru süsteemid võivad salvestiste, biomeetriliste mustrite, suhtlusandmete põhjal seaduslikult järeldada esitajate tundlikke omadusi seni kuni ettevõtte väidab, et see polnud tahtlik ja eemaldamine oleks liiga keeruline. Kuna keskendutakse kogumise vältimisele, mitte järeldamise takistamisele, jääb enamik tundlikust profileerimisest nähtamatuks, kuid mõjutab otsuseid. Näiteks võib ametiühingusse kuuluva näitleja märgistada „probleemseks“, mis mõjutab valikuid tegevas *casting*-süsteemis otsuseid. Esitajad jäävad varjatud profileerimise, diskrimineerimise ja töökaotuse ohtu ilma nõusoleku, läbipaistvuse või tõhusa kaitseta.

AI-määruse ettepanek lisab ka uue reegli, mis lubab tehisaru arendajatel kasutada tundlikke andmeid laiemalt „põhjaneva kallutatuse tuvastamiseks ja parandamiseks“. Selle asemel, et piirata seda rangelt vajaliku ja kõrge riskiga süsteemidega (nii nagu esialgses AI-määruses), langetatakse künnis tasemele „vajalik“ ning laiendatakse see kõigile tehisaru süsteemidele ja mudelitele. See muudab tundlike andmete kasutamise tavalisemaks ja normaliseerituks.

Näide 1: *Casting*-platvorm analüüsib fotosid, proovisalvestisi või häälenäiteid. Tehisaru järeldab esineja etnilise päritolu näojoonte, nahatoonid või aktsendi põhjal. Kuigi kasutatakse biomeetrilisi andmeid, väidab tehisaru ettevõtte, et tundlikku infot ei kogutud tahtlikult ja selle eemaldamine oleks liiga keeruline. Andmed jäävad süsteemi ja mõjutavad valituks saamise protsessi.

Näide 2: Tehisaru süsteem skaneerib avalikke materjale, intervjuusid või sotsiaalmeediat, et

ennustada näitleja seksuaalset orientatsiooni, religioosseid või poliitilisi vaateid või ametiühingu liikmelisust. Ettevõtte väidab, et see info ei olnud tahtlikult kogutud ja selle filtreerimine oleks ebaproportsionaalne. Järeldatud omadused mõjutavad siiski näitleja kategoriseerimist valituks saamise protsessis.

4. JUURDEPÄÄSUÕIGUS ON OHUSTATUD

GDPR annab inimestele õiguse tutvuda oma isikuandmetega ning teatud tingimustel nõuda nende parandamist või kustutamist. Praegu võib vastutav töötaja keelduda juurdepääsutaotluse täitmisest või küsida mõistlikku tasu ainult siis, kui taotlus on ilmselgelt põhjendamatult või ülemääraselt suur, ning tõendamiskoormus lasub töötajal. Komisjoni ettepanek laiendab „ülemäärase“ taotluse mõistet, lubades ettevõtetal keelduda taotlustest või küsida tasu, kui nad peavad taotlust „kuritarvitavaks“ s.t. mitte peamiselt isikuandmete kaitse eesmärgil esitatuks või liiga laiaulatuslikuks või eristamatuks. See toob sisse taotleja oletatava motiivi hindamise, avades ukse keeldumistele väidetava sobimatu või strateegilise kavatsuse alusel. Ettepanek vähendab ka töötajate tõendamiskoormust, väites, et see peaks olema minimaalne, kuna hinnang põhineb valdavalt teguritel, mis ei asu töötaja enda süsteemides. Selle tulemusena suureneks tööandjate kaalutusõigus kitsendada, edasi lükata või tagasi lükata nii individuaalseid kui ka kollektiivseid juurdepääsutaotlusi, sealhulgas ka õigusi esindavate organisatsioonide poolt esitatud või toetatud taotlusi.

Murekoht: see raskendab esitajate õigusi esindavatel organisatsioonidel oma liikmete nimel juurdepääsutaotluste esitamist, et teada saada, kuidas nende häält, pilti, sarnasust, salvestisi või muid andmeid talletatakse, taaskasutatakse ja kasutatakse ka tehisaru süsteemides, mis on oluline info õiglase tasu läbirääkimistel. Ettepaneku kohaselt võiksid tööandjad või platvormid hõlpsamini väita, et sellised taotlused on „kuritarvitavad“, „strateegilised“ või „mitte peamiselt andmekaitsega seotud“.

5. JUURDEPÄÄS SEADMES TALLETATUD ISIKUANDMETELE (JA NENDE EDASINE KASUTAMINE) LAIENEB OLULISELT

Väidetavalt nn „küpsiseväsimumuse“ vähendamiseks laiendab ettepanek põhjuseid, mille alusel võib ettevõtte ilma nõusolekuta pääseda ligi inimese telefonis või arvutis talletatud andmetele, näiteks auditooriumi mõõtmiseks, statistika tegemiseks või turvalisuse tagamiseks. See tähendab, et inimestel on vähem kontrolli selle üle, kuidas nende veebikäitumist jälgitakse ja kuidas sellest profile luuakse. Kuna need reeglid viiakse ePrivaatsuse direktiivist (mis reguleerib juurdepääsu seadmetele) GDPR-i (mis reguleerib andmete kasutamist pärast juurdepääsu), saavad ettevõtted seejärel tugineda mis tahes GDPR-is sätestatud õiguslikule alusele, sealhulgas „õigustatud huvile“. Praktikas võimaldab see ettevõtetal oluliselt laiendada juurdepääsu inimese seadmes talletatud isikuandmetele ja nende kasutamist ilma nõusolekuta, seni kuni nad väidavad, et see teenib nende õigustatud ärihuve.

Murekoht: *casting*-platvormid, agentuurid või tootmisettevõtted võivad (otse või kaudselt) pääseda ligi esitajate telefonides või arvutites talletatud andmetele ja neid töödelda ilma

nõusolekuta, kasutades laia põhjendust nagu „statistika“ või „turvalisus“, ning seejärel tugineda „õigustatud huvile“, et profileerida, järjestada või filtreerida esinejaid. See mõjutab, keda kutsutakse prooviesinemistele või kellele pakutakse tööd, samal ajal kui esitajatel on üha raskem mõista, kontrollida või vaidlustada, kuidas nende digitaalne käitumine mõjutab nende töövõimalusi.

6. MASINPÕHINE OTSUSTAMINE LAIENEB OLULISELT

Digitaalse Omnibus'i ettepanekud sõnastavad ka, et isegi kui otsuseid, millel on inimese elu oluliselt mõjutav õiguslik toime, võiks teha inimene, ei takista see ettevõttel tugineda „lepingulisele vajadusele“, et lasta need otsused teha masinal ilma inimliku järelevalveta, tingimusel et see põhineb EL-i õigusel või isiku „selgesõnalisel nõusolekul“.

Murekoht: *casting'u* otsused, millel on olulised karjääri mõjutavad tagajärjed, võivad olla juhitud automatiseeritud hindamis- või filtreerimissüsteemidest ja neid võib käsitleda „lepinguliselt vajalikena“, isegi kui otsuse oleks võinud teha inimene. See võimaldab tootjatel või platvormidel tugineda tehisarude lühinimekirjade, järjestamise või välistamise tööriistadele, mis vaikselt määravad, keda nähakse, kuulatakse või palgatakse, samal ajal kui esitajatel endil puudub info selle kohta, kuidas neid hinnati ning puudub ka sisuline võimalus vaidlustada kallutatud või ebatäpseid profile.

7. LISAKS

Eelkõige on murekohaks, et tehtud ettepanekutega saavad tehisarud arendajad ise hinnata, kas nende süsteemid kvalifitseeruvad „kõrge riskiga“ kategooriasse, ning kui nad leiavad, et need ei kujuta endast olulist ohtu tervisele, ohutusele või põhiõigustele, vältida kandmist EL-i andmebaasi. Samuti lükatakse AI-määruse kõrge riskiga kohustuste kohaldamine edasi rohkem kui aasta võrra. Kõige tõsisemad ja süsteemsemad probleemid tulenevad aga AI-määruse ja GDPR-i uue koostöö loomisest.

Oluline on märkida, et ükski neist ettepanekutest ei näi tuginevat eelnevale mõjuhindangule, mis hindaks nende mõju põhiõigustele, kultuuriõigustele või demokraatlikele vabadustele. Samuti ei näi need põhinevat selgetel tõenditel, et nii ulatuslikud muudatused on vajalikud innovatsiooni või konkurentsivõime edendamiseks EL-is. Praktikas tootsid need meetmed peamiselt kasu suurtele tehnoloogiaettevõtetele, valdavalt väljaspool EL-i asuvatele, kellel on pikk ajalugu EL-i andmekaitseõuete rikkumisel ja kes püüavad nüüd neid nõudeid veelgi nõrgendada, et toita oma tehisarude mudeleid isiku- ja tundlike andmetega näilise kaitsekatte all, mida on vähe tõenäoline tõhusalt jõustada.

Lugupidamisega

Reimo Sagor
Eesti Näitlejate Liit
juhatuse esimees