



ANDMEKAITSE INSPEKTSIOON

Lp Laura Reinurm
Keskkonnaagentuur
Laura.Reinurm@Envir.ee

Teie 10.08.2026

Meie 24.08.2026 nr 2.3-8/26/3094-2

Vastus nõudekirjale

Pöördusite Andmekaitse Inspeksiooni poole seoses uue tootjavastutuse registri (TVR) loomisega ning palusite hinnangut ettevõtjate andmete hoidmisele pilveteenuses. Selgitasite, et kavandatud register on mõeldud tootjavastutuse kohustuste täitmise, aruandluse ja järelevalve toetamiseks ning selle põhiandmestik koosneb valdavalt juriidiliste isikute esitatavatest andmetest. Isikuandmeid sisaldaks register piiratud ulatuses (nt kontaktisikute andmed). Samuti märgite, et uue TVR alla on kavas koondada olemasolevate pakendiregistri (PAKIS) ja probleemtoodete registri (PROTO) andmed.

Alljärgnevalt annab Andmekaitse Inspeksioon üldise selgituse. Tegelikult sõltub konkreetse pilvelahenduse sobivus muu hulgas töödeldavate andmete koosseisust, teenusepakkuja ja alltöötajate rollidest, andmete asukohast, juurdepääsuvõimalustest, kohaldatavast õigusruumist ning rakendatavatest tehnilistest ja korralduslikest meetmetest.

Kas andmekaitsealane regulatsioon seab piiranguid sellise registri põhiandmete hoidmisele pilveteenuses, kui tegemist on valdavalt juriidiliste isikute andmetega?

Selgitame, et isikuandmete kaitse regulatsioon on tehnoloogianeutraalne ega keela iseenesest pilveteenuse kasutamist. Samuti ei kohaldu [isikuandmete kaitse üldmäärus](#) (IKÜM) juriidilise isiku kui sellise andmetele. Seega ei tulene IKÜM-ist ka üldist keeldu hoida TVR-i ettevõtjate kohta käivaid põhiandmeid pilveteenuses.

Samas, nagu ka oma pöördumises märgite, võib register sisaldada isikuandmeid, nt kontaktisikute andmeid, aga ühtlasi ka esindajate, kasutajakontode ja menetlustoimingute tegijate andmeid, samuti autentimis- ja logiandmeid. Isikuandmeteks võivad osutuda ka füüsilisest isikust ettevõtjate andmed ning muud andmed, mis võimaldavad füüsilist isikut otseselt või kaudselt tuvastada. Selles osas tuleb täita kõiki IKÜM-ist tulenevaid nõudeid.

Kui pilveteenuse pakkuja töötleb isikuandmeid registri vastutava töötleja nimel, on teenusepakkuja üldjuhul isikuandmete volitatud töötleja. IKÜM artikli 28 lõikest 1 tuleneb nõue, et vastutav töötleja kasutab ainult selliseid volitatud töötlejaid, kes annavad piisava tagatise, et nad rakendavad asjakohaseid tehnilisi ja korralduslikke meetmeid viisil, et töötlemine vastab IKÜM-i nõuetele. Sellisel juhul peab ka teenusepakkujaga sõlmitud leping vastama IKÜM artikli 28 nõuetele. Lepingus tuleb muu hulgas kindlaks määrata töötlemise sisu, kestus, laad ja eesmärk, isikuandmete liigid, andmesubjektide kategooriad ning vastutava ja volitatud töötleja õigused ja kohustused. Samuti tuleb reguleerida konfidentsiaalsus, turvameetmed, alltöötajate kasutamine, andmesubjekti õiguste tagamisele kaasaaitamine, rikkumistest teavitamine, auditivõimalused ning andmete tagastamine või kustutamine teenuse lõppemisel.

Siinjuures peame vajalikuks rõhutada, et kuigi IKÜM artiklis 28 loetletud elemendid moodustavad lepingu põhisisu, ei tohiks andmetöötlusleping siiski lihtsalt korrata IKÜM-i sätteid, vaid vastutava ja volitatud töötleja vaheline leping peab olema põhjalik ning kajastama täpselt poolte rolle ja vastutust isikuandmete töötlemisel.

Samuti tuleb pilveteenuse kasutamisel tagada IKÜM artikli 32 kohased riskile vastavad tehnilised ja korralduslikud turvameetmed. Sealjuures tuleb ühtlasi arvestada ka küberturvalisuse seaduse ning selle alusel kehtestatud võrgu- ja infosüsteemi turvameetmete nõuetega. Asjakohasel juhul tuleb hinnata avaliku pilveteenuse kasutamise tingimusi, Riigi Infosüsteemi Ameti (RIA) teavitamise kohustust ning Eesti infoturbestandardist (E-ITS) tulenevaid nõudeid infoturbe halduse süsteemile ja meetmeid ohtude käsitlemiseks. Seetõttu tuleb pilveteenuse kasutamise lubatavust hinnata tervikuna, võttes arvesse nii andmekaitse-, andmekogu- kui ka küberturvalisuse nõudeid.

Millised andmekaitsealased nõuded ja piirangud kohalduvad ettevõtjate andmete hoidmisele ja töötlemisele pilveteenuses, kui pilveteenuse pakkuja on rahvusvaheline ettevõtte ning andmed võivad paikneda Euroopa Liidu või Euroopa Majanduspiirkonna territooriumil või väljaspool seda? Kas hinnang sõltub andmete liigist, andmete füüsilisest asukohast või teenusepakkuja suhtes kohaldatavast õigusruumist?

Hinnang sõltub kõigist eelnimetatud asjaoludest. Nagu varasemalt selgitatud, siis olukorras, kus pilves hoitakse üksnes juriidiliste isikute andmeid, siis ei kohaldu neile IKÜM. Kui andmestik sisaldab aga ka tuvastatavate füüsiliste isikute andmeid, tuleb sellele osale kohaldada IKÜM-i.

Teenusepakkuja valikul annab suurema õiguskindluse olukord, kus teenusepakkuja on Euroopa Liidus või Euroopa majanduspiirkonnas asuv ettevõtte ning isikuandmete töötlemiseks kasutatavad vahendid, sh andmekeskused ja varukoopiad, asuvad Euroopa majanduspiirkonnas. Sellisel juhul ei ole tegemist isikuandmete edastamisega kolmandasse riiki IKÜM-i 5. peatüki tähenduses. Samas ei vabasta see vastutavat töötlejat IKÜM-i nõuete täitmisest ehk täita tuleb siiski kõik tavapärased IKÜM-i nõuded, sh tagada õiguslik alus, volitatud töötleja nõuete täitmine, juurdepääsude haldus, logimine, turvameetmed ning andmesubjekti õiguste kasutamise võimalus.

Teenusepakkuja hindamisel ei piisa siiski üksnes andmekeskuse asukoha kindlakstegemisest. Kontrollida tuleb kogu andmetöötlusahelat, sh kus asuvad põhiaandmed ja varukoopiad; kust võib andmetele ligi pääseda; kus osutatakse kasutajatuge, hooldust ja kaughaldust; milliseid alltöötlejaid kasutatakse ja kus nad asuvad; kas teenusepakkuja töötleb meta-, kasutus-, telemeetria- või logiandmeid; millise riigi õigusele alluvad teenusepakkuja, tema kontserni kuuluvad ettevõtted ja alltöötlejad; kas välisriigi õigus võib kohustada teenusepakkujat andmeid ametiasutusele avaldama; kas vastutaval töötlejal on tegelik võimalus kontrollida ja auditeerida andmete töötlemist.

Kui isikuandmed edastatakse Euroopa majanduspiirkonnast väljapoole või võimaldatakse neile juurdepääs kolmandast riigist, siis tuleb lisaks IKÜM-i muudele nõuetele järgida ka IKÜM artikleid 44–49. See tähendab, et edastamine peab põhinema nt Euroopa Komisjoni kaitse piisavuse otsusel või IKÜM-is ette nähtud asjakohastel kaitsemeetmetel.

Üksnes standardsete andmekaitseklauslite sõlmimisest ei pruugi igas olukorras piisata. Vastutav töötleja peab hindama ka sihtriigi õigust ja praktikat ning seda, kas lepingulisi tagatise on tegelikult võimalik järgida. Vajadusel tuleb rakendada täiendavaid tehnilisi, lepingulisi või korralduslikke meetmeid.

Kas sellise registri kavandamisel tuleks lisaks IKÜM nõuetele arvestada veel mõne konkreetse õigusakti või juhendiga, mis käsitleb ettevõtete andmete töötlemist pilveteenustes?

Lisaks IKÜM-ile tuleb uue andmekogu kavandamisel arvestada avaliku teabe seaduse andmekogude regulatsiooni ning riigi infosüsteemi puudutavate nõuetega.

Andmekogu õiguslikus regulatsioonis peavad olema piisavalt selgelt määratud andmekogu eesmärk, vastutav töötleja, vajadusel volitatud töötleja, andmekoosseis, andmeandjad koos edastatava andmekoosseisuga, andmete saajad, juurdepääsu- ja avalikustamisreeglid ning säilitustähtajad. PAKIS-e ja PROTO andmete üleviimisel tuleb hinnata andmekoosseisude jätkuvat vajalikkust, andmete kvaliteeti, varasemaid säilitustähtaegu ning uues andmekogus kasutamise eesmärgipärasust. TVR volitusnormi ja põhimääruse koostamisel soovitame kindlasti tutvuda [Justiits- ja Digiministeeriumi juhise](#)¹.

Samuti, nagu varasemalt selgitatud, tuleb pilveteenuse kasutamisel lisaks andmekaitseõigusele hinnata infoturbe ja küberturvalisuse nõudeid, sh E-ITS-i, küberturvalisuse seaduse, võrgu- ja infosüsteemide küberturvalisuse nõuete ning asjakohaste pilveteenuseid puudutavate nõuete kohaldumist. [E-ITS portaalis](#) on selgitatud, et E-ITS tagab avalike ülesannete täitmiseks kasutatavate äriprotsesside ja infosüsteemide kaitse ning selle põhidokumentides käsitletakse muu hulgas infoturbe halduse süsteemi, etaloniturbe kataloogi ja auditeerimiseeskirja.

Lisaks on asjakohane arvestada Euroopa Andmekaitse Nõukogu ja Euroopa Andmekaitseinspektori pilveteenuseid käsitlevate seisukohtadega. [Euroopa Andmekaitseinspektori juhend](#) on suunatud EL institutsioonidele, organitele ja asutustele, kuid selles esitatud põhimõtted on sisuliselt asjakohased ka avaliku sektori andmekogude pilvelahenduste kavandamisel. Juhendi kohaselt ei tohi pilveteenuse kasutamine vähendada isikuandmete kaitse taset võrreldes muu IT-taristu kasutamisega ning pilveteenuse kasutamisel tuleb säilitada vastutava töötleja kontroll andmetöötluse üle. Juhend rõhutab eriti, et pilveteenuse kasutamisel tuleb enne teenuse hankimist ja kasutuselevõttu hinnata andmekaitseriske, kajastada andmekaitse nõuded hanketingimustes ja lepingus, määrata selgelt poolte vastutus, reguleerida alltöötajate kasutamine, tagada auditivõimalused, määrata andmete ja varukoopiate töötlemise asukohad ning leppida kokku teenuse lõpetamise, andmete tagastamise ja kustutamise kord. Lisaks soovitame tutvuda ka Andmekaitse Nõukogu pilvteenuste kasutamise [ühisjärelvalve kokkuvõttega](#).

Kokkuvõtteks juhime tähelepanu sellele, et Andmekaitse Inspeksiooni pädevus on eeskätt isikuandmete kaitse ja avaliku teabe valdkonnas. Seetõttu ei anna me käesoleva vastusega hinnangut konkreetse pilvearhitektuuri tehnilisele sobivusele ega infoturbestandardite täitmisele. Nendes küsimustes tuleb arvestada RIA pädevust ning vajadusel kaasata RIA juba arhitektuuriliste valikute ettevalmistamise etapis.

Lugupidamisega

/allkirjastatud digitaalselt/

Terje Enula
jurist
peadirektori volitusel

¹ [Andmekaitseõiguse ja avaliku teabe juhised eelnõu koostajale](#)