ANDMEKAITSE INSPEKTSIOON

Lp Lauri Luht
Justiits- ja Digiministeerium
info@justdigi.ee

Teie 11.02.2026 nr 7-1/1040

Meie 23.02.2026 nr 2.3-4/26/576-2

Arvamus EL andmeliidu strateegiale ja tehisaru rakendamise strateegiale

Täname, et saatsite Andmekaitse Inspektsioonile (AKI) arvamuse avaldamiseks EL andmeliidu strateegia ja tehisaru rakendamise strateegia. Käesolevaga esitab AKI oma seisukohad.

1. Pseudonüümimine ja anonüümimine

Pseudonüümimise ja anonüümimise piiritlemine vajab strateegias täpsustamist. Digivaldkonna koondpaketi ettepanekuga[1] soovitakse viia sisse võimalus, et teatud juhtudel ei pruugi pseudonüümitud andmed olla käsitletavad isikuandmetena konkreetse andmevaldaja vaates, kusjuures täpsemad tingimused soovitakse määrata Komisjoni rakendusaktiga. Samas on Euroopa Andmekaitsenõukogu (EAKN) ja Euroopa Andmekaitseinspektor (EDPS) rõhutanud digivaldkonna koondpaketi ettepaneku ühisarvamuses[2], et selline lähenemine võib minna vastuollu Euroopa Kohtu praktikaga ning tekitada ohtliku pretsedendi, kus rakendusakt mõjutab sisuliselt isikuandmete mõiste ulatust ja seeläbi ka isikuandmete kaitse üldmääruse (IKÜM) kohaldamisala. Seetõttu on vajalik üheselt selge ja objektiivne raamistik, mis määratleb, millal pseudonüümimine on praktikas piisav ning kuidas välditakse olukorda, kus andmete õiguslik staatus sõltub liigselt subjektiivsest hinnangust ja tekitab taastuvastuse riski.

Kuigi digivaldkonna koondpaketi ettepanekuga kavandatakse anda Komisjonile volitus anda välja rakendusakt pseudonüümimise selgitamiseks, puudutab see eeskätt piiri isikuandmete ja konkreetse andmekaitse meetme vahel, mitte aga pseudonüümitud ja anonüümsete andmete eristust, seega ei teki endiselt selget kriteeriumit, millal tuleb andmeid pidada täielikult anonüümseteks. See tähendab, et seadusandlikus raamistikus puudub jätkuvalt andmete anonüümseks pidamise standard, mida praktikasse rakendada.

Isikuandmete ja isikustamata andmete eristamist ei saa taandada üksnes andmevaldaja subjektiivsele hinnangule selle kohta, kas tal on mõistlikult tõenäolised vahendid isiku tuvastamiseks. Selline lähenemine võib viia selleni, et sama andmestik on ühe osapoole jaoks anonüümne, kuid teise jaoks pseudonüümitud (st jätkuvalt isikuandmed), mis vähendab õiguskindlust. Seetõttu on vaja objektiivseid ja tõendatavaid kriteeriume, mille tulemusena saaks

[1] Ettepanek: Euroopa Parlamendi ja Nõukogu määrus, millega muudetakse määrusi (EL) 2016/679, (EL) 2018/1724, (EL) 2018/1725 ja (EL) 2023/2854 ning direktiive 2002/58/EÜ, (EL) 2022/2555 ja (EL) 2022/2557 seoses digivaldkonna õigusraamistiku lihtsustamisega ning tunnistatakse kehtetuks määrused (EL) 2018/1807, (EL) 2019/1150, (EL) 2022/868 ja direktiiv (EL) 2019/1024 (digivaldkonna koondpakett)

[2] EDPB-EDPS Joint opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)

andmetöötleja tõsikindlalt väita, et andmed on anonüümsed.

2. Tehisandmed

Tehisandmetega seoses leiab AKI, et tervitatav on näha strateegia rõhuasetust privaatsust tagavate tehnoloogiate (PET) kasutamisele. Strateegia näeb andmelaborites ette töövahendid ning eksperditeadmised tehisandmete genereerimiseks, valideerimiseks ja võrdlemiseks. Strateegia kirjeldab andmelaboreid kui turvalisi keskkondi, mis pakuvad praktilisi tööriistu ja tuge isikuandmete kaitseks kasutatavate võtete rakendamiseks. Sealhulgas nähakse andmelaborite teenustena ette tehisandmete loomine ja valideerimine tehisaru treenimiseks ja testimiseks.

Samas vajab täpsustamist väide, et tehisandmed täiendavad anonüümimismeetmeid[3]. Tehisandmed ei ole anonüümimise lisakiht, vaid üks võimalikest meetoditest privaatsusriski vähendamiseks ja anonüümsuse saavutamiseks. Strateegias endas on tehisandmete genereerimine paigutatud teistest kaitsemeetmest eraldi (koos on sellised meetodid nagu pseudonüümimine, anonüümimine ja diferentsiaalprivaatsus), mistõttu on täpsem käsitleda tehisandmeid kui alternatiivset või täiendavat lahendust sõltuvalt kasutusjuhust, mitte kui anonüümimise täiendust. Tehisandmete kasutamine vajab õiguslikke ja tehnilisi täpsustusi, sest tehisandmete genereerimine ei taga alati tegelikku anonüümsust, eriti väikeste, haruldaste või muul viisil tundlike andmestike korral. Väikeste (nt harvikhaigused) ja äärmuslike juhtumite puhul võib jääda alles taastuvastamise risk või võib andmetes säilida unikaalne teave, mis võimaldab isiku taas tuvastamist. Ka sünteetiliste andmete käsitlused rõhutavad, et kui tehisandmeid ei genereerita ja hallata hoolikalt, võivad need lekitada tundlikku infot, võimendada algandmete kallutatust või olla otsuste tegemisel eksitavad. Strateegia küll rõhutab kvaliteeditagamise ja dokumenteerimise olulisust, kuid vajab konkreetseid, rakendatavaid kriteeriume.

Selgemalt tuleks määratleda, millistel tingimustel võib tehisandmeid pidada anonüümseteks, olles seega väljaspool IKÜM kohaldamisala. Praktikas on määrav küsimus, kas ja millisel tasemel jääb alles andmesubjekti taastuvastamise risk, eriti juhul, kui tehisandmed on loodud tegelike isikuandmete põhjal. Strateegias võiks seetõttu täpsustada, milliseid tehnilisi ja metoodilisi kriteeriume kasutatakse anonüümsuse hindamisel ning kuidas arvestatakse tehisintellektist tulenevaid riske (nt võib mudel info meelde jätta ja sellest tulenevalt võib olla lekkeoht). Ilma selliste selgete kriteeriumideta võib tekkida ebaühtlane praktika, kus tehisandmeid kvalifitseeritakse anonüümseks pelgalt nende tehisliku päritolu tõttu, kuigi tuvastatavuse risk ei pruugi olla sisuliselt maandatud.

Lisaks vajab selgitamist tehisandmete loomise protsessi õiguslik käsitlus. Isegi kui lõpptulemusena loodud andmestik on anonüümne, võib genereerimise etapis toimuda isikuandmete töötlemine, millele kohaldub IKÜM koos kõigi sellest tulenevate nõuetega. Seega tuleks selgemalt eristada sisendandmete töötlemise etappi (kus on vaja õiguslikku alust, eesmärgipärasust, minimaalsust ja turvameetmeid) ja väljundandmestiku staatust (kas anonüümne või endiselt isikuandmete alla kuuluv). Ilma selle eristuseta võib praktikas kujuneda väärarusaam, et tehisandmete kasutamine vabastab automaatselt andmekaitsenõuetest, kuigi tegelik risk ja töötlemistoimingud võivad paikneda just genereerimise ja valideerimise faasis.

3. Andmelaborid

Andmelaborite õiguslik roll vajab täiendavat selgitust, kuna strateegias kirjeldatakse andmelaboreid kui keskseid pseudonüümimise ja andmetöötluse teostajaid, ent ei ole selge, kas nad tegutsevad vastutava töötleja, volitatud töötleja või ühise vastutava töötlejana. Ebakindlus rollide osas tekitab riske ka andmesubjektide õiguste tagamisel. Seetõttu on vaja täpsustada, millised on andmelaborite õigused ja kohustused andmete töötlemisel.
Läbipaistvuse tagamine andmesubjektide jaoks eeldab selget regulatiivset raamistikku ja praktilisi

[3] 4. peatükk: I sammas: ii. Andmelaborid: Tehisandmete genereerimine

mehhanisme olukorras, kus andmelaborites toimub ulatuslik pseudonüümimine, tehisandmete loomine või andmete koondamine. Tuleb määratleda, millisel õiguslikul alusel selline töötlemine toimub, kuidas täidetakse teavitamiskohustust ning millises ulatuses on andmesubjektil võimalik saada arusaadavat teavet töötlemise eesmärkide ja mõjude kohta. Eriti oluline on hinnata, kas ja kuidas on tagatud andmesubjekti õigused. Samuti tuleb selgitada, kas ja kuidas vastab andmelaborite tegevus õiguspärasuse, minimaalsuse ja eesmärgipärasuse põhimõtetele.

Lisaks tuleb hinnata riski, et andmelaboritest kujuneb keskne andmekogum, kuhu koondub suur hulk erinevatest allikatest pärinevaid andmeid. Selline koondumine võib suurendada nii turvariske, sh volitamata juurdepääsu või andmeleket. Mida suurem ja mitmekesisem on andmestik, seda suurem on ka tagasituvastamise oht, eriti kui erinevaid andmekihte on võimalik omavahel ristkasutada. Seetõttu on vajalik läbi viia põhjalik andmekaitsealane mõjuhinnang ning selgelt piiritleda andmete säilitamise tähtajad ja juurdepääsuõigused.

4. Isikustamata andmete edastamine kolmandatesse riikidesse

On tervitatav, et strateegia kohaselt hakatakse kaitsma ka isikustamata andmete kolmandatesse riikidesse edastust. Strateegia kohaselt on plaanitud 2026. aasta II kvartalis avaldada suunised, kuidas hinnata ELi üksuste kohtlemist kolmandate riikide poolt, ning 2026. aasta I kvartalis töötada välja andmelekkevastane meetmepakett. See loob olulise kaitsemeetme olukordadeks, kus edastatavateks andmeteks pole ainult isikuandmed.

Küll aga võib isikuandmete kaitse seisukohast probleemseks osutuda, kui digivaldkonna koondpaketi ettepaneku tulemusel hakatakse pseudonüümitud andmeid teatud juhtudel käsitlema isikustamata andmetena. Sellisel juhul tekib reaalne oht, et IKÜMiga ettenähtud kolmandatesse riikidesse edastamise range raamistik (IKÜM V peatükk) ei rakendu, kuna selle peatüki kohaldamine eeldab, et edastatavad andmed on isikuandmed. Seetõttu on EAKN ja EDPS digivaldkonna koondpaketi ettepaneku ühisarvamuses rõhutanud, et koondpaketi ettepanek mõjutab otseselt IKÜM-i kohaldamisala ja tulemuseks võib olla kaitsetaseme ebaühtlus.

Kuigi praktikas võib ette tulla olukordi, kus teatud andmestik liigitatakse isikuandmete asemel isikustamata andmeteks, on positiivne, et strateegia järgi plaanib Komisjon tugevdada kaitset ka rahvusvaheliste andmevoogude kontekstis, sh töötada välja andmelekkevastase meetmepaketi ja suunised kolmandate riikide kohtlemise hindamiseks. Seetõttu võib andmetele mõningane kaitse laieneda ka isikustamata kujul, mis on tervitatav, arvestades isikustamata andmete kaitse kasvavat tähtsust kolmandatesse riikidesse edastamisel, kuivõrd ka isikustamata andmeid on võimalik isikustada või kasutada inimese või ettevõtte kohta järelduste tegemiseks, eriti riikides, kus riigiasutustel on lai juurdepääs andmetele.

Lugupidamisega

(allkirjastatud digitaalselt)

Pille Lehis
peadirektor

Kirsika Nigul
kirsika.nigul@aki.ee
6828712