Andmekaitse Inspektsioon

2025

AASTARAAMAT

Sisukord

01 Peadirektori Pille Lehise eessõna

Inspektsioonil on ümber saanud üks strateegiaperiood ja algamas teine.

Teadlikkus, pädevus, kompetentsus, koostöö ja avatus on jätkuvalt need väärtused, millele meie töö toetub, ja seetõttu järgneval perioodil suuri kannapöördeid oodata ei ole. 2025. aasta on aga väga selgeks teinud, et neid põhimõtteid tuleb rakendada oluliselt keerukamas ja tihedamas õiguslikus ning ühiskondlikus raamistikus kui seni.

Euroopa Liidu digiregulatsioonide laine, mis meid viimasel ajal tabanud on, ei ole lihtne Läänemere loksumine, vaid avamere tohutut jõudu koondav ookeanilaine, kui mitte lausa tsunami. Tulnud on tehisintellekti määrus, andmehalduse määrus, andmemäärus, poliitreklaami määrus, digiturgude määrus. Kõik need toovad Andmekaitse Inspektsiooni töösse uusi rolle, uusi ootusi ja uusi vastutusi. Samas tegutseme kärpetingimustes ja riigi sõnum on kõigile selge. Kuidas sellises vastuolulises olukorras hakkama saada, seda näitab aeg. Sellest tuleb kindlasti üks järgmiste aastate suurimaid väljakutseid.

2025. aastal tundsime selgelt ka ühiskondliku ootuse kasvu. Oodati, et järelevalve oleks jõulisem. Oodati, et reegleid rakendataks ühtemoodi nii avalikus kui ka erasektoris. Oodati, et riik tegutseks läbipaistvalt, selgete seadusest tulenevate normide alusel. Samas ei liigu õigusloome tihti nii kiirelt, kui oodatakse, ja see tekitab pahameelt. On siiski õigustatud ootus, et just riik peab oma tegevuses eeskuju näitama. Alles siis saab teistelt sama nõuda.

2025. aastal oli kaebuste arv rekordkõrge. Iga kaebus on kellegi mure ja kellegi ootus, et riik reageerib. Samal ajal on avalikkuse ootus, et avalik sektor tervikuna oleks väiksem, kiirem ja efektiivsem. Kuidas lahendada seda võrrandit, kus muutujaid on rohkem kui esmapilgul hoomatav? Aus vastus on: see ei ole lihtne.

Just seetõttu tuleb uue strateegia keskmesse paratamatult panna valikute tegemine ja prioriteetide seadmine. Kõiki asju ei saa ega tohi teha korraga. Peame organisatsioonina otsustama, kus on riskid kõige suuremad ja kus on kaalul rohkem kui üksik vaidlus või erimeelsus. See on ka laiem ühiskondlik mõttekoht.

Näeme oma töös üha enam vaidlusi, mis saavad alguse mitte niivõrd andmekaitse rikkumisest, vaid inimeste omavahelistest pingetest: naabrite kaameravaidlused, korteriühistute sisemised konfliktid, peresisesed arusaamatused, sotsiaalmeediapostitused. Sageli on andmekaitse neis lugudes vaid pealispind, mille all on lahendamata inimsuhted.

01

See ei tähenda, et inimesed ei tohiks oma õigusi kaitsta või ei peaks seda tegema. Vastupidi. Ehk on see aga koht, kus igaüks meist võiks küsida, enne kui riigilt abi otsib: kas olen proovinud ise probleemi lahendada? Kas olen rääkinud, selgitanud, kompromissi otsinud? Kas olen üldse pöördunud küsimustega selle isiku poole, kes minu arvates mu õigusi rikub? Kas olen kasutanud elementaarseid eneseabivõimalusi: otsinud infot, miks mitte ka guugeldanud, küsinud küsimusi tehisintellektilt, nõu juristilt või muult õigusnõustajalt? Vahel näib, et peetakse lihtsamaks riigiasutusel seda enda eest teha lasta. Kas see on aga kõige mõistlikum ressursikasutus? Iga kirjarida, e-kiri sinna ja tänna, kõne või arutelu on kellegi töötund, mille jooksul jääb midagi muud ootele. See muu võib olla näiteks hoopis suurema mõjuga ja meid kõiki ohustava rikkumise uurimine.

Valikute tegemisega on tihedalt seotud ka küsimus, mis juba pikka aega Eesti andmekaitsemaastikul õhus ripub: kas ja kuidas on Eestis võimalik tõhusalt trahvida? Sel aastal võeti vastu andmekaitseasutuste koostöö määrus. Selle eesmärk on ambitsioonikas ja vajalik: viia riikidevaheline koostöö piiriülestes menetlustes uuele tasemele. Praktikas tähendab see aga Eesti jaoks uusi, väga huvitavaid väljakutseid. Teame, kui keeruline on Eestis juba praegu olnud väärteomenetluse raames andmekaitsetrahvide rakendamine. Mitu küsimust, mis meid praktikutena vaevavad, ei ole veel vastust saanud. Nüüd aga toob koostöö määrus piiriülestes menetlustes meile uusi ootusi ja seega ka väljakutseid. Et neile küsimustele vastuseid saada ja õigusselgust tuua, tuleb sihikindlalt tegutseda ja julgeid otsuseid teha. Seegi eeldab aga selgete valikute tegemist.

Meie missioon on kasvatada Eestis igal tasandil andmekaitsekultuuri: arusaamist, et andmekaitse ei ole pelgalt reeglid ja takistused. See on usalduse, vastutuse ja üksteisega arvestamise küsimus maailmas, mis muutub kiiremini kui kunagi varem. Meie ülesanne on aidata seda tasakaalu hoida – kui vaja, siis jõuliselt, kuid alati läbimõeldult ja kaalutletult.

Pille Lehis

02 Ennetustöö tegevustes: koolitused, juhised ja proaktiivne lähenemine

Andmekaitse Inspektsioon on iga aasta tähtsaks pidanud ja rõhutanud ennetus- ning koostöö tähtsust. Erandlik ei ole ka möödunud aasta – vastupidi, see kinnitas, et ennetus ei ole ainult riskide vähendamine, vaid strateegiline investeering turvalisusesse, usaldusse ja tulevikku. Järjest rohkem ettevõtteid ja asutusi on hakanud teadvustama andmekaitse vajalikkust ning seda soovitakse integreerida juba protsesside kavandamise ja teenuste disaini algfaasis. On ülimalt positiivne, et sellise teadlikkuse kasvuga kaasneb ka üha sagedasem pöördumine inspektsiooni poole – soovitakse saada nõuandeid, juhiseid ja koolitusi. Kohtumised ja individuaalsed nõustamised on meie jaoks väga olulised, sest need aitavad konkreetseid küsimusi kiiremini lahendada ja tugevdavad koostööd.

Samas on inspektsioon ilmselt üks väiksemaid järelevalveasutusi Eestis, mistõttu ei ole võimalik iga ettevõtet ja asutust alati eraldi koolitada ja nõustada. Selle asemel oleme valinud tegevused, millel on laiem mõju ja mis jõuavad korraga paljudeni – näiteks 2025. aastal käivitatud regionaalsete koolituste sari, ringkirjad, juhendmaterjalid, uudiskirjad ning taskuhäälingu episoodid. Kuigi järelevalveasutusena ei saa me anda õigusabi, siis soovime jätkuvalt pakkuda selgeid juhiseid ja tuge just ennetuse tasandil.

Möödunud aastal külastasid inspektsiooni teenistujad 9 kuu jooksul kaheksat suuremat Eesti linna ja viisid seal läbi tasuta koolitusi väikestele ja keskmiste suurustega ettevõtetele. 2026. aasta alguses toimus veel kaks koolitust Tallinnas ja Tartus. Muu hulgas avaldasime kümnel eri teemal taskuhäälingu „Andmehääling“ saateid, millesse kaasasime ka majaväliseid valdkonna eksperte, et pakkuda kuulajatele mitmekülgset ja praktilist vaadet andmekaitse küsimustele. Kuigi koolitusi korraldada ja taskuhäälingut salvestada aitas Euroopa Liidu CERV-programm (Citizens, Equality, Rights and Values Programme), siis soovib inspektsioon ka tulevikus nende tegevustega jätkata.

Järjest enam soovime reageerida ka proaktiivselt: märgates mõnes valdkonnas või sektoris võimalusi protsesside täiustamiseks ja parimate praktikate juurutamiseks, saadame inspektsioonis ka märguja ringkirju ning uudiskirju – möödunud aastal saatsime neid neljal korral ning adressaate oli kokku ümardatult 450. Samamoodi kajastame aktuaalseid teemasid ka inspektsiooni kvartaalselt ilmuvas uudiskirjas, millel on tellijaid juba umbkaudu 500 isiku ringis.

Kõik need tegevused – koolitused (sh regionaalsed), ringkirjad, taskuhäälingud ja uudiskirjad – on osa meie strateegiast, mille eesmärk on muuta andmekaitse loomulikuks osaks organisatsioonide igapäevatöös. Tulevikku vaadates soovime jätkata laia mõjuga tegevustega, arendada uusi formaate, laiendada koostööd ning reageerida proaktiivselt.

03

Andmekaitsevõrgustike
loomine ja teadlikkuse tõstmine

Isikuandmete kaitse üldmääruse artikli 57 kohaselt on ennetus ja teadlikkuse tõstmine üks andmekaitse järelevalveasutuse põhiülesannetest. Selle paremaks täitmiseks on loodud koostöö valdkonda eraldi tiim: koolitus- ja ennetustiim. Koolitus- ja ennetustiimi eesmärk on luua eri juhendmaterjale, koolitada ja tõsta üldist andmekaitseteadlikkust nii ettevõtete, avaliku sektori kui ka eraisikute seas. Tiimi eesmärgiks on luua kanaleid, mis aitavad andmekaitsekultuuri kujundada ja tugevdada.

Oluliseks sammuks andmekaitsekultuuri edendamisel on 2024. aastal alustatud andmekaitsevõrgustike loomine, et ühtlustada andmekaitsepraktikaid üle Eesti ning pakkuda spetsialistidele võimalusi oma teadmiste täiendamiseks. Esimesena käivitasime haiglate ja kiirabide andmekaitsespetsialistide võrgustiku, millele järgnes andmekaitse võrgustik kohalikele omavalitsustele. Kohalike omavalitsuste võrgustiku tegevustest saab täpsemalt lugeda käesolevast aastaraamatust.

Haiglate ja kiirabide võrgustiku raames oleme alates 2024. aastast korraldanud kokku 6 eri teabepäeva. Haiglate ja kiirabide andmekaitsespetsialistide teabepäevadel on teinud ettekandeid nii meie ise kui ka mitu teist riigiasutust, näiteks Riigi Infosüsteemi Amet, Tervise ja Heaolu Infosüsteemide Keskus, Terviseamet ja Tööinspektsioon. 2025. aasta kevadel kaasasime teabepäevale Tervise Arengu Instituudi inimuuringute eetikakomitee, mille esimees tegi ettekande teadusuuringutest ja patsiendiregistrist, tuues praktilisi näiteid nende erinevustest. Samuti tegi ettekande Terviseamet, kes avas dokumenteerimiskohustuse mõistet ning selgitas, kuidas see erineb terviseandmete edastamistest tervise infosüsteemi.

Haiglate ja kiirabide andmekaitsespetsialistide võrgustiku teabepäevad on andnud parema ülevaate tervishoiusektori probleemkohtadest ja praktilistest muredest nii spetsialistidele endile kui ka järelevalveasutustele. Oleme arutanud koos andmekaitsespetsialistidega, mis tingimused peavad olema täidetud kaamerate paigaldamiseks, kuidas toimida surnu isikuandmetega, millist infot võib edastada lähedastele ning ka seda, kas ja kuidas tohib organisatsioon kui tööandja enda töötaja kohta andmeid koguda ja teda kontrollida.

Teabepäevadest on saanud tervishoiuvaldkonna andmekaitsespetsialistidele järjepidev kohtumispaik, kus enda kogemusi ja väljakutseid jagada. Samas on kinnitust saanud ütlus, et kordamine on tarkuse ema. Näiteks oleme teabepäevadel keskendunud kaameratele ja salvestamisele, kuid siiani kerkib haiglates seoses kaamerate paigaldamisega esile praktilisi probleeme.

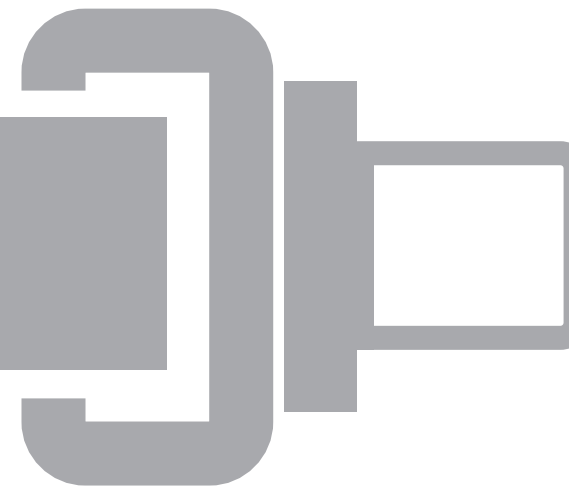
Andmekaitsevõrgustike loomine on kujunenud oluliseks osaks ennetustegevusest ning andmekaitsekultuuri tugevdamisest. Andmekaitsevõrgustikke toetavad ka liikmetele loodud meililistid, mille abil saab omavahel mõtteid põrgatada ja vajadusel meilt varasema praktika kohta küsida. Seetõttu plaanime lisaks haiglate ja kiirabide andmekaitsespetsialistide ning kohalike omavalitsuste võrgustikele luua 2026. aastal eraldi võrgustiku ka haridusvaldkonna töötajatele. Tugev ennetus ja teadlikkuse tõstmine on nii organisatsiooni kui laiemalt ühiskonna turvalisuse ja privaatsuse nurgakiviks.

04 Kohalike omavalitsuste andmekaitsevõrgustik

Andmekaitse Inspektsiooni kohalike omavalitsuste (KOV-ide) andmekaitsevõrgustik on kujunenud oluliseks koostöö ja ennetustöö platvormiks, mille eesmärk on tugevdada omavalitsuste võimekust isikuandmete turvalisel ja õiguspärasel töötlemisel. Soovime, et asutused teadvustaksid veelgi enam, et andmekaitse ei ole pelgalt formaalne nõue, vaid osa avaliku sektori institutsionaalsest vastutusest ja seda olenemata omavalitsuse suurusest. Käesoleva aasta võrgustiku kohtumistel toodigi muu hulgas esile, et andmekaitseriskid on igapäevased, sageli märkamatud ning võivad kiirelt realiseeruda, kui ennetustöö ei ole süsteemselt kavandatud.

Andmekaitsespetsialisti (AKS) määramine KOV-is ei ole formaalsus, vaid seadusest tulenev kohustus[1]. Põhiseadus tagab kohaliku omavalitsuse õiguse otsustada ja korraldada kohaliku elu küsimusi. Mõistagi peavad KOV-id oma tegevuses seaduste raamesse jääma. Kohalikel omavalitsustel on kohustus austada inimeste põhiõigusi ja -vabadusi ning tegutseda ausalt, sh isikuandmete töötlemisel. Tuletame järjepidevalt meelde, et omavalitsusel peab olema määratud pädev andmekaitsespetsialist (AKS)[2], kelle kontakt on nii elanikele kui ka riiklikule järelevalvele ehk inspektsioonile teada. AKS-ile on määrusega antud eri ülesanded[3], sh asutusete personali koolitamine ja nõustamine võimalike rikkumiste ärahoidmiseks. Just AKS on see, kelle erialased teadmised aitavad tõlkida isikuandmete töötlemist puudutavad õigusnormid praktilisteks juhisteks, tagab järjepideva teadlikkuse tõstmise ning hoiab organisatsioonis üleval seadusi ja inimesi arvestavat andmekaitsekultuuri. AKS on oma tegevuses sõltumatu ja tegutseb oma parimate teadmiste alusel. Lõpliku otsuse, kas andmekaitselisi suuniseid järgida või mitte, teeb KOV-i juhtkond, kellel lasub ka vastutus korraldada ja tagada kohane andmetöötlus asutuses.

AKS-i mittemääramine või rolli formaalne täitmine on omavalitsustes endiselt probleem. Kui omavalitsuses puudub inimene, kes tagab süsteemse andmekaitse järelevalve, ennetuse ja ametnike nõustamise, suureneb risk andmeleketeks ja isikuandmete väärkasutuseks, mille tagajärjeks võib olla nii õiguslikud vaidlused kui ka mainekahju. See muudab asutuse haavatavaks ja vähendab usaldusväärsust. Ja kui usaldus on kord kaotatud, siis on seda väga keeruline taastada. Seda näitab praktika.



[1] IKÜM artikkel 37 lg 1 p a
[2] IKÜM artikkel 37, põhenduspunkt 97
[3] IKÜM artikkel 39
[4] Seired | Andmekaitse Inspektsioon

04

Ka inspektsiooni 2025. aasta dokumendiregistrite seire[4] toob välja, miks pädev AKS hädavajalik on. Mitmes omavalitsuse dokumendiregistris olid avalikud näiteks sotsiaalvaldkonna alla kuuluvad dokumendid, mille pealkirjades sisaldusid tundlikud isikuandmed. Sellised rikkumised ei ole pelgalt tehnilised apsud, vaid otseselt inimeste privaatsust kahjustavad juhtumid, mis näitavad selgelt, et teadlikud ennetavad kontrollmehhanismid puuduvad või ei toimi. AKS-i roll ongi muu hulgas aidata selliseid juhtumeid ära hoida, kehtestada anonümiseerimise ja dokumentide haldamise praktika ning tagada, et teenistujad teaksid, kuidas isikuandmeid korrektselt käsitleda. Eesmärk on väärpraktika miinimumini viia, tõstes personali teadlikkust.

Inspektsiooni KOV-ide andmekaitsevõrgustik, mille tegevustega alustati 2024. aasta lõpus ning mille raames on toimunud neli kohtumist, toetab omavalitsusi ennetustöö kaudu. Peame oluliseks konstruktiivset suhtlust ning praktikate vahetamist. Regulaarsetel teabepäevadel saavadki osalejad kogemusi jagada, konkreetseid juhtumeid lahendada ja üksteise praktikast õppida. Selline teadmiste ringlus aitab ühtlustada andmekaitse standardit üle Eesti ning vähendada riski, et mõni omavalitsus andmekaitse süsteemsetest nõuetest maha jääb. KOV-ide andmekaitsevõrgustik jätkab oma tegevusi ka 2026. aastal.

Kokkuvõttes moodustab KOV-ide andmekaitsevõrgustik ühtse ennetussüsteemi, mis tugevdab asutuste sisemist andmekaitsekultuuri ning aitab inimeste usaldust suurendada. Andmekaitse ei ole pelgalt seaduse täitmine, vaid osa heast haldusest ja avaliku võimu legitiimsusest. Seetõttu on ka selle aasta fookus õigustatud olnud: tugev andmekaitse algab pädevast andmekaitsespetsialistist, kes koordineerib asutuses andmekaitsealast teadlikkust ja ennetustööd, ja toimivast koostöövõrgustikust, mille eesmärgiks on teadmiste ja parimate praktikate leviku hoogustamine kõigis Eesti omavalitsustes. Meie eesmärk on, et isikuandmete kaitse oleks KOV-ides sama loomulik kui turvavöö kinnitamine. Praktika näitab, et pädeva andmekaitsespetsialistita on piisavat isikuandmete kaitse taset keeruline saavutada.

05 Andmekaitse
ennetus ja järelevalve koolides

Ennetus. Andmekaitseteadlikkuse tõstmine koolides ja laste seas on olnud läbi aastate meie üks peamistest eesmärkidest. See on olnud tõsine proovikivi: tänapäeva õpilased on kasvanud üles digitaalses ühiskonnas, kus nutiseade on igapäevaelu lahutamatu osa, kuid sageli ei mõelda, milliseid riske isikuandmete liigne jagamine endaga kaasa toob või ei hoolita sellest. Koolide jaoks on väljakutseks aga aja ja ressursside puudus. Kooli esmane ülesanne on hariduse pakkumine, mis hõlmab nii lapse vaimse, füüsilise, kõlbelise, sotsiaalse kui emotsionaalse arengu toetamist. Selle ülesande täitmiseks on vaja jälgida õppekavade täitmist, pakkuda õpilasele vajadusel erituge, tagada kvaliteetne haridus ning täita veel muid kohustusi. Kõige selle tagamisel jäävad andmekaitse ja selle olulisus tihti viimasele kohale.

Selleks et andmekaitset lihtsustada ja tuua nii õpetajatele kui ka koolijuhtidele lähemale, oleme läbi aastate saatnud kooliaasta alguses ringkirju. 2025./2026. õppeaasta alguses saatsime koolidele üle Eesti ringkirja küsimus-vastus-vormis, kus tutvustasime kolme eri teemat: lapsevanema nõusolek, piltide ja videote tegemine ning avaldamine ja tehisintellekti kasutuselevõtmine. Ringkirja tutvustamiseks korraldasime avaliku veebiseminari, kus osalejad said inspektsiooni koostöövaldkonna koolitus- ja ennetustiimi juristidelt nõu küsida ja oma kogemusi jagada. Lisaks võõrustasime nii 2025. kui ka 2024. aastal kahte riigigümnaasiumit. Viisime Andmekaitse Inspektsioonis läbi külalistunnid, mille käigus tutvustasime õpilastele andmekaitse põhimõtteid ja isikuandmete kaitse üldist olulisust.

2025. aasta tõi kaasa ka suure hüppe – TI-hüppe. Tehisintellekt on igapäevatööriistaks saamas nii õpilastel kui ka õpetajatel, mistõttu ei tasu unustada andmekaitset. Tehisintellekt teatavasti ei unusta, vaid õpib talle sisestatud või digitaalsetes allikates leiduva teabe põhjal. Iga sisend võib olla uus ühenduslüli tehisintellekti tehnoloogia arenemisel. Samas on igal inimesel õigus paluda andmetöötlejalt oma isikuandmete kustutamist ehk õigus olla unustatud. Kas tehisintellekt suudab sisestatud isikuandmeid „unustada“ – seda näeme ilmselt alles tulevikus. Seetõttu soovitame koolidel alati iga uue tehnoloogilise lahenduse kasutuselevõtuga läbi mõelda, kas see vastab nii andmekaitse kui ka andmeturbe nõuetele ning milliseid andmeid nii koolitöötajad kui ka õpilased sinna sisestada võivad.

2025. aasta sügisel osalesime ka rahvusvahelises seires, mida koordineerib ülemaailmne privaatsuse jõustamise võrgustik GPEN (Global Privacy Enforcement Network). Seire raames uurisime 30 erinevat laste seas populaarset veebisaiti ja mo-

05

biilirakendust. Seire eesmärgiks oli hinnata, kas ja kuidas laste isikuandmeid kogutakse ning kas see vastab andmekaitse nõuetele. Uurisime näiteks, kas veebileht või mobiilirakendus küsib vanuse tuvastamist, milliseid isikuandmeid kogutakse, kas ja kuidas on võimalik kasutajat või isikuandmeid kustutada ja ka seda, millise sisuga võib laps konkreetsel veebilehel või mobiilirakenduses kokku puutuda. Seire täpsemaid tulemusi tutvustatakse 2026. aasta kevadel.

Haridusvaldkonna töötajate ja ka õpilaste andmekaitseteadlikkus on väga erinev, mistõttu tuleb jätkata eelmistel aastatel seatud eesmärki ning pakkuda järjepidevat teadmiste täiendamise võimalust nii juhendmaterjalide kui ka eri loengutega. Uuest aastast plaanime alustada veebiseminaride sarjaga ja võrgustiku loomisega haridusasutuste töötajatele. Hariduse andmekaitsevõrgustiku eesmärk on luua kogukond, kus pakume liikmetele nii loenguid, juhendmaterjale kui ka võimalust omavahel kogemusi jagada ja üksteiselt õppida, et tagada lastele turvaline ja usaldusväärne keskkond nii koolis kui digimaailmas. Eelmistel aastatel seatud eesmärk kandub seega edasi ka käesolevasse ning suure tõenäosusega tulevasse aastasse, sest laste isikuandmete kaitse olulisus ei ole pelgalt sõnakõlks, vaid oluline põhimõte, mille väärtus peegeldub nii koolis, digikeskkonnas kui ka kodus.

Järelevalve. Ainult heaga alati ei saa, mistõttu on nii mõnigi kaebus ja märgukiri järelevalvemenetluseni jõudnud. 2025. aasta menetlustest nähtus, et andmekaitse haridusvaldkonnas on väga mitmetahuline ning nõuab jätkuvat tähelepanu. Koolid, lasteaiad ja omavalitsused töötlevad iga päev suurt hulka laste isikuandmeid – alates õpitulemustest ja kohalkäimise andmetest kuni tundlikuma teabeni nagu terviseandmed, haridusliku erivajadused ja peresuhted. Selliste andmete käsitlemine eeldab selgeid reegleid ja teadlikke otsuseid, sest iga eksimus võib lapse privaatsust negatiivselt mõjutada ning vanemate ja asutuste vahel arusaamatusi tekitada. Aasta jooksul ilmnes, et kõige rohkem probleeme tekitas just see, kuidas andmeid jagati ja kellel oli neile juurdepääs. Sageli tuli ette olukordi, kus tundlikku infot edastati liiga laialt, puudus selge õiguslik alus või ei vastatud vanemate päringutele õigel ajal. Lisaks tõid digikeskkonnad ja sotsiaalmeedia kaasa uusi riske, mis nõudsid kiiret sekkumist.

Menetlustes piirduti enamasti selgituste ja tähelepanu juhtimisega. Asutustele rõhutati minimaalsuse põhimõtet, õigusliku aluse olulisust ning vajadust vastata vanemate päringutele korrektselt ja õigeaegselt. Mitmel juhul paluti andmetele juurdepääsu piirata ning tõhusamaid turvameetmeid rakendada.

05 Olulisemad järeldused ja soovitused haridusasutustele

1

Selged reeglid andmete töötlemiseks

Iga kool ja lasteaed peaks kirjalikult määratlema, milliseid andmeid kogutakse, kes neile ligi pääseb ja mis eesmärgil.

2

Töötajate regulaarne koolitamine

Paljud rikkumised tulenevad teadmatusest. Oluline on, et töötajad oskaksid isikuandmete töötlemise olukordi ära tunda, mõtleksid enne tegutsemist, kas selline andmete töötlemine on lubatud, ja teaksid, kust vajadusel abi küsida.

3

Ainult vajaduspõhised juurdepääsuõigused

Töötajatel on juurdepääs ainult nende tööülesannete täitmiseks vajalikele andmetele.

05

4

Korrektsed ja õigeaegsed vastused andmetega tutvumise taotlustele

Isikuandmete kaitse üldmääruse (IKÜM) artikli 15 alusel on lapsevanematel õigus tutvuda oma alaealise lapse isikuandmetega ning täiskasvanud õpilastel õigus tutvuda enda isikuandmetega. Vastus tuleb anda 30 päeva jooksul alates taotluse saamisest ning keeldumine peab olema põhjendatud.

5

Sotsiaalmeedias ja õppeinfosüsteemides laste privaatsuse tagamine

Laste pilte, nimesid ja hinnanguid ei jagata laiale ringile ilma nõusoleku või muu õigusliku aluseta.

6

Turvameetmete tugevdamine

Selleks tuleb kasutada sobivaid tehnilisi ja korralduslikke meetmeid, näiteks turvalisi paroole, mitmeastmelist autentimist ja vajadusel andmete krüpteerimist.

06 Töötajate joobe kontrollimisest – kas on tulemas oodatud lahendus?

Läbi aastate on kirgi kütnud tööandjate õigused ja kohustused, mis puudutavat töötaja joovet ja selle tuvastamist[1], sest tööandja peab tagama ohutu töökeskkonna ja täitma oma seadusest tulenevat kohustust mitte lubada joobes töötajaid tööle.

Isikuandmete kaitse vaatest on joove eriliiki isikuandmed (terviseandmed), mis on tugevamalt kaitstud, kui nii-öelda tavalised isikuandmed. Ühtlasi peab terviseandmete töötlemisel olema tavapärasest hoolsam, sest võimalik privaatsuseriive on suurem ning selliste tundlike andmete kasutamisel võib olla töötajale märkimisväärne kahjulik mõju. Seega on tööandjal kohustus tagada ka andmekaitsenõuete täitmine. Mh peab töötaja terviseandmete töötlemiseks olema õiguslik alus.

Praegusel hetkel sellist õiguslikku alust üheski seaduses ei ole ning ei ole võimalik tugineda ka otse isikuandmete kaitse üldmäärusele, nt töötaja vabatahtlikule nõusolekule. Samuti ei ole võimalik tööandjatele joobe kontrollimise õigust anda eri õigusaktides toodud kohustuste tõlgendamise teel, vaid säte, mis näeb ette eriliigliste isikuandmete töötlemise (joobe kontrollimine), peab olema seaduses välja toodud, selge, täpne ja ettenähtav.

[1] Oleme sellel teemal varemgi kirjutanud: Tähelepanekuid terviseandmete töötlemise osas | Andmekaitse Inspektsiooni aastaraamat

06

Seega on seadusandja pannud tööandjale palju kohustusi tööohutuse tagamiseks, kuid ei ole andnud efektiivset meedet selle teostamiseks. Ka töötervishoiu ja tööohutuse seaduse muudatusest jäeti aastal 2022 välja säte, mis võimaldaks tööandjal töötaja joovet kontrollida.

Probleem aga ei kadunud ning üha rohkem tööandjaid jõudis meieni küsimusega, kuidas täita seaduse nõuet ohutu töökeskkonna tagamisel ja samal ajal kaitsta töötajate isikuandmeid.

Seega pöördusime selle aasta suvel ettepanekuga[2] Sotsiaalministeeriumi ja Majandus- ja Kommunikatsiooniministeeriumi (MKM) poole täiendada asjakohaseid õigusakte ning luua siseriiklikult õiguslik alus, mis reguleeriks töötajate joobe kontrollimist. 05.11.2025 algatas MKM töötervishoiu ja tööohutuse seaduse muudatuse, mis muu hulgas käsitleb ka tööandjale laiemate õiguste andmist töötaja joobe kontrollimisel. Hetkel on eelnõu kooskõlastuste saamise etapis ning ei ole teada, kas planeeritav muudatus ka tegelikult jõustub, kuid samm selgema õigusliku raamistiku suunas on astutud.

[2] Vt ka Andmekaitse Inspektsioon saatis ministeeriumitele ettepaneku luua õiguslik alus töötajate joobe kontrollimiseks | Andmekaitse Inspektsioon

07 Töötajate jälgimine
töökeskkonnas

Tänapäeva töökeskkond on üha digitaliseeritum. Jälgimisseadmete kasutamine on saanud vältimatuks osaks igapäevasest töökorraldusest ning paraku ka töötajate kontrollimise vahendiks. Kuigi tehnoloogia pakub tööandjale võimalusi turvalisuse tagamiseks ja tööprotsesside tõhustamiseks, mõjutab jälgimine otseselt töösuhete kvaliteeti, sest läbipaistvuse puudumine, ebamäärased reeglid ja kontroll võivad tekitada töötajates ebakindlust, vähendada initsiatiivi ja nõrgestada usaldust tööandja vastu.

Levinumad jälgimisviisid on videovalve, GPS-seadmed, arvutite ja e-posti kasutamise monitoorimine ning biomeetrilised süsteemid, näiteks näokujutise- või sõrmejäljelugejad. Praktikas ei ole tööandjad nende vahendite kasutamisel sageli läbipaistvad ega õiguspärased. Inspektsioon sai 2025. aastal arvukalt kaebusi ja märgukirju, kus töötajad tõid välja, et nende töökohustusi kontrollitakse jälgimisseadmete abil ning seetõttu on tööõhkkond stressirohke. Pöördumistes ilmnes murettekitav trend: paljud ei julge probleemi tööandja juures tõstatada või kui seda on tehtud, pole see olnud tulemuslik. Tihti pöördutakse meie poole alles pärast töösuhte lõppu. Inspektsiooni lauale jõudis juhtumeid, kus näiteks videovalve katab kogu töökeskkonda, jälgitakse reaalajas tööülesannete täitmist, tööl tekkinud erimeelsusi soovitakse lahendada helisalvestistega. Ühe juhtumi puhul anti töötajale kaamerapildi abil distantsilt häälkäsklusi töövõtete parandamiseks ja puhkepauside lõpetamiseks. Selline tegevus on töötaja õigusi äärmiselt riivav ning ei vasta proportsionaalsuse ning eesmärgikohasuse nõuetele. Küsimusi on tekitanud ka ebaselgus biomeetriliste andmete töötlemise reeglites tööaja arvestamiseks ning GPS-seadmete kasutamine töötajate liikumiste jälgimiseks, mis viitab sellele, et seadmed võetakse kasutusele läbimõtlematult või töötajatele nende õigusi selgitamata. Selline praktika tekitab ebakindlust ja õõnestab usaldust tööandja vastu.

Töölepingu seaduse järgi on tööandja kohustatud töötaja privaatsust austama ning kontrollima töökohustuste täitmist viisil, mis ei riku töötaja põhiõigusi. Üldmääruse kohaselt on andmete kogumine ja töötlemine lubatud üksnes siis, kui selleks on selge õiguslik alus. Üldjuhul tugineb see tööandja õigustatud huvile ning alati tuleb järgida ka proportsionaalsuse ja minimaalsuse põhimõtteid. Koguda tuleks ainult neid andmeid, mis on õigustatud huvide elluviimise seisukohalt hädavajalikud. Enne jälgimisseadmete kasutuselevõttu tuleb kaaluda mõlema poole huvisid, meede peab olema proportsionaalne ja töötajat mitte ülemäära riivav ning koostada tuleb õigustatud huvi analüüs. Näiteks võib õigustatud huvi seisneda ettevõtte vara kaitses või tööohutuse tagamises, kuid pelgalt soov kontrollida töökohustuste täitmist ei kaalu üles töötaja õigust jälgimisvabale töökeskkonnale. Biomeetriliste andmete, näiteks sõrmejälgede või näokujutiste töötlemine

07

nõuab aga erilist ettevaatust, kuna tegemist on töötaja eriliiki andmetega ning selliste tundlike andmete töötlemine ei saa tugineda õigustatud huvile, vaid eeldab vaba nõusoleku olemasolu ning seega alternatiivide pakkumist.

Liigne jälgimine võib viia usalduskriisini tööandja ja töötaja vahel ning suurendab riski, et kogutud andmeid kasutatakse diskrimineerivalt või need lekivad kolmandatele osapooltele. Seetõttu tuleb jälgimismeetmeid hinnata ka tööpsühholoogilisest ja organisatsioonilisest vaatenurgast, mitte üksnes tehnilisest efektiivsusest. Eraelu puutumatus peab olema tagatud ka töökohal. Probleemide vältimiseks peab tööandja selged töökorraldusreeglid kehtestama. Töötajate teavitamine ja regulaarne koolitamine aitab suurendada usaldust ning vähendada konflikte. Töötajal on õigus teada, milliseid andmeid temalt kogutakse ja kuidas neid kasutatakse, kui kaua andmeid säilitatakse ning kellele need avaldatakse. Samuti võib töötaja vaidlustada jälgimise, mis on ebaproportsionaalne. Tööandja huvides on luua keskkond, kus tagasisidet saab anda turvaliselt, kartmata negatiivseid tagajärgi. Nii toetab jälgimine praktikas seda, milleks ta on mõeldud – turvalise keskkonna loomist –, ilma et see muutuks kontrolliks usalduse ja õiguste arvelt. Läbipaistvus ei ole pelgalt formaalsus: see vähendab usaldamatust ja võimaldab töötajatel adekvaatselt reageerida ning vajadusel oma õigusi kaitsta.

Jälgimisseadmete kasutamine töösuhetes on paratamatu osa kaasaegsest töökorraldusest. Kui kontroll muutub peamiseks eesmärgiks ja puudub läbipaistvus, kannatavad töösuhe ning töötajate õigused. Tasakaalu leidmine seadmete kasutamise vajaduse ja töötaja privaatsuse vahel on võtmetähtsusega, et tagada terve ja usaldav tööõhkkond.

08 Patsiendisaladusega kaitstud andmete väljastamine – kas võib ja kellele?

Viimase aasta jooksul on hüppeliselt sagenenud Andmekaitse Inspektsiooni pöördumiste arv, kus soovitakse selgitusi, kas tervishoiuteenuse osutaja (TTO) võib patsiendi terviseandmeid väljastada kolmandale osapoolele – nt kindlustus, lastekaitse, tööandja, kohtutäitur jne. Selline areng on positiivne, sest näitab tervishoiutöötajate teadlikkuse kasvu ning hoolikat kaalumist enne andmete väljastamist. Samuti on vähenenud kaebused nn uudishimupäringute[1] kohta, mis kinnitab, et isikuandmete kaitse põhimõtteid järgitakse üha enam.

Isikuandmete kaitse seisukohalt kuuluvad terviseandmed eriliiki andmete hulka ning nende töötlemine ilma õigusliku aluseta on keelatud. Tervishoiuteenuse osutajate õiguslik alus andmete töötlemiseks tuleneb otseselt tervishoiuteenuse osutamisest, kuid sellega kaasneb ka kohustus kaitsta patsiendisaladust. Oluline on rõhutada, et iga andmete töötlemise toiming peab põhinema eraldi õiguslikul alusel. Seega ei saa patsiendile teenuse osutamise alusel kogutud andmeid hiljem kolmandatele isikutele samal alusel edastada, sest tegemist on eraldiseisva toiminguga, mis ei ole seotud esialgse eesmärgiga ehk patsiendile teenuse osutamisega.

Seega peab ka andmete väljastamiseks olema õiguslik alus ning patsiendi andmeid ei tohi väljastada, kui seaduses või kokkuleppel patsiendiga ei ole ette nähtud teisiti (võlaõigusseadus § 768).

Riigikohus on lahendis 1-20-5071 (1.04.2022) asunud seisukohale, et seadusest tulenev alus terviseandmete väljastamiseks võib olla kahetine – kas andmete avaldamist lubav või selleks kohustav. Kohustus patsiendisaladuse avaldamiseks võib tuleneda mõnest valdkondlikust õigusaktist. Sellisel juhul on seadusandja otsustanud, et avalik huvi on olulisem patsiendi huvist hoida tervishoiuteenuse osutamise käigus avaldatud andmed saladuses. Näiteks saab siin tuua abivajavast lapsest teavitamise kohustuse.

Lubav alus võib seevastu olla seotud mõne asutuse või ettevõtte seadusest tulenevate ülesannete täitmisega, näiteks kohaliku omavalitsuse kohustus hinnata lapse abivajadust, kindlustusandja kohustus hüvitada kahjujuhtumi kulud või kohtutäituri ülesanne kontrollida kohtumääruse täitmist hooldusõiguse vaidlustes. Igal juhul peab andmeid küsiv asutus alati viitama konkreetsele seadusesättele, pelgalt menetluse olemasolu ei ole piisav alus.

Ka õigusliku aluse olemasolu ei tähenda aga, et välja võib anda kogu teabe tervisliku seisundi kohta ning TTO kohustus on hinnata, kas andmete väljastamine küsitud ulatuses on põhjendatud.

Patsiendi andmete väljastamisel peab mh lähtuma ka isikuandmete kaitse üldpõhimõtetest, eelkõige eesmärgipärasuse ja minimaalsuse põhimõttest (IKÜM-i artikkel 5). See tähendab, et andmeid peab

[1] Uudishimupäringutest on AKI varasemalt kirjutanud siin: Andmelekked ja isikuandmete töötlemise rikkumised | Andmekaitse Inspektsiooni aastaraamat.

väljastama ainult nii palju, kui on vajalik eesmärgi täitmiseks ja nii minimaalselt kui võimalik (lihtsalt päringule vastamine vrd epikriisi väljastamine). Kui tekib kahtlus, on tervishoiuteenuse osutajal õigus küsida täpsustust, milliseid andmeid vajatakse ja miks just sellises mahus.

Kokkuvõttes võib järeldada, et ükski seadus ei anna tervishoiutöötajale õigust avaldada patsiendiandmeid kolmandale isikule laiemalt, kui see on seaduses või patsiendiga kokkuleppes ette nähtud. Patsiendisaladuse kaitse on tervishoiutöötaja kohustus ning andmete avaldamine peab alati põhinema selgel õiguslikul alusel ja järgima isikuandmete kaitse põhimõtteid.

Pane tähele! Kui eelnevalt käsitlesime olukorda, kus tervishoiuteenuse osutaja peab otsustama, kas ja millises ulatuses võib patsiendi andmeid kolmandatele isikutele väljastada, siis sama oluline on eristada olukordi, kus andmete väljastamist taotleb andmesubjekt ise. Kolmandate isikute puhul on aluseks nende seadusest tulenev õigus või kohustus, samas kui andmesubjekti puhul tuleneb õigus otse isikuandmete kaitse üldmäärusest (artikkel 15). Seda õigust saab piirata ainult rangelt määratletud tingimustel, näiteks teiste isikute õiguste kaitseks (art 15 lg 4) või siseriikliku seaduse sättega, mis vastab artikli 23 nõuetele.

Viimasel juhul peab olema selgelt määratletud, milliseid andmesubjekti õigusi piirang puudutab ja millises ulatuses neid piiratakse. Näiteks võib piirang puudutada õigust andmetega tutvumisele, nende parandamisele või kustutamisele. Ühtlasi ei või IKÜM-i artikli 23 alusel kehtestatud piirang olla absoluutne ega tähtajatu ning seega peaks olema reguleeritud ka piirangu tähtaeg.

Viimase aasta jooksul on ette tulnud mitu menetlust, kus tervishoiuteenuse osutaja on andmesubjektile andmete väljastamisest keeldunud, tuginedes tervishoiuteenuste korraldamise seaduse (TTKS) muudatusele, täpsemalt § 32 lõikele 4. Selle sätte kohaselt on dokumenteeritud patsiendiohutusjuhtumitele ja nende analüüsimisega seotud dokumentatsioonile juurdepääs lubatud üksnes tervishoiuteenuse osutajale ning kriminaalmenetluses uurimist teostavale organile. Käesoleval juhul TTKS-i § 32 lõige 4 andmesubjekti õigusi siiski ei piira. Mõistame probleemi olemust ning seadusandja tahet piirangu kehtestamisel ning oleme vastava sätte ja IKÜM-i artikli 23 omavahelise suhte kohta esitanud seisukoha ka ministeeriumile.

09

Kui avalik info muutub isiklikuks: andmekaitse piiridest infoportaalide näitel

Tänapäeval koguvad mitmed portaalid avalikest allikatest kättesaadavaid andmeid ning taasavaldavad neid uuel kujul – näiteks loovad juriidilise isiku esindajate kohta mahukaid profiile. Ei tasu unustada, et ka juriidilist isikut esindava füüsilise isiku kohta käivad andmed on isikuandmed.[1] Sageli pöörduvad meie poole murelikud kodanikud, kes tunnevad, et selliseks andmete taaskasutamiseks ei ole keegi nende nõusolekut küsinud. Kuigi esmapilgul võib tunduda, et tegemist on avaliku teabega, tekib küsimus, kas sellisel moel avalike andmete taasavaldamine eraettevõtete poolt on ikkagi lubatud? Kas inimesel säilib kontroll selle üle, kuidas tema andmeid kasutatakse?

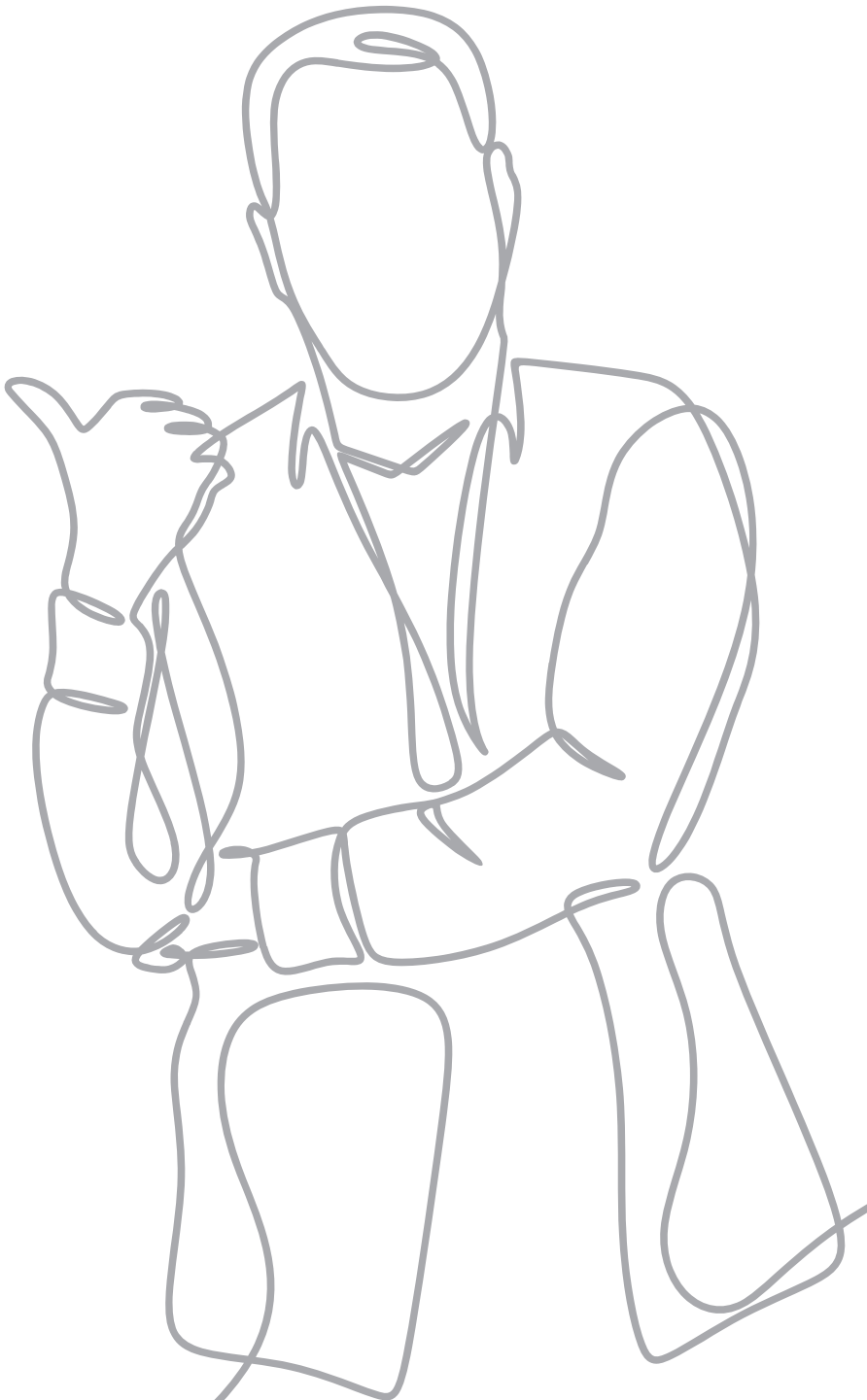
Kui isikuandmete taasavaldamisel tugineb andmetöötleja õigustatud huvile, siis ei eelda see isikult eelneva nõusoleku võtmist. Samas peab õigustatud huvi alusel andmete töötlemine olema inimesele ettenähtav ja läbipaistev ja see ei tohi inimese õigusi ülemääraselt kahjustada. Oluline on tähele panna, et isikuandmete kaitse üldmääruse ehk IKÜM-i artikkel 21 annab igale inimesele õiguse oma isikuandmete töötlemisele vastuväiteid esitada, kui see toimub õigustatud huvi alusel. Vastuväide peab olema põhjendatud – inimene peab selgitama, kuidas töötlemine tema õigusi ülemääraselt riivab. Andmetöötlejal aga lasub kaasaaitamise kohustus – ta võib inimeselt täiendavat teavet küsida, et olukorda õiglaselt hinnata.

Viisime 2025. aastal ühe infoportaali kohta läbi omaalgatusliku menetluse, mille raames tegime andmetöötlejale ettepaneku isikuandmete kaitse nõuete paremaks järgimiseks. Andmetöötleja nõustus üldjoontes meie ettepaneku täitmisega ning viis vajalikud muudatused sisse, sealjuures lõpetas füüsiliste isikute jälgimise funktsiooni pakkumise ja muutis maine- ja krediidiskoori kuvamise lahendust. Täiendavalt lihtsustas andmetöötleja andmete eemaldamise protsessi avalikust vaatest, lõpetas automaatse meediamonitooringu, muutis eri alajaotiste sõnastust läbipaistvamaks, võttis kasutusele anonümiseerimise lahenduse seoses kohtulahendite taasavaldamisega ning asus inimesi süsteemselt andmetöötlusest teavitama. Meie hinnangul on tehtud muudatused äärmiselt positiivsed ning suurendavad andmesubjektide kontrolli oma isikuandmete üle.

[1] Eko C-710-23, p 21-22.

09

Soovitame andmetöötlejatel, kes taasavaldavad avalikest allikatest kogutud isikuandmeid, sh ka juriidilise isiku esindaja andmeid, veenduda selles, et andmetöötluseks on olemas õiguslik alus ja et töötlemisel järgitakse isikuandmete kaitse nõudeid. Andmetöötlus peab olema läbipaistev ja isikul peab olema tagatud reaalne võimalus sellele omapoolseid vastuväiteid esitada (st et taotlust hinnatakse sisuliselt) ning andmete kustutamist nõuda. Samas peaksid vastuväidet esitada soovivad isikud oma pöördumises välja tooma ka argumendid, mismoodi töötlemine nende õigusi ülemääraselt riivab. Seejärel saab andmetöötleja neid ka oma hinnangus arvesse võtta.



10 Äriregistri läbipaistvus ja privaatsus: kus jookseb piir?

Äriregister on andmekogu, mis koondab kõiki Eestis asutatud juriidiliste isikute andmeid. Selle eesmärk on tagada läbipaistvus ja õiguskindlus äritegevuses – et igaüks saaks kontrollida ettevõtte olemasolu, juhtorganite koosseisu, nende esindusõigust, otsuste vastuvõtmist ja muid olulisi andmeid. Kuna iga juriidilise isiku tegevus on seotud inimestega ja toimub nende kaudu, koondab äriregister vältimatult märkimisväärses mahus isikuandmeid: nimesid, isikukoode, sünniaegu, aga ka tegevusega seotud dokumente. Nii jõudsid meieni üha sagedamini inimeste pöördumised, kes on pidanud äriregistris nende isikuandmete töötlemisega seonduvat problemaatiliseks.

Viisime läbi järelevalvemenetluse, et hinnata, kas isikuandmete töötlemine äriregistris vastab kehtivatele nõuetele. Tegime äriregistri pidajale Justiits- ja Digiministeeriumile ettepaneku isikuandmete kaitse nõuete paremaks täitmiseks. Ministeerium on oma praktikat andmetöötluse osas osaliselt juba muutnud ja väljendanud valmisolekut võtta ette ka õigusaktide muudatused.

Esimene olulisem ministeeriumile tehtud ettepanek puudutab äriregistris välismaiste isikukoodide avaldamise lõpetamist. Praegu näeb äriregistri seadus ette, et juhatuse liikme nimi ja isikukood tuleb kanda registrikaardile. Need andmed on avalikud. Kui inimesel Eesti isikukoodi ei ole, avaldatakse tema välismaine isikukood. See praktika on tekitanud küsimusi, sest mitmes riigis on isikukoodil oluliselt suurem õiguslik tähendus kui Eestis. Nii tuleb meie hinnangul arvestada, et äriregistris avaldatavad andmed puudutavad ka muid Euroopa Liidu kodanikke ja nende andmed peavad üldmääruse kohaselt olema kaitstud ka siin.

Kuigi kehtiv regulatsioon äriregistris isikukoodide avaldamise kohta ei tee vahet Eesti ja välismaiste isikukoodide vahel, on Justiits- ja Digiministeerium analüüsinud isikukoodide sisulisi erinevusi ning nõustunud meiega, et mõne välismaise isikukoodi avaldamine võib isiku eraelu puutumatust riivata. Seetõttu kaalub ministeerium seadusemuudatust, mille kohaselt avalikustatakse Eesti isikukoodi puudumisel e-äriregistris isiku sünniaeg.

10

Teine meie tehtud olulisem ettepanek puudutab äriregistris isikuandmete tähtajatut avaldamist. Praegu on registris määramata ajaks nähtavad endiste juhatuse liikmete ja muude esindusõiguseta isikute andmed. Olukord puudutab mh näiteks neid, kes on olnud ettevõtte juhatuse liikmed juba 20 aastat tagasi ega soovi enam, et nende isikuandmeid äriregistris avalikkusele kuvataks. Leidsime, et selline igavene isikuandmete kuvamine ei ole kooskõlas üldmäärusest tuleneva säilitamise piirangu põhimõttega, mille järgi tohib isikuandmeid säilitada ainult seni, kuni see on vajalik eesmärgi täitmiseks. Esindusõiguseta isikute andmete tähtajatu avaldamine ei täida enam registri eesmärki ega ole õiguskindluse tagamiseks vajalik. Tegime ministeeriumile ettepaneku määrata selged ajavahemikud või kriteeriumid, kui kaua isikuandmeid äriregistris avalikkusele kuvatakse. Seejuures ei ole vaidluse all arhiiviseadusest tulenev äriregistri andmete alalise säilitamise küsimus, vaid just nimelt isikuandmete avalik kuvamine, mis peab meie hinnangul olema ajaliselt piiratud. Ministeerium on meie ettepanekuga nõustunud ja asunud ka selles osas muudatusi ette valmistama.

Lisaks käsitlesime menetluses ka teisi teemasid, mis tähelepanu vajasid. Nende hulgas on äriregistris olevate isikuandmete indekseerimine otsingumootorites, mis võib suurendada andmete väärkasutuse riski, ning avalikes dokumentides – näiteks korteriühistute protokollides ja volikirjades – leiduvate tundlike isikuandmete avalikustamine. Ka nende teemade puhul tuleb leida tasakaal läbipaistvuse ja privaatsuse vahel ning rakendada tehnilisi ja korralduslikke meetmeid, mis vähendavad riske. Ministeerium on selle kohta oma selgitused edastanud ja arvestanud ka meie tähelepanekutega.

Nii tulebki tõdeda, et kuigi äriregister on juriidiliste isikute ja ettevõtjate tegevuses õiguskindluse ja läbipaistvuse tagamiseks oluline, toob selle avatus kaasa vastutuse kaitsta inimese õigust isikuandmete kaitsele. Leida tuleb tasakaal ettevõtlusega seotud läbipaistvuse ja inimeste privaatsuse vahel, et viimane neist liigselt riivatud ei saaks.

11

Apotheka andmeleke:
kui turvameetmed jäävad ajale jalgu

Veebruaris 2024 leidis aset Eesti seni ulatuslikuim andmeleke, mis puudutas rohkem kui poolt elanikkonnast – sisuliselt iga teist Eesti elanikku. Kuu aega kestnud ründe käigus pääsesid ründajad ligi Allium UPI OÜ hallatavale Apotheka lojaalsusprogrammi süsteemile ning laadisid alla kliendiandmebaasi varukoopiafailid 2014.–2019. aastatel programmi kogutud Apotheka apteekide, Apotheka Beauty veebipoe ning PetCity poe kliendiandmetega. Kokku lekkis 19 GB andmeid, mis sisaldasid üle 750 000 inimese isikuandmeid (nimi, isikukood või sünniaeg, sugu, kontaktandmed, elukoha aadress) ning ostuajalugu. Ligi saadi ka hilisemale, 2020. aasta ostuajaloole. Ostuajalugu hõlmas väga suures ulatuses isikustatud tundlike ostude andmeid, sealhulgas ravimite, tervisetoodete ja tervisenäitajate mõõtmise teenuste kohta. Lekkinud andmekoosseis annab otseselt või kaudselt teavet inimese tervise kohta, mistõttu kvalifitseerub see terviseandmeteks ehk eriliiki isikuandmeteks IKÜM-i artikli 9 tähenduses ning vajab seetõttu kõrgematasemelist kaitset.

Algatasime intsidendi kohta järelevalvemenetluse ja hiljem väärteotunnuste ilmnemisel ka väärteomenetluse.

Kuigi Allium UPI OÜ andis meile nõuetekohaselt isikuandmetega seotud rikkumisest teada, otsustas ta andmesubjekte juhtunust mitte teavitada, hinnates ekslikult, et lekkinud andmestik ei sisaldanud ravimite andmeid ja seetõttu oli potentsiaalne kahju piiratud. Jõudes vastupidisele järeldusele ja leides, et süsteemist lekkinud andmestikku kuulub ka tervisele osundav teave ja selle kolmandale isikule teatavaks saamine kujutab endast andmesubjektidele suurt ohtu IKÜM-i artikli 34 tähenduses, kohustasime ettevõtet inimesi teavitama ja andma juhised ohtude leevendamiseks.

2025. aasta sügisel määrasime Allium UPI OÜ-le 3 miljoni euro suuruse rahatrahvi Apotheka lojaalsusprogrammi süsteemis isikuandmete töötlemisel IKÜM-i artikli 5 lg 1 punktis f ette nähtud usaldusväärsuse ja konfidentsiaalsuse põhimõtte rikkumise eest, mis seisnes vastutava töötleja üldise kohustuse (IKÜM-i artikkel 24), andmekaitsemeetmete lõimimise ja vaikimisi rakendamise kohustuse (IKÜM-i artikkel 25) ning riskipõhist lähenemist kasutades isikuandmetele asjakohase turvalisuse tagamise kohustuse rikkumises (IKÜM-i artikkel 32).

Heitsime Allium UPI OÜ-le väärteona ette, et tema rakendatud turvameetmed ei taganud süsteemis töödeldavate isikuandmete IKÜM-i nõuetele vastavat turvalisuse taset. Ründajad said süsteemile volitamata juurdepääsu turvanõrkuste ärakasutamise tõttu, mis tõi kaasa ulatusliku isikuandmete, sealhulgas terviseandmete ebaseadusliku kaotsimineku.

IKÜM kohustab vastutavat töötlejat tagama, et isikuandmeid töödeldakse viisil, mis kaitseb neid loata või ebaseadusliku töötlemise, juhusliku kaotsimineku, hävimise või kahjustumise eest, rakendades asjakohaseid tehnilisi ja korralduslikke meetmeid. Selleks tuleb arvesse võtta töötlemise laadi, ulatust, konteksti ja eesmärke ning lõimida andmekaitsemeetmed töötlemisprotsessi ja neid vaikimisi rakendada. Rakendatavad korralduslikud ja tehnilised meetmed peavad olema proportsionaalsed ohuga andmesubjektide õigustele ja vabadustele.

11

Väärteomenetluses selgus, et Allium UPI OÜ ei rakendanud mitut kriitilist ja ka tavakasutajale üldteada turvameedet. Näiteks kasutati süsteemi sisenemisel autentimisvahendiks üksnes parooli, ei rakendatud mitmikautentimist, administraatorikonto kasutajanime ja parooli kasutas mitu isikut ühiselt, võimaldades selle edasijagamist. Puudusid ka need kaitsemeetmed, mida võis andmetöötlejalt eeldada, arvestades töötlemise laadi, konteksti ja ulatust ja arvestades talle IKÜM-iga pandud kohustusi. Näiteks:

- võrgupiirangud ja turvaseire olid puudulikud;
- andmebaasi varukoopiad hoiti ebaturvaliselt;
- volitatud töötlejate rollid ja vastutus olid ebaselged ning kontroll nende tegevuse üle vähene;
- ettevõttes kehtivad andmekaitsemeetmed jäeti süsteemile rakendamata;
- puudusid ennetusmeetmed mittevajalike (nt ravimitega seotud) andmete süsteemi sattumise vältimiseks jt.

Mida juhtumist õppida? Apotheka andmeleke näitas, et andmekaitse ei ole pelgalt formaalsus, vaid valitud reeglite tegelik rakendamine ning turvameetmete ajakohasuse ja töötlemise riskile vastavuse pidev hindamine ja kontroll kogu andmetöötluse elutsükli vältel. Vastutav töötleja peab jälgima tehnoloogia arengut ja rakendama sellele vastavaid turvalahendusi. Juhtum tuletab meelde, et vastutava töötleja kohustus ei piirdu usaldusväärse volitatud töötleja valimisega – ta peab aktiivselt kontrollima rakendatud meetmete asjakohasust ja toimivust, vajadusel kaasama pädevaid eksperte ning korraldama kasutatavate lahenduste auditeid.

Eriti olukorras, kus isikuandmete töötlemine on ettevõtte äritegevuse keskne osa, peab sellega kaasas käima ka vastav andmekaitse tase. Kord lekkinud andmeid ei ole võimalik tagasi pöörata ning nende väärkasutuse risk võib realiseeruda alles aastate pärast, mistõttu inimese kontroll oma andmete üle ei tohi teenuste või hüvede nimel kunagi kaduda.

Allium UPI OÜ-le karistuse määramisel lähtusime rikkumise raskusest, ettevõtte võimekusest, ning võtsime arvesse ka koostöö ulatuse menetluse käigus. Arvestades rikkumise süsteemset ja pikaajalist iseloomu, lekkinud andmete tundlikkust, mõjutatud isikute suurt arvu ning kasutusele võetud turvameetmeid, oli rahatrahvi määramine selles olukorras proportsionaalne ja sobiv meede. Allium UPI OÜ kaebas otsuse kohtusse ning edasine selgub kohtumenetluses.

12 Politsei andmekogu järelevalve

Algatasime aprillis järelevalvemenetluse politsei andmekogus „Infosüsteem POLIS“, et hinnata isikuandmete töötlemise vastavust õigusaktidele ning kontrollida tööprotsesside toimivust. Vaatluse all olid päringute teostamine, andmete arhiveerimine ja kustutamine, logimine, juurdepääsuõigused ning numbrituvastuskaameratega seotud tegevused. Menetluse tulemusel tegime Politsei- ja Piirivalveametile (PPA) ettekirjutuse, et tuvastatud puudused saaksid kõrvaldatud. Menetluse jooksul tegi PPA meiega igakülgset koostööd, selgitas oma praktikat, rakendas muudatusi ning on nüüdseks ettekirjutuse nõuded täitnud.

Kuigi järelevalve oli ajendatud aprilli lõpus numbrituvastuskaamerate kasutusega seotud küsimustest, siis sellel teemal me oma menetluses tähelepanekuid kordama ei hakanud. Nimelt oli PPA ise viinud läbi teenistusliku kontrolli ja jõudnud oluliste järelduste ning muudatusteni. Samuti võttis Riigikogu vastu numbrituvastuskaamerate andmetöötluse regulatsiooni.[1]

POLIS-e eripäraks on, et see koosneb mitmetest alaminfosüsteemidest. Üheks alaminfosüsteemiks on menetluse infosüsteem (MIS), kus töödeldakse süüteomenetluse andmestikku (menetluste ja toimingutega seotud andmed). Selle puhul tuvastasime, et PPA ei järginud õigusaktidega kehtestatud andmete arhiveerimise ja kustutamise tähtaegu. MIS-is hoiti alles andmed, mis tegelikult oleksid

12

pidanud olema kas arhiveeritud ja/või kustutatud. Isikuandmete kaitse üldmäärus näeb ette isikuandmete säilitamise piirangu põhimõtte, mille järgi ei tohi isikuandmeid säilitada vajalikust kauem. Õigusaktides on kindlaks määratud tähtajad, millal tuleb POLIS-es olevad andmed esmalt arhiveerida ja seejärel kustutada. On lubamatu andmeid edasi säilitada, kui alust selleks ei ole.

Õigel ajal MIS-is olevate andmete arhiveerimata ja kustutamata jätmine oli üks põhjustest, miks tegime Politsei- ja Piirivalveametile ettekirjutuse. Samas ei piisanud olukorra lahendamiseks üksnes vanade andmete kustutamisest. Kohustasime PPA-d looma ka toimiva lahenduse, mis tagaks edaspidi andmete regulaarse arhiivi kandmise ja kustutamise vastavalt õigusaktides sätestatud tähtaegadele. Tänaseks on see nõue täidetud.

Teine suurem probleem tuli esile seoses analüüsi ja andmelao infosüsteemiga. Leidsime, et PPA kasutatav andmeladu ja selles toimuv andmetöötlus vajab suuremat läbipaistvust. POLIS-e põhimäärusest ning PPA selgitustest nähtus, et andmelao andmeid kasutatakse muu hulgas politseitegevuse analüüsimisel ja statistilistel eesmärkidel. Eesmärke võib andmelao kasutamisel veelgi olla, kuid andmelao olemasolu ega selle kasutamise eesmärke õigusaktidest ei ilmne. Meie hinnangul tuleb andmelao olemasolu sõnaselgelt nimetada vastava andmekogu põhimääruses või muus õigusaktis. Samuti tuleb eristada, mida tehakse lähteandmekogus ja mida andmelaos. Seejuures peab asutuses olema selgelt määratletud tööprotsess, millistel tingimustel on lubatud andmelaos olevate isikuandmete põhjal koostada isikustatud aruandeid, näiteks millistele kontrollküsimustele peab aruande tellija enne selle tellimist vastama ning millal on kohustuslik andmekaitsespetsialisti kaasamine. Andmelaost isikuandmete põhjal koostatavate aruannete tellimine peab toimuma alati kindlal eesmärgil, mis on selgelt määratletud ja vajaliku andmekoosseisuga piiratud.

Andmelaoga seoses jätkub mitmete asutuste omavaheline koostöö. Tõdeme, et regulatsiooni andmelao osas sisuliselt ei olegi ja olemasolevad juhised võivad eriarvamusi põhjustada. On oluline, et saavutaksime selles osas selguse.

Politsei andmekogu menetlus näitas, kui oluline on tehniliste ja organisatsiooniliste meetmete pidev arendamine ja süsteemne lähenemine. Seejuures ei ole andmekaitsega seonduv ühekordne tegevus, vaid järjepidev protsess, mis peab käima kaasas tehnoloogia ja õigusruumi arenguga. Isikuandmete töötlemise läbipaistvus on usalduse alus – inimesed peavad teadma, kuidas ja milleks nende andmeid kasutatakse. Esile tõstmist väärib veel kord PPA tahe vajalikud muudatused ellu viia. Meie kõigi huvides on, et andmeid töödeldakse õiguspäraselt ja turvaliselt.

[1] Politsei ja piirivalve seaduse täiendamise seadus 670 SE.

13 SMS vahendusteenuse pakkujate seire

Viisime 2025. aasta maikuust kuni septembrini läbi seire mobiilsideteenuse osutajate ja nende kaudu SMS-vahendusteenust pakkuvate andmetöötlejate vahel. Seire eesmärk oli välja selgitada andmetöötluses osalejate rollid, andmete liikumise ahel ja kasutatavad turvameetmed.

Seire tulemusel selgus, et SMS-vahendusteenuse puhul käsitletakse agregaatorite rolli sageli ekslikult iseseisvate vastutavate töötlejatena, kuigi tegelikkuses tegutsevad nad pigem volitatud töötlejatena kliendi juhiste alusel. Samuti tuvastasime, et turvameetmete tase erineb osapoolte vahel ning on valdavalt reaktiivne – tihtipeale ennetav kontroll puudub. See võib aga isikuandmete turvalisuse tagamise ohtu seada.

SMS-vahendusteenus võimaldab kliendil (ettevõttel või eraisikul) saata mass-sõnumeid lõppkliendi seadmesse. Selleks kasutatakse vahendusteenuse pakkujat ehk agregaatorit, kes edastab sõnumid vastavatele mobiilsideoperaatoritele, kes tagavad omakorda nende kohaletoimetamise.

Seire esimeses etapis esitasime järelepärimise Eesti mobiilsideoperaatoritele (Telia, Elisa, Tele2) ja teises etapis Eestis tegutsevatele SMS-vahendusteenuse pakkujatele (Messente, ESTERIA, Top Connect). Vastuste põhjal saime teha järgnevad järeldused.

Kuidas on üles ehitatud andmetöötluse ahel?

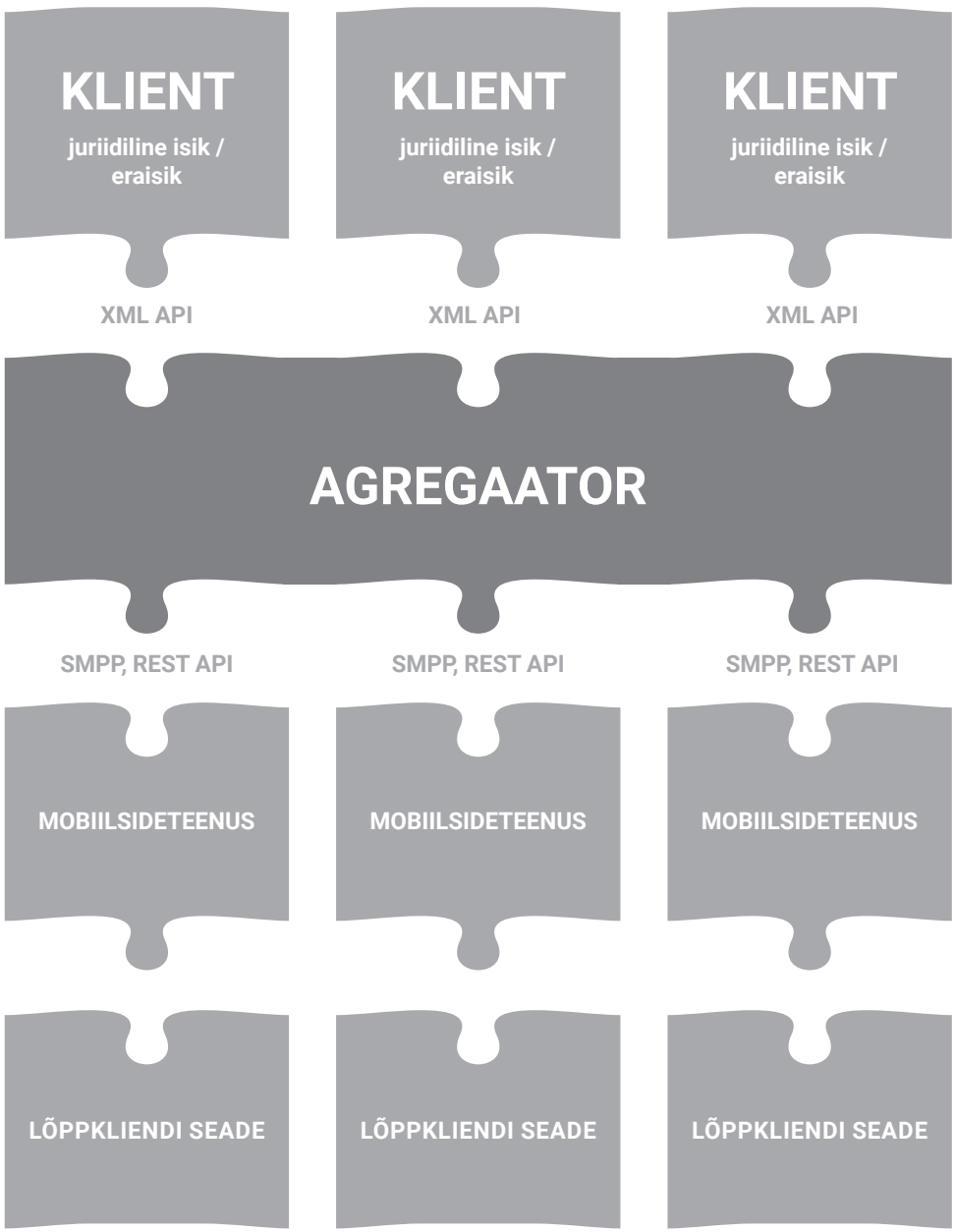
Andmevahetuse ahela skeem kujutab andmevoogu klientide ja lõppklientide seadmete vahel. Kliendid (eraisikud või juriidilised isikud) algatavad teenuse agregaatoriga teatud sõnumi gateway ehk lüüsi (XML API[1] vms lahenduse) kaudu. Agregaator omakorda edastab andmed lõppkliendi telefoninumbri alusel vastavale mobiilsideteenustele SMPP[2] või REST API[3] kaudu. Mobiilsideteenused suunavad seejärel info lõppklientide seadmetesse.

[1] XML API on rakendusliides, mis vahetab andmeid, kasutades sõnumivorminguna XML-vormingut (eXtensible Markup Language).

[2] SMPP (short message peer-to-peer protocol ehk lühiteadete otseühendusprotokoll) on telekommunikatsioonitööstuse protokoll SMS-sõnumite vahetamiseks iInterneti kaudu. SMS-sõnumid läbivad tavaliselt SMPP, et ühendada välised süsteemid sõnumikeskusega, mis töötleb suuri SMS-mahtusid. SMPP kasutab TCP/IP-d või sellega seotud protokolli, et ühenduda sõnumikeskusega ja edastada või vastu võtta tellija (abonent) sõnumeid.

[3] rakendusliidese (API) programmiliides, mis järgib REST-arhitektuuristiili disainipõhimõtteid. REST on lühend sõnadest representational state transfer (esitusoleku siire) ja on reeglite ja juhiste kogum, mis käsitleb veebi API ehitamist.

13


KLIENT
juriidiline isik / eraisik
KLIENT
juriidiline isik / eraisik
KLIENT
juriidiline isik / eraisik
XML API
XML API
XML API
AGREGAATOR
SMPP, REST API
SMPP, REST API
SMPP, REST API
MOBIILSIDETEENUS
MOBIILSIDETEENUS
MOBIILSIDETEENUS
LÕPPKLIENDI SEADE
LÕPPKLIENDI SEADE
LÕPPKLIENDI SEADE

13

Andmetöötlejate rolliselgus

Kogutud vastuste põhjal märkasime trendi, kus agregaatoreid peeti iseseisvaks vastutavaks töötlejaks. Selline käsitlus ei ole meie hinnangul kooskõlas isikuandmete kaitse üldmääruse (IKÜM) loogikaga ega Euroopa Andmekaitsenõukogu juhistega (Guidelines 07/2020).

SMS-vahendusteenuse puhul edastab klient (ettevõte või eraisik), kes soovib sõnumit saata, agregaatorile isikuandmeid: saaja info ning sõnumi sisu (sh võivad selle taotluse korral teatavaks saada ka teised isikuandmed). Agregaator edastab need andmed omakorda mobiilioperaatorile, kes tagab sõnumi kohaletoimetamise. Kuigi operaator ei pruugi sõnumi sisu näha, töötleb ka tema saaja isikuandmed IKÜM-i artikli 4 lõike 1 ja 1 tähenduses.

Andmetöötlus toimub algse taotluse esitanud kliendi nimel ja eesmärgil – klient algatab sõnumi saatmise, valib sihtrühma ning määrab sõnumi sisu. Agregaator tegutseb seejuures kliendi nimel ja juhiste alusel, mistõttu on ta volitatud andmetöötleja IKÜM-i artikli 4 lõike 8 ja artikli 28 tähenduses.

Samas saame nõustuda sellega, et mobiilioperaator võib olla SMS-vahendusteenuse puhul iseseisev vastutav töötleja, kes pakub sideteenust elektroonilise side seaduse alusel. Tema kohustused andmete töötlemisel ja säilitamisel tulenevad pigem seadusest, mistõttu on ta ka nende andmete iseseisev vastutav töötleja.

Andmetöötluse ahela puhul võib vale rollimääratlus vähendada läbipaistvust ja raskendada oma õiguste tagamist andmesubjekti ehk lõppkliendi jaoks ning samuti võib kaasa tuua vastutuse hajumise eri osapoolte jaoks nt pettuste ennetamisel ning nende käsitlemisel. Seejuures on ääretult oluline, et kõigil osapooltel oleks selge nende roll andmetöötluses ja sellest tulenevad kohustused.

Reaktiivne lähenemine turvalisusele

Mobiilsideteenuse osutajad ja SMS-vahendusteenuse pakkujad on meie hinnangul küll kasutusele võtnud eri tehnilisi ja korralduslikke turvameetmeid (nt krüpteerimine, logimine, turbeauditid), kuid tuvastasime, et andmetöötluses osalevatel osapooltel puudub piisav ennetav kontroll sõnumite sisu ja saatjate üle. Enamikul juhtudel reageeritakse vaid andmesubjektide kaebustele. See ei pruugi aga olla piisav IKÜM-i artikli 32 nõuete täitmiseks, mis eeldab proaktiivseid turvameetmeid.

Oluline on rõhutada, et agregaatoritele saadetud andmete hulk (sõnumite sisu ja lõppkliendi andmed) on sageli avatud tekstide, st krüpteerimata kujul. Agregaatoritel on seega tehniline võimalus näha kogu saadetava info sisu. On ääretult oluline, et agregaatorite süsteemides oleks turvalisus tagatud kõrgel tasemel.

Kõigil andmetöötluse osapooltel, sealhulgas operaatoritel ja agregaatoritel, on kohustus teha koostööd, et rakendada ühtseid ja mõjusaid lahendusi, mis aitavad ennetada sõnumite teel levivaid pettusi ning tagada isikuandmete asjakohase turvalisuse.

13

Siin on mõned konkreetsed soovitused, mida saavad kõik agregaatorid ja mobiilsideteenuse pakkujad juba täna rakendada selleks, et tagada turvalisem isikuandmete töötlemine ning pettuste ennetamine:

1. **sõnumite logimise ja analüüsi automatiseerimine, et tuvastada kahtlaseid mustreid;**
2. **süsteemide regulaarne turbeaudit, mis hindab nii tehnilisi kui ka protseduurilisi riske;**
3. **anomaaliaid tuvastavate süsteemide kasutamine, mis võimaldab varakult märgata pettusele viitavaid tegevusi;**
4. **ligipääsukontrollide rakendamine ja jälgimine, et piirata juurdepääsu sõnumite sisule;**
5. **rangemad reeglid saatja ID kuvamisele, et vältida saatja maskeerimist (nn spoofingut[4]).**

[4] Spoofing-rünnak (teisisõnu teesklus) on olukord, kus isik või programm identifitseerib end edukalt teisena, võltsides andmeid, et ebaseadusliku eelist saada. Näiteks võib keegi sulle helistada või sõnumi saata riigiasutuse numbrilt, aga tegelikult ei ole see riigiasutus, vaid pettur.

14 Kohalike omavalitsuste dokumendiregistrite seire

Seire taust

Alates 2001. aastast reguleerib avaliku sektori tegevuse läbipaistvust avaliku teabe seadus (AvTS). Selle seaduse eesmärgiks on tagada üldiseks kasutamiseks mõeldud teabe avalikkus, võimalusega igaühel sellisele teabele juurde pääseda. Riigi- ja kohalike omavalitsuse (KOV) tegevuse avalikkus ja läbipaistvus on üks olulisemaid põhimõtteid, mis tagab demokraatliku riigikorralduse ning igaühe õiguste ja vabaduste teostamise. Üheks olulisimaks printsiibiks teabe avalikustamisel on avaliku sektori kohustus oma tegevuse käigus saadud ja loodud teave avalikustada seda küsimata ning üheks selliseks teabe avalikustamise väljundiks on asutuse võrguleht. Avaliku teabe seaduse § 28 lg 1 annab loetelu teabest, mille teabevaldajad on kohustatud oma võrgulehel avalikustama. AvTS § 28 lõike 1 punkti 31 kohaselt tuleb võrgulehel avalikustada ka asutuse dokumendiregister. Täpsemad nõuded dokumentide avalikustamise kohta dokumendiregistri kaudu on ära toodu AvTS §-s 12.

Seire eesmärgid

Seire eesmärgiks oli vaadelda, kuidas omavalitsused avaliku teabes sätestatud teabe avalikustamise nõudeid täidavad. Valiku tegemisel, millise teabe avalikustamist kontrollida, sai lähtutud ka sellest, mille kohta on esitatud enim kaebusi ning millise teabe leidmine võiks kodanikule oluline olla. Samuti soovisime kaardistada üldist teabe avalikustamise olukorda omavalitsustes.

14

Seire teiseks eesmärgiks oli hinnata dokumendiregistris dokumendile juurdepääsu võimaldamise ja AK teabe kaitsmise olukorda. Samuti oli seire eesmärgiks kontrollida, kas ja kuidas kevadise märgukirja saatmine on parandanud dokumendiregistrites AK teabe kaitsmise olukorda. Kuigi kevadine märgukiri puudutas eelkõike ühinenud valdade vanu dokumendiregistrid, palus inspektsioon oma märgukirjas üle vaadata ka kasutusel olevad dokumendiregistrid. Seekordne seire puudutaski eelkõige just praegu kasutusel olevaid ajakohaseid dokumendiregistreid.

Lisaks oli seire eesmärgiks ka välja selgitada parim dokumendiregister. Selleks hindasime ka dokumendiregistrites avaliku teabe seaduse paragrahvis 12 toodud erinevate nõuete täitmist. Kui dokumendiregistris registreeritud dokumentide osas olid nõuded nõuetekohaselt täidetud, siis oli omavalitsusel iga kontrollitud dokumendiliigi või seaduses sätestatud nõude täitmise eest võimalik saada ühe punkti. Kui aga leidsime mingi kontrollitud nõude täitmisel vähemalt kolm eksimust, siis punkti ei saanud. Väiksemate eksimuste puhul oli võimalik saada ka 0,25-0,75 punkti. Seire tulemused avalikustati 29.oktoobril toimunud avaliku teabe ja avaandmete konverentsil.

Seire kokkuvõte olulisemate tähelepanekutega

AK-märgete olemasolu ja dokumentidele juurdepääs. AvTS § 12 lõike 3 punkt 6 kohustab dokumendiregistrisse kandma ka dokumendi kohta kehtivad juurdepääsupiirangud.

Kuigi aasta-aastalt on piirangute kajastamise olukord dokumendiregistrites paremaks muutunud ning dokumente, millel puudub piirangumärge, kuid samas ei võimaldata dokumendile dokumendiregistri kaudu juurdepääsu, on küll vähem, kuid siiski on dokumendiregistrites selliseid dokumente jätkuvalt lubamatult palju.

Ka on dokumendiregistris jätkuvalt üsna palju asutustevahelist kirjavahetust ja lepinguid, millele on kehtestatud juurdepääsupiirang eraelu kaitseks. On üsna küsitav, kas asutustevaheline kirjavahetus või lepingud ikka sisaldavad nii paljudel juhtudel kellegi eraelu kahjustavat teavet. Eraelu kahjustavaks teabeks ei ole kindlasti asutuse või ettevõtte töötaja tööalased kontaktid. Samas on dokumendiregistritest võimalik leida aga füüsiliste isikute kirju, kus on avalikud nii isiku nimi kui kontaktandmed.

Eksimusi on ka piirangu tähtaegades. Näitena võib tuua olukordi, kus piirang on kohe kehtestatud maksimaalselt kümneks aastaks, kuigi seadus lubab piirangu kehtestada korraga viieks aastaks. Oli ka palju dokumente, millele oli eri sätete alusel kehtestatud piirang 75 aastaks, kuigi seadus lubab piirangu 75 aastaks kehtestada ainult isikuandmeid sisaldavale teabele.

Samas on isikuandmetele mõnel juhul kehtestatud piirang hoopis viieks aastaks. Viimane ei ole iseenesest rikkumine, kui dokument tõesti enne piirangu lõppu hävitatakse või tähtaega enne piirangu lõppu pikendatakse, kuid kui dokumente ei jõuta õigel hävitada või piirangut pikendada, tekib oht, et piiranguga isikuandmed saavad avalikuks.

Uurides omavalitsustelt põhjusi, miks kevadel leitud vanad dokumendid avalikuks said, oligi üheks põhjuseks see, et isikuandmeid sisaldavatele dokumentidele oli piirang kehtestatud viieks aastaks ning tähtaja möödumisel piirangut pikendatud ei olnud.

14

Seega on isikuandmete puhul mõistlik kehtestada piirang kohe 7. aastaks. Eeltoodu ei keela säilitustähtaja möödumisel dokumente hävitada. Piirangu tähtaeg ei ole seega kuidagi seotud säilitustähtajaga.

Seire käigus leidsime, et tihti on dokumentidele märgitud juurdepääsupiirangu alused, mida konkreetne dokument ilmselt ei sisalda. Näitena võib tuua dokumendi, kus veeohutusstendide paigaldamise lepingule oli kehtestatud piirang kui kriminaal- või väärtoemenetluses kogutud teabele, või kus volikogu liikme arupärimisele oli kehtestatud piirang volikogu töökorraga, kuigi piiranguid saab kehtestada ainult seaduse alusel. Need on ainult mõned näited piirangu ebaõigetest alustest.

E-kirjadele juurdepääsu võimaldamine

AvTS § 12 lõige 41 kohustab teabevaldajaid dokumendiregistri kaudu võimaldama juurdepääsu dokumendihaldussüsteemis sisalduvatele elektroonilistele dokumentidele, millele ei ole kehtestatud juurdepääsupiirangut. Selliseid kirju, millele ei ole kehtestatud piirangut, kuid millele ei ole dokumendiregistri kaudu ka juurdepääsu võimaldatud, on dokumendiregistrites ka eelnevate seirete käigus leidunud. Leidsime neid ka käesoleva seire käigus. Käesoleva seire läbiviimise ajaks oli olukord küll paranenud, kuid rahul olla siiski ei saa. Kuna seire käigus ei ole võimalik kogu dokumendiregistrit dokumendihaaval kontrollida, otsustasime, et kui leidsime juba kolm e-kirja, millele ei olnud kehtestatud juurdepääsupiirangut, kuid ei võimaldatud ka dokumendiregistri kaudu juurdepääsu, siis konkreetne omavalitsus e-kirjadele juurdepääsu võimaldamise eest punkti ei saanud.

Dokumendiregistrites hakkas silma ka metaandmete ebakorrektne täimine ning ka eksitava teabe edastamine, seda eriti dokumendihaldusprogrammi Amphora kasutajate puhul. Kuigi seires ei antud punkte metaandmete korrektsuse eest, siis ei saa jätta tähelepanu juhtimata asjaolule, et paljudes dokumendiregistrites oli dokumendi saajaks/saatjaks märgitud eraisik, kuid kui dokument oli avalik, siis selgus, et tegelikult oli kirja saajaks/saatjaks hoopis juriidiline isik. Sellisel juhul on tegemist eksitava teabe andmisega ning tekib kahtlus, kui palju eraelu kaitseks seatud piirangutest on üldse õiguspärased.

Füüsiliste isikute nimede kajastamine dokumendiregistri avalikus vaates

Alates 2016. aastast ei luba seadus dokumendiregistri avalikus vaates kajastada füüsilisest isikust kirjasaatja/-saaja kohta teavet, mille kaudu on füüsilised isikud tuvastatavad. Üldiselt seda nõuet täidetakse ja eraisikute nimesid dokumendiregistri metaandmetes ei avalikustada, s.t nimed on asendatud initsiaalidega või märgitud „eraisik".

Kuigi enamik omavalitsusi seda jälgib, on siiski omavalitsusi, kus just sotsiaalvaldkonna dokumentides on isikute nimed avalikud. Selliste näidetena võib välja tuua näiteks „Eeskoste seadmine Mari Maasikas" või „Sotsiaaltoetuse taotlemine Jüri Juurikas". Eeltoodu on eriti kahetsusväärne just seetõttu, et tihti on avalikud just nende isikute nimed, kes pole võimelised oma õigusi kaitsma ja on kõige haavatavamad. See hakkab eriti silma ka seetõttu, et kui asutuse töötajate nimesid püütakse varjata ka seal, kus selleks puudub õiguslik alus, siis abivajajate nimede avalikustamise puhul riivet ei nähta. Ka siis, kui dokumendid ise ei ole avalikud, kuid pealkirjas

14

on isiku nimi avalik, võib olla riive juba toimunud. Nii saab näiteks eestkoste puhul järeldada, et isik ei tule oma eluga iseseisvalt toime. Seekord jäi selliseid dokumente eriti palju silma. Kuigi dokumendid ise avalikud ei olnud, võttis inspektsioon kõigi omavalitsustega, kelle dokumendi pealkirjades olid isikute nimed avalikud, telefonitsi ühendust ja juhtis valla tähelepanu isikute õiguste rikkumisele ning palus nimed eemaldada, et rikkumine kiiresti lõpetada.

Selline olukord teeb inspektsiooni väga murelikuks, sest tekib küsimus, et kui pistelise kontrolli käigus tuleb ka peale kevadise märgukirja edastamist jätkuvalt välja nii palju dokumente, kus on eestkostetavate isikute nimed avalikud, siis kui palju neid tegelikult võib veel dokumendiregistrites avalikult kättesaadaval olla. Seda, et kontrolli käigus ei ole võimalik kõiki dokumente avastada, ilmestab ka näide, kus näiteks ühe hästi eeskujuliku ja avaliku dokumendiregistri kontrollimisel ei leidnud seire läbiviija selliseid dokumente, kuid enne parema asutuse väljaselgitamist palus seire läbiviija ka oma kolleegidel selle asutuse dokumendiregistrit kontrollida ning teine ametnik leidis ikkagi dokumendi, mis sisaldas eestkostetava andmeid.

Eeltoodu näitab, et KOV-ide dokumendiregistrites on jätkuvalt palju sotsiaalvaldkonna dokumente, mis sisaldavad ka abivajavate isikute nimesid ning halvemal juhul on ka mõni selline dokument avalik. On lubamatu, et kui isik vajab abi ning pöördudes omavalitsuse poole, ei saa ta olla kindel, et omavalitsus ei tee tema abivajadust oma dokumendiregistri kaudu kõigile kättesaadavaks. Omavalitsustel tuleb oma registrid üle kontrollida, sest ka ühe sellise dokumendi avalikuks saamine on palju.
AK-teabe avalikkus

Avaliku teabe seadus kohustab kehtestama juurdepääsupiirangu dokumentidele, mis sisaldavad piiranguga andmeid, ning mitte avalikustama dokumente isikutele, kellel puudub õigus neid dokumente saada. Paraku leidsime ka selle seire käigus dokumendiregistris dokumente, mis peaksid olema piiranguga, kuid olid avalikud.

Kuna seire käigus pöörasime erilist tähelepanu just tundlikes sarjades registreeritud dokumentidele, leidsime nii sotsiaaltoetuste avaldusi, kus küsitakse isikutelt hulgaliselt andmeid ka pereliikmete kohta, sh ka nende tervisliku seisundi kohta. On äärmiselt kahetsusväärne, kui mõni selline dokument on dokumendiregistri kaudu kõigile kättesaadav – see riivab väga tugevalt isiku eraelu puutumatust.

Kuigi iga avalikuks saanud dokumendi puhul ei saa alati asuda seisukohale, et seda dokumenti on loetud ja alla laetud, ei tähenda see seda, et rikkumist ei ole toimunud.

Tihti tuuakse järelevalvemenetluse käigus põhjuseks, et konkreetse dokumendi on registreerinud uus töötaja ning peale dokumendi avalikukssaamist ta meil enam ei tööta. Siinkohal tahaks juhtida omavalitsuse töötajate tähelepanu sellele, et uute töötajate puhul kontrollige esialgu, kuidas nad dokumentidele piiranguid kehtestavad ja dokumente registreerivad, s.t aidake neil sisse elada, et oma tööd hästi teha. Samas ei saa ju garanteerida, et järgmine uus töötaja ei eksi.

Tähelepanu köitis ka see, et kui asutusetega peetud kirjavahetusele kehtestame piirangu AvTS § 35 lg 1 p 12 alusel, siis füüsiliste isikute kirjavahetuse puhul avalikustame nii nime, elukoha kui e-posti aadressi.

14

Kõiki dokumente ei kuvata dokumendiregistri avalikus vaates

Seiret läbi viies hakkas silma, et õigusaktide, sh käskkirjade puhul on dokumendiregistris osa numbreid puudu. Dokumendiregistrist peab olema üle teksti otsinguga võimalik otsida kõigi metaandmete järgi, sh kas otsida ainult ühe metaandmete välja (näiteks dokumendi liigi järgi) või mitme välja kaudu korraga (näiteks dokumendi liigi ja sarja numbri järgi).

Seire käigus sai ka selgeks, et mõnel juhul võivad dokumendid küll dokumendiregistris avalikud olla, kuid kui ei ole teada, kuidas registris on otsingud üles ehitatud, ei pruugi dokumente leida. Sai ka selgeks, et eri omavalitsuste dokumendiregistrites on dokumendid leitavad eri otsingutega, mis teeb teabe soovijatele teabe leidmise tihti keeruliseks.

Kuna avaliku teabe seaduse üheks põhimõtteks on teabele lihtsa ja kiire juurdepääsu võimaldamine, ei saanud seiratav omavalitsus punkti siis, kui kõiki dokumente leida ei õnnestunud, kuna ei saa eeldada, et asutuseväline dokumendiotsija peaks täpselt teadma, millise otsinguga dokumendid leitavad on.

Lisatasude ja puhkuse käskkirjade avalikustamine

AvTS § 12 lg 2 kohaselt tuleb asutuse dokumendiregistris registreerida ka asutuses koostatud ja allkirjastatud õigusaktid, milleks on ka personalikäskkirjad. Samas lubab seadus dokumendid dokumendiregistris ka registreerimata jätta, kui need on registreeritud mõnes teises registris ja neile võimaldatakse selle kaudu juurdepääs. See tähendab, et kui mõni omavalitus avalikustab oma personalikäskkirju mõnes muus registris, tuleks dokumendiregistri juurde lisada link, kust vastav teave leitav on.

Lisaks eeltoodule hakkas 15.03.2019 avaliku teabe seaduses kehtima säte, mis ei luba kehtestada juurdepääsupiirangut ka töölepinguga töötajate palgaandmetele. See tähendab, et töölepinguga töötajate palgaandmeid ei pea küll avalikustama avaliku teenistuse veebilehel, kuid kuna seadus ei luba neile juurdepääsupiirangut kehtestada, siis dokumendiregistris neile piirangut kehtestada ei saa.

Seire käigus ilmnes aga, et mõned omavalitsused on töölepinguseaduse § 28 lõike 2 punkti 13 alusel kehtestanud preemiate ja lisatasude maksmise käskkirjade piirangu. Kuna avaliku teabe seadus on avaliku sektori asutuste osas eriseaduseks lisatasude ja preemiate käskkirjade avalikustamise osas – sellele seisukohale asus ka Riigikohus oma 17.10.2018 otsuses nr 3-15-3228 –, siis preemia ja lisatasude maksmise käskkirjadele piirangu kehtestamine töölepingu seaduse § 28 lõike 2 punkti 13 alusel ei ole seadusega kooskõlas ega õiguspärane. Kuigi käesolevas seires ei kontrollitud, kas omavalitsusete hallatavad asutused on lisatasude käskkirjadele piiranguid kehtestanud, köitis siiski tähelepanu, et väga paljud hallatavad asutused, kelle töötajad saavad töötasu eelarvelistest vahenditest, on töölepingu seaduse alusel lisatasu käskkirjadele piirangu kehtestanud.

Lisaks oli tihti nii puhkuse, lähetuse kui ka lisatasu käskkirjadele kehtestatud piirang AvTS § 35 lõike 1 punkti 12 alusel. Mööname, et mõnel juhul võib eeltoodu alusel piirangu kehtestamise õiguspärane olla: kui käskkiri sisaldab ka eraelu puudutavat sündmust, nagu näiteks lapsehoolduspuhkust või

toetuse maksmist seoses perekondliku sündmusega. Kui aga enamikule personalikäskkirjadele on kehtestatud piirang AvTS § 35 lõike 1 punkti 12 alusel, siis ei ole usutav, et kõik käskkirjad sisaldavad eraelu puudutavat teavet.

Vallavalitsuse protokollide avalikustamine

Kuna volikogu istungite protokollid on reeglina leitavad, vaatlesime seekord vallavalitsuste istungite protokollide leitavaust. Üldiselt olid protokollid leitavad, kuid siiski oli mõnel vallal mõni protokoll vahelt puudu. Samuti ei õnnestunud ühe omavalitsuse istungite protokolle leida.

Kokkuvõtete tegemine

Seekordse seire käigus tuli tõdeda, et kohalike omavalitsuste dokumendiregistrites on hulgaliselt andmeid, mis ei tohiks seal avalikud olla – eriti just füüsiliste isikute nimed sotsiaalvaldkonna dokumentide pealkirjades. Kuigi dokumendid ise avalikud ei olnud, on riive toimunud ka juhul, kui pealkiri koos füüsilise isiku nimega reedab isiku tervisliku seisundi või sotsiaalse toimetuleku.

Seega tuleb kohalikel omavalitsustel oma dokumendiregistrid täiendavalt üle vaadata ning piiranguga andmed eemaldada. Kuna dokumendiregistrites on ka väga palju vanu dokumente alates 2000. aastate algusest, tuleks üle vaadata, millistel dokumentidel on säilitustähtaeg möödunud, need hävitada ja arhiiviväärtuslikud dokumendid arhiivile üle anda.

Lisaks seires leitud puudustele teeb inspektsiooni murelikuks ka asutuste teabenõuetele vastamine. Seda põhjustel, et viimasel ajal on jõudnud inspektsiooni menetlusse vaideid, kus teabenõude esitamisel küsitakse teabenõudjatelt põhjendusi, miks üht või teist teavet küsitakse või teabenõude allkirjastamist nõutakse, kuigi teabenõudja märgib oma teabenõudes, et ei soovi piiranguga andmeid. Avaliku teabe seadus ei näe ette kohustust, et teabenõudja peaks põhjendama, miks ta mingit avalikku teavet soovib. Põhjendamise kohustus on ainult juhul, kui soovitakse piiranguga andmeid või kui seadus näeb selgesõnaliselt ette, et teavet väljastatakse ainult õigustatud huvi alusel. Muul juhul ei pea teabenõudja põhjendama, miks ta mingit teavet soovib ega ka teabenõuet allkirjastama.

Viimasel ajal ei ole enam haruldased ka juhtumid, kus isegi juhul, kui isik põhjendab oma teabe saamise soovi, keeldutakse ikkagi teabenõude täitmisest põhjendusega, et küsitud teave ei ole teabenõudjaga seotud ning seetõttu puudub vajadus teabe väljastamiseks. Avaliku teabe seadus ei anna teabevaldajale õigust asuda teabenõudja eest otsustama, kas, mis eesmärgil ja millist teavet ta vajab. Ka juhul, kui dokument sisaldab piiranguga teavet, ei tähenda see seda, et teabenõude korral sellist dokumenti ei väljastata. Teabenõude korral tuleb väljastada see osa teabest või dokumendist, millele piirangud ei laiene. Seega vajavad kohalike omavalitsuste teenistujate teadmised siin järele aitamist ning vajadusel tuleb kohalikel omavalitsustele oma teenistujaid koolitada.

15 Euroopa andmekaitseasutuste ühisseire: andmesubjekti õigus olla unustatud

Euroopa Andmekaitsenõukogu koordineerib tänavu juba neljandat aastat liikmesriikide järelevalveasutuste ühistegevust, mille raames keskendutakse igal aastal ühe andmekaitsevaldkonnas aktuaalse probleemi uurimisele. 2023. aastal keskenduti andmekaitsespetsialistide rollile. 2025. ja 2024. aastal on olnud fookus aga andmesubjekti õigustel. Kui 2024. aastal keskenduti andmesubjekti õigusele tutvuda töödeldavate isikuandmetega, siis möödunud 2025. aastal on ühisseire keskmes isikuandmete kaitse üldmääruse (IKÜM) artiklist 17 tulenev õigus olla unustatud. Andmete tutvumise õiguse kõrval on õigus olla unustatud enim kasutatud õigustest.

Andmekaitse Inspektsiooni 2025. aastal läbi viidud seire keskendus küsimusele, kuidas suuremad jaekaebandus- ja tanklaketid tagavad õiguse olla unustatud püsikliendiprogrammide raames. Kuna populaarsemates püsikliendiprogrammides töödeldakse tuhandete klientide isikuandmeid, on äärmiselt oluline, et andmesubjekti õiguste tagamiseks on ettevõttesiseselt olemas selge raamistik. Seiresse kaasati sel korral 12 Eestis tegutsevat jaekaubandus- ja tanklaettevõtet.

Seire tulemusena tuvastasime mõned kitsaskohad õiguse olla unustatud tagamisel. Samas tuli esile ka mitmeid häid praktikaid, mis andmetöötlejal seda õigust tõhusamalt tagada aitavad.

Ühe suurema kitsaskohana saab esile tuua andmetöötlejate äärmiselt erineva detailsusastmega paika seatud mehhanismid andmesubjekti õiguse olla unustatud tagamiseks. Mõni ettevõte on välja töötanud üksikasjalikud juhised tegutsemiseks olukorras, kus andmesubjekt esitab taotluse oma isikuandmete kustutamiseks, sealhulgas on ennetavalt arvestatud ka kõikvõimalike erandolukordadega, mille puhul on andmetöötlejal alus andmete kustutamisest keelduda ning isikuandmete töötlemist jätkata. Samas leidus ka ettevõtteid, kes ei ole vastavaid juhiseid kustutamistaotluste käsitlemiseks välja töötanud ega taganud, et taotlusi käsitlevad töötajad läbiksid asjakohase koolituse. See probleem puudutab eeskätt väiksemaid andmetöötlejaid, kes on oma senises praktikas saanud vähe või mitte ühtegi IKÜM-i artikli 17 kohast taotlust.

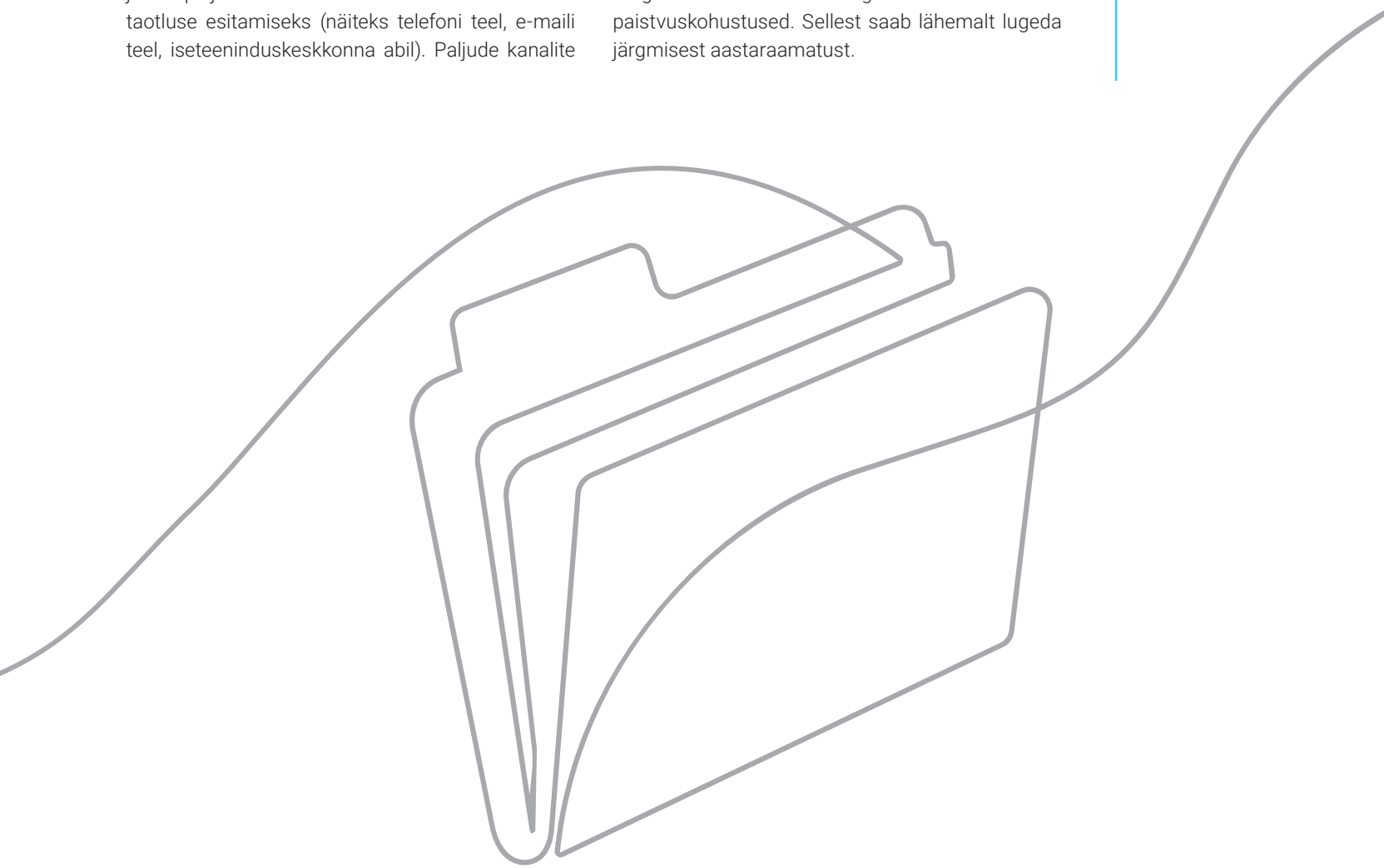
Teise suurema ja eelkirjeldatud probleemiga tihedalt seotud kitsaskohana saab esile tuua mitme ettevõtte puuduliku raamistiku tegutsemiseks IKÜM-i artikli 17 lõike 3 kohase erandi esinemisel. Puuduliku tegutsemisraamistiku põhjuseks on tõenäoliselt andmetöötlejate piiratud teadmised selle kohta, kuidas käituda olukorras, kus esineb õiguspärane põhjus andmete kustutamise taotluse rahuldamata jätmiseks. Nimelt väitsid paljud ettevõtted, et ei ole viimase kolme aasta jooksul keeldunud ühegi andmete kustutamise taotluse rahuldamisest. Samas tuli seiretulemustest välja, et jaekaubandus- ja tanklakettidel on mitu asjakohast alust, mis takistavad teatud juhtudel isikuandmete kohest kustutamist (näiteks raamatupidamisseadusest tulenevad nõuded ning õigusnõuete esitamise vajadus). Kui olu-

15

kordasid, mille puhul esineb IKÜM-i artikli 17 lõike 3 kohane alus selle rahuldamisest keeldumiseks, ei käsitleta keeldumistena või vastavaid taotlusi õiguspäraste taotlustena IKÜM-i artikli 17 mõttes, tekib oht, et andmesubjektile ei edastata tema taotluse suhtes võetud meetmete kohta nõutavat infot, mis toob kaasa tema õiguste rikkumise.

Vastukaaluks eelkirjeldatud probleemidele tuvastasime ka mitu head praktikat. Ühe näitena võib rõhutada mitme ettevõtte praktikat tagada andmesubjektile palju eri kanaleid isikuandmete kustutamise taotluse esitamiseks (näiteks telefoni teel, e-maili teel, iseteeninduskeskkonna abil). Paljude kanalite võimaldamine hõlbustab andmesubjektidel õiguse olla unustatud teostamist. Seejuures võimaldab mitu ettevõtet näiteks nõusolekul põhinevate isikuandmete automaatset kustutamist vastava tahteavalduse esitamisel iseteeninduskeskkonnas. Selline automatiseeritud isikuandmete kustutamine võimaldab lühendada aega, mis kulub taotlustele reageerimiseks, ning vältida käsitsi taotluste läbivaatamisega kaasnevat riski, et mõni taotlus jääb märkamata.

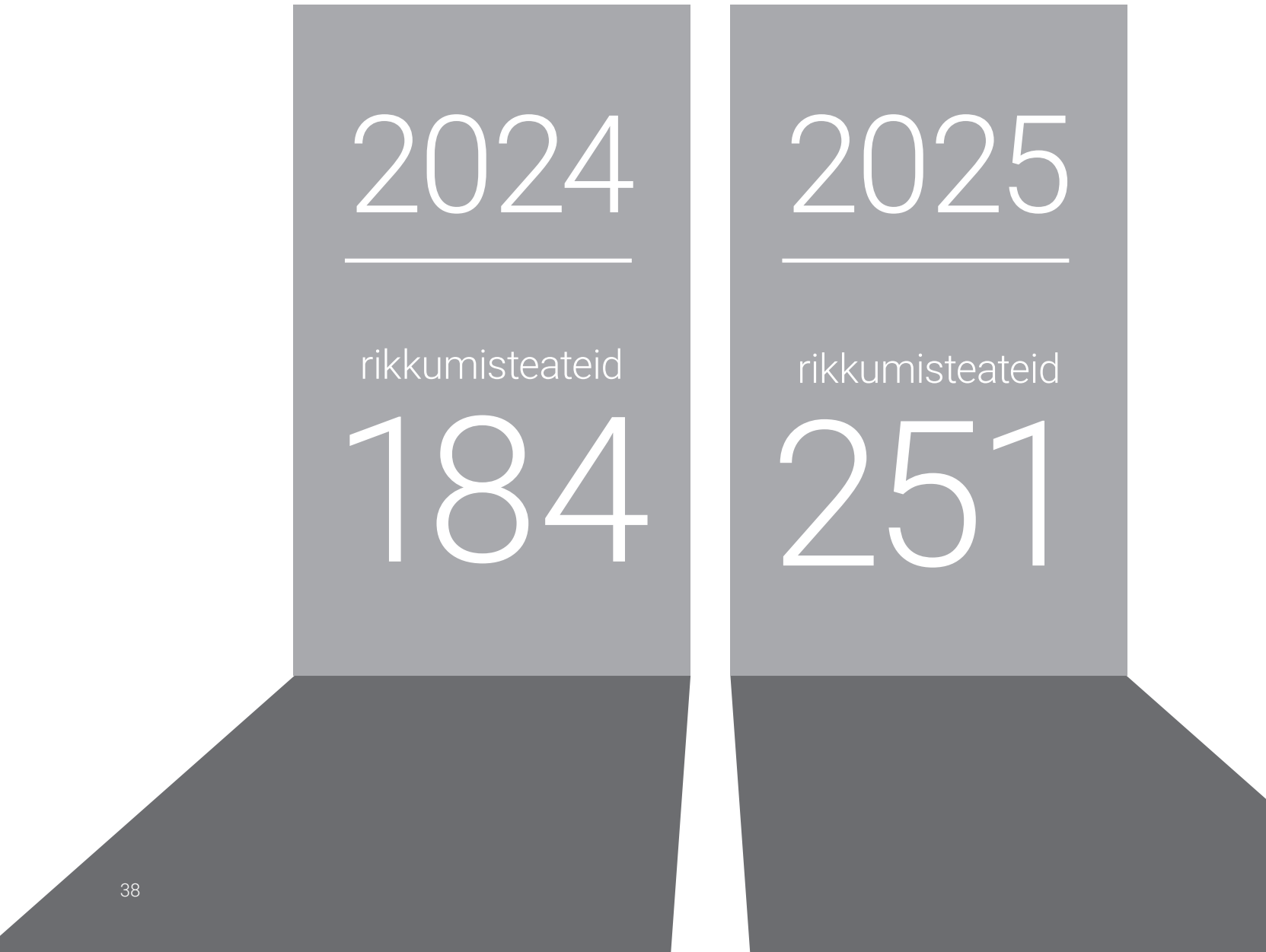
Järgmisel aastal on ühistegevuse keskmes läbipaistvuskohustused. Sellest saab lähemalt lugeda järgmisest aastaraamatust.



16 Rikkumisteated

Andmekaitse Inspektsioonile esitatud isikuandmetega seotud rikkumisteavitused annavad hea ülevaate sellest, milliste riskidega andmetöötlejad praktikas kokku puutuvad ning millised probleemikohad on püsivad. Rikkumisteated laekusid väga erinevatest valdkondadest ning hõlmasid nii üksikjuhtumeid kui ka väga suure mõjuga intsidente, kus puudutatud oli sadu tuhandeid inimesi.

2025. aastal oli edastatud teavituste arv alates 2018. maist seni suurim. Võrreldes 2024. aastaga oli kasv ca kolmandik - 184 teavitust 2024 vs 251 teavitust 2025.



16

Kõige sagedamini esines inimlikke eksimusi (nt valele adressaadile saatmine, andmete ekslik avaldamine). Sellele järgnesid hooletus ja tehnilised vead (sh süsteemide vale seadistamine, ebapiisavad kontrollmehhanismid). Eraldi grupi moodustasid õiguste väärkasutused ja turvanõrkused, sealhulgas küberintsidendid.

See kinnitab, et kuigi tehnoloogilised lahendused on olulised, on organisatsioonikultuuril, töötajate teadlikkusel ja ligipääsuhaldusel jätkuvalt suur roll.

Valdav osa rikkumisi puudutas üksikuid nn tavalisi isikuandmeid nagu inimese nimi, e-posti aadress või telefoninumber. Mitmel juhul olid ohus aga ka suuremad andmekogumid või potentsiaalselt tundlikud andmed. Sageli ilmneb, et rikkumised ei ole põhjustatud pahatahtlikkusest, vaid ebaadekvaatsest riskihindamisest, protsesside puudulikkusest või muudatuste (nt personali vahetus, IT-arendused) ebapiisavast juhtimisest.

Märkimisväärne on ka see, et mitu rikkumist avastati alles tagantjärele – kas kolmandate isikute teavituste, auditite või juhuslike avastuste käigus. See viitab vajadusele paremate seire- ja logimislahenduste järele.

Näiteks tuvastas IT-audiitor ühes riigi äriühingus, et ettevõtte eri infosüsteemide testandmebaasides on kasutusel töötajate pärisandmed.

Riigiasutus edastas seadistusvea tõttu teise asutuse andmekogu testkeskkonda andmeid, mis pidanuks jõudma päris andmekogusse.

Mitu andmeleket leidis aset eri majutusasutustes. Ühel juhul kasutas ründaja ära VPN-teenuse turvanõrkust. Teiste puhul oli põhjuseks turvanõrkus broneerimisteenust osutava ettevõtte infosüsteemis. Majutusasutuses broneeringu teinud inimestele hakati saatma õngitsuskirju, milles paluti broneeringu kehtivuse kinnitamiseks täiendavalt maksevahendi andmed sisestada.

Reisijavedu korraldava ettevõtte töötaja langes õngitsuskirja ohvriks, sisestades kirjas olnud petulingile enda tööprofiili sisselogimisandmed. Kuna ettevõttes oli kasutusel SSO (single sign-on), sai ründaja automaatselt juurdepääsu ettevõtte mitmele infosüsteemile.

Seda, et ka paberdokumentide kaitsmisel tuleb jätkuvalt hoolas olla, ilmestab järgmine näide. Haigla toidujagamiskärus oli tasku, kus hoiti paberkandjal patsientide toidunäidustusi koos põgusa terviseinfoga – kas patsient on näiteks vaegkuulja või motoorse häirega. Ühel patsiendil õnnestus see paber enda valdusesse saada ning ta tegi sellest telefoniga pildi.

Kokkuvõtvalt näitavad 2025. aasta rikkumisteated, et isikuandmete kaitse suurimad riskid ei tulene üksnes keerukatest küberohtudest, vaid sageli igapäevastest tööpraktikatest, inimlikest eksimustest ja puudulikest protsessidest. Tõhus andmekaitse eeldab lisaks tehnilistele meetmetele ka teadlikke töötajaid, läbimõeldud sisekordi ning pidevat järelevalvet. Andmekaitse Inspektsioonile esitatud rikkumisteated annavad väärtusliku sisendi ennetustegevuste kavandamisele ja andmetöötlejate teadlikkuse kasvatamisele.

17 Olulised kohtuasjad

Jõudsid lõpule SA Viljandi Haiglat (4-24-2034), SA Pere Sihtkapitali (4-24-2473) ja Asper Biogene OÜ-d (4-25-326) puudutavad väärteomenetlused. Kuigi kohtud lõpetasid kõik väärteoasjad[1], anti siiski mõned olulised seiskohad, millega saab edaspidi menetlustes arvestada.

Viljandi Haigla kaasuses tekkis põhimõtteline küsimus IKÜM-ist tuleneva vastutava töötleja kaasaaitamiskohustuse ja karistusõigusliku enese mittesüüstamise privileegi ulatusest. Kohus nõustus meiega, et siseriiklikud väärteomenetlust reguleerivad õigusnormid (koosmõjus VTMS §-ga 2, § 19 lõike 1 punktiga 4 ja KrMS § 34 lõikega 1 ja § 75 lõikega 2) on vastuolus otsekohalduva IKÜM-i artikli 31 ja artikli 58 lõike 1 punktidega a ja e ulatuses, milles need võimaldavad juriidilisest isikust menetlusalusel isikul jätta väärteomenetluses IKÜM-is sätestatud kaasaaitamiskohustus täitmata ning siseriiklikud normid tuleb jätta selles ulatuses kohaldamata. IKÜM-ist tulenev kaasaaitamiskohustus kehtib Eestis juriidiliste isikute puhul nii järelevalvemenetluses kui ka väärteomenetluses.

Väärtegude puhul, mis pandi toime enne 01.11.2023, ei ole võimalik juriidilisele isikule määrata rahatrahvi IKÜM-ist tuleneva rikkumise eest. Kohtud leidsid, et menetlusalusele isikule ei saanud olla mõistlikult ette nähtav, et EL-i õigusega pole kooskõlas kuni 31. oktoobrini 2023 kehtinud KarS § 14 regulatsioon[2]. Vastupidine käsitlus läheks vastuollu seaduse määratletuse põhimõttega ning tekkida võib olukord, kus menetlusalune isik võetakse tagasiulatuvalt vastutusele tingimustel, millistel ei oleks teda varem karistada saanud.

Kohus nõustus meie seisukohaga, et olukorras, kus andmekaitsespetsialistiks on ainuisikuline juhatuse liige, kes otsustab muu hulgas ettevõttes andmetöötluse eesmärgid ja vahendid, ei ole võimalik tagada andmekaitsespetsialisti sõltumatust, kuna tegemist on kahe rolli huvide konfliktiga.

Väärteomenetlusega seotult on 2026. aastal eelduslikult oodata kohtulahendit Allium UPI OÜ (4-25-3512)[3] kaasuses, kus on tekkinud mitu küsimust seoses väärteomenetluse, karistusõiguse ja IKÜM-i omavahelise koostoimimisega.

Seoses maksehäirete avaldamisega on jõustunud kaks ringkonnakohtu lahendit[4]. Ringkonnakohus leidis, et maksehäireregistril on esmajoones kohustus hinnata, kas krediidivõimelisuse hindamise eesmärk on konkreetse juhtumi asjaolusid arvestades kaalukam andmesubjekti huvidest ja õigustest. IKÜM-i artikli 21 lõikest 1 tuleneva kohustuse

[1] SA Viljandi Haigla osas lõpetati VTMS § 29 lg 1 p- i 5 alusel ehk aegumise tõttu, SA Pere Sihtkapital osas lõpetati VTMS § 29 lg 1 p 1 alusel ehk väärteotunnuste puudumise tõttu ja Asper Biogene OÜ osas lõpetati ühe väärteo puhul VTMS § 29 lg 1 p 1 alusel ja teise väärteo puhul VTMS § 30 lg 1 alusel ehk otstarbekuse kaalutlusel.

[2] Vt ka Riigikohtu 20.06.2024 otsus väärteoasjas nr 4-23-742.

[3] Apotheka kliendiandmete lekkega seotud väärteomenetlus, kus AKI määras ettevõttele rahatrahvi summas 3 miljonit eurot.

[4] nr 3-23-1168 ja nr 3-23-1839

17

täitmine ei saa olla üksnes formaalne. Kuigi oma „konkreetset olukorda“ saab kirjeldada ja tõendada üksnes andmesubjekt ise, peab vastutav töötleja andmesubjekti õiguste teostamisele kaasa aitama. Maksehäireregistril on kohustus kontrollida, et avaldatavad andmed oleksid seotud võlasuhte rikkumisega, kuid temalt ei saa nõuda otsustamist selle üle, milline tähendus või kaal peaks konkreetsetel andmetel olema isiku krediidivõimelisuse hindamisel. Andmesubjekti esialgne isikuandmete töötlemisest teavitamata jätmine ei too kaasa andmetöötleja tegevuse õigusvastasust andmete jätkuval avaldamisel. Samuti märkis kohus, et MKS-i § 10 alusel avaldamise ülemäärast kahjustamist hinnates tuleb välisriigis tekkinud nõuete puhul lähtuda Eesti õiguses ette nähtud aegumise sätetest.

Maksehäirete teemal on Riigikohtus menetluses kaks sarnast kaasust, mis puudutavad samuti IKÜM-i artikli 21 lõike 1 sisu ja selle kohaldamist. Artikli kirjutamise ajaks ei ole kohus veel otsuseid teinud ning neid on oodata 2026. aasta alguses.

2025. aastal on jõustunud ka kohtulahendid[5] kahes asjas seoses vangiregistri päevikukannetega. Tegime vanglale ettekirjutuse, kuid vangla ei olnud nõus seda täitma, mistõttu tuli meil protestiga halduskohtusse pöörduda. Vangid on vangiregistrist enda isikuandmete töötlemise kohta teavet soovinud. Vanglal on kohustus andmed väljastada, kui ei esine VangS § 52 lõikes 6 ja/või IKS-i § 24 lõikes 2 loetletud asjaolusid.[6]

Kohtud on olnud seisukohal, et VangS § 52 lõiget 6 ei saa tõlgendada selliselt, et see välistab kõigile kinnipeetavatele kõigi nende kohta vangiregistrisse kogutud andmete avaldamise julgeolekukaalutlusel või manipulatsioonide vältimiseks, sest see muudaks sisutuks VangS § 52 lõikes 4 sätestatud õiguse andmeid saada. Andmete avaldamisest keeldumine peab põhinema enamal kui üldsõnalisel viitel julgeolekuriskide ja vangistuse täideviimise ohustamisele. Samuti on kohtus leidnud kinnitust, et meil on õigus teha vangla üle haldusjärelevalvet ja vajadusel teha vanglale ettekirjutus viia isikuandmete töötlemine kooskõlla õigusaktis sätestatuga.

[5] nr 3-22-454 ja nr 3-21-2254

[6] Praegu kehtivas redaktsioonis VangS § 52 lg 7.

17

Ajakirjanduslikul eesmärgil isikuandmete avaldamine tekitab jätkuvalt palava diskussiooni. Jooksva aasta alguses jõustunud kohtuotsuses käsitles kohus isiku õigust olla unustatud, vastandades seda ajakirjandusvabadusele ja artikli ajaloolise väärtusele. Kohus leidis, et digiarhiivis isikute anonüümseks muutmisel ei ole tegemist „ajakirjandusvabadusse ega internetiarhiivide terviklikkusesse sekkumisega" ega ka artiklite „hilisema muutmisega", vaid tegemist on isiku eraelu kaitse eesmärgil toimuva teabele juurdepääsu tingimuste muutmisega. Arvestada tuleb sündmusest möödunud aega ja sellest tingitud avaliku huvi langust, aga ka tänapäeva infotehnoloogilisi lahendusi, mis võimaldavad kõikvõimalikku, sh tundlikku teavet lihtsasti leida ja seeläbi isiku eraelu puutumatust kahjustada. Veebiarhiivi anonümiseerimine muudab üksnes teabe kättesaadavuse määra, mitte ei „kustuta" teavet ajaloo tarbeks.

Lisaks rõhutas kohus, et ei oma määravat tähtsust, kas avaldatud teave ise käsitleb isiku eraelu, vaid hinnata tuleb seda, millist mõju avaldatud isikuandmed isiku eraelule avaldavad, sõltumata sellest, kas avaldatakse isiku kohta n-ö eraelulisi detaile või muud infot, nt infot isiku süüdimõistmise kohta.

Meil on pooleli veel mitu põhimõttelist kohtuvaidlust, milles on eeldatavasti lahendeid oodata 2026. aasta jooksul. Näitena võib tuua kohtuasja, kus vaidluse all on meie tegutsemise võimalused olukorras, kus siseriiklik õigusakt on vastuolus IKÜM-iga. Samuti saab näiteks tuua kohtuasja, kus kohtul tuleb kujundada seisukoht, kas isikuandmete kaitse asjas toimuva järelevalvemenetluse raames on meil võimalik üle minna AvTS-i nõuete täitmise kontrollimisele või mitte, olukorras, kus tegemist on olemuselt erinevate järelevalvemenetlustega.

Ringkonnakohtus on menetlusse võtmise otsustamisel meie apellatsioonkaebus halduskohtu otsusele, milles on võtmeküsimuseks asutusele esitatud dokumendi registreerija nime väljastamine teabenõude korras. Meie ei nõustu kohtu seisukohaga, et dokumendiregistris dokumente salvestanud isiku nime avaldamine on tingimusteta kohustuslik ning seda kohustust ei väära ka IKÜM või mõni teine õigusakt.

Ringkonnakohtu seisukohta on oodata ka isikuandmete töötlemise alust puudutavas vaidluses, kus andmetöötleja tugineb õigusliku aluse sisustamisel enda kui rahvaesindaja ja andmesubjekti kui ametniku rollidele, leides, et sellises olukorras ei kohaldu isikuandmete avalikustamisele IKÜM ega IKS ning et inspektsioonil järelevalvepädevus puudub. Esimese astme kohus ei nõustunud andmetöötleja seisukohaga, leides, et ametnikuks olemise fakt või ametiülesannete täitmine ei ole iseseisev õiguslik alus isikuandmete töötlemiseks. Lisaks on kohus rõhutanud, et Eestis ei ole Riigikogu liikmete tegevust, sh väljaspool ametiülesannete täitmist, inspektsiooni järelevalve alt välistatud.

17

18 Õigusloome tähelepanekud ja soovitused õigusloojatele 2026. aastaks

2025. aasta oli tihe aasta nii siseriiklikus õigusloomes kui ka Euroopa Liidu omas. Andmekaitse Inspektsioon esitas oma arvamuse 98 siseriiklikule seaduseelnõule ja Euroopa Liidu õigusakti ettepanekule. 2024. aastal oli samaks näitajaks 65, seega on meie kaasamine õigusloomeprotsessi kasvavas trendis.

See tõdemus toob meid ka esimese tähelepaneku juurde. Kuigi inspektsioon on üha enam õigusloomesse kaasatud, kui loodav õigusakt puudutab isikuandmete töötlemist, ei ole kõik õigusloojad endale siiski veel inspektsiooni kaasamise vajadust teadvustanud ja ei ole harvad olukorrad, kus meieni- jõuab info menetluses oleva olulise isikuandmete töötlemist puudutava õigusakti kohta alles siis, kui see on juba Riigikogu laual või hoopiski vastu võetud. Kui tahame olla täpsed, peaksime muidugi pigem rääkima meie kaasamise kohustusest, mis tuleneb otse IKÜM-i artikli 36 lõikest 4: see ütleb, et liikmesriik konsulteerib järelevalveasutusega, kui koostamisel on riigi parlamendis vastu võetava õigusliku meetme ettepanek või sellisel õiguslikul meetmel põhinev reguleeriv meede, mis seondub isikuandmete töötlemisega.

Tervitatav on, et üha enam on hakatud meid kaasama ka enne seda, kui eelnõu ametlikule kooskõlastamisele saadetakse. Kui oleme algusest peale protsessis kaasas, aitab see meil paremini aru saada loodava normi eesmärgist ja sisust ning anda mõistlikus ajaraamis parimat tagasisidet. Oluline on seejuures märkida, et kui meid ka kaasatakse normide väljatöötamise protsessis eri aruteludesse, ei asenda see seda, et eelnõu saadetakse ametlikult arvamuse saamiseks, kui eelnõu kooskõlastusringile läheb. Meie jaoks on oluline näha paberile pandud lõpptulemust, et saaksime veenduda, kas arutelude käigus on üksteisest õigesti aru saadud ja kas tulem peegeldab meie ettepanekuid.

Minnes siit edasi sisuliste küsimuste juurde, on alljärgnevalt välja toodud mõned tähelepanekud, mis on meie lauale jõudnud eelnõude peamised murekohad.

Eesmärk. Igasuguse isikuandmete töötlemise puhul on alati kõige olulisem esimese asjana sõnastada, mis on töötlemise eesmärk ehk vajadus, mis isikuandmete töötlemise tingib. Ikka veel näeme aeg-ajalt sõnastusi – õnneks küll kahaneval hulgal –, kus andmete töötlemise eesmärk on piltlikult öeldes töödelda andmeid.

Eesmärgi sõnastamisel tuleb silmas pidada ka seda, et see peab olema piisavalt selgelt piiritletud ja selle sisu üheselt mõistetav. Vastasel juhul on raske hinnata, kas seaduses nimetatud andmete töötlemine on eesmärgiga kooskõlas ja kas päriselt ei ole eesmärk saavutatav ilma nende andmete töötlemata.

18

Andmekogude osas tahaks veel eraldi rõhutada, et norm peab andma vastuse küsimusele, millisel eesmärgil ja milliste ülesannete täitmiseks on vaja andmekogu asutada. Näiteks „avaliku korra kaitsmine" andmekogus tehtava andmetöötluse eesmärgina on liiga lai, sest see ei anna vastust küsimusele, milliste ülesannete lihtsustamiseks on andmekogu vajalik.

Isikuandmete koosseis. Seaduses peab ammendavalt sätestama eesmärgi täitmiseks töödeldavate isikuandmete kategooriad, põhjendades seletuskirjas iga kategooria töötlemise vajadust. Andmekogude puhul ei pea seaduse tasandil üksikasjalikult loetlema kõiki isikuandmeid, kuid esitada tuleb isikuandmete kategooriad selliselt, et oleks võimalik aru saada, mis liiki andmeid kogutakse. Lisaks seadusele tuleb andmekogude puhul kehtestada ka põhimäärus ja see peab sisaldama andmekogusse kogutavate andmete täpset ammendavat loetelu. Näiteks ei saa põhimääruses kirja panna, et andmekogus sisalduvad „muud andmed", vaid kirja tuleb panna nende muude andmete loetelu.

Volitusnorm. Selge on see, et kõiki detaile ei ole alati kas võimalik või mõistlik (või mõlemat) seaduse tasandil sätestada ning nähakse ette volitusnorm täpsemaks reguleerimiseks, näiteks ministri määrusega. Sageli eksitakse volitusnormi sõnastamisel sellega, et norm ei kata kõike, mida hiljem täpsustada soovitakse. Kui seaduse säte ei anna näiteks ministrile selgesõnalist volitust reguleerida isikuandmete säilitustähtaegu (olukorras, kus seaduses on määratletud maksimaalne tähtaeg), siis ei ole ka ministri määrusega võimalik tähtaegu sätestada (vt ka järgmine lõik). Seega tuleb kogu andmetöötluse protsess paralleelselt õigusloomega läbi mõelda ja kõik see, mida soovitakse reguleerida madalama taseme õigusaktiga, täpselt seaduse volitusnormi kirja panna.

Säilitustähtajad. Isikandmete säilitamine kindlalt määratud tähtajaga – sealjuures arvestades, et andmeid ei tohi töödelda (sh säilitada) pikemalt kui eesmärgi täimiseks vajalik – on üks IKÜM-i (artikkel 5) isikuandmete töötlemise aluspõhimõte. Kuna alati ei ole seaduse tasandil võimalik täpset säilitustähtaega määrata, võib seadusesse kirja panna maksimaalse tähtaja ning seda küsimust detailsemalt reguleerida näiteks ministri määrusega, eeldusel, et seaduses on olemas selge volitusnorm (vt ka eelmine lõik). Kui andmete kustutamine toimub perioodiliselt, tuleb ära kirjeldada, milline on kustutamise protsess ja see peab alati toimuma maksimaalse tähtaja sees. Andmete kustutamata jätmine pärast tähtaja saabumist tähendab andmete edasist töötlemist, kuid seda juba ilma õigusliku aluseta. Seega juhul, kui andmete kustutamine toimub kindlaksmääratud perioodi jooksul (nt üks kord kuus või aastas), siis tuleb ka kustutamise tähtaega eraldi reguleerida.

18

Andmekogude osas tasub välja tuua veel paar täiendavat mõtet nende spetsiifikast tulenevalt.

1 Esiteks, kuna AvTS keelab samade andmete kogumise eri andmekogude põhiandmetena, tuleb välja tuua, mis on selle andmekogu unikaalsed põhiandmed ja millised andmed on saadud teistest andmekogudest. Sealjuures on oluline mainida, et kui samu andmeid kogutakse juba teise andmekogusse, tuleb need võtta sealt, mitte hakata looma nende kogumiseks uut paralleelset andmekogu. See omakorda tähendab, et põhimääruses tuleb selgelt ära reguleerida, millistest teistest andmekogudest (andmeandjad) milliseid andmeid saadakse (andmekoosseis).

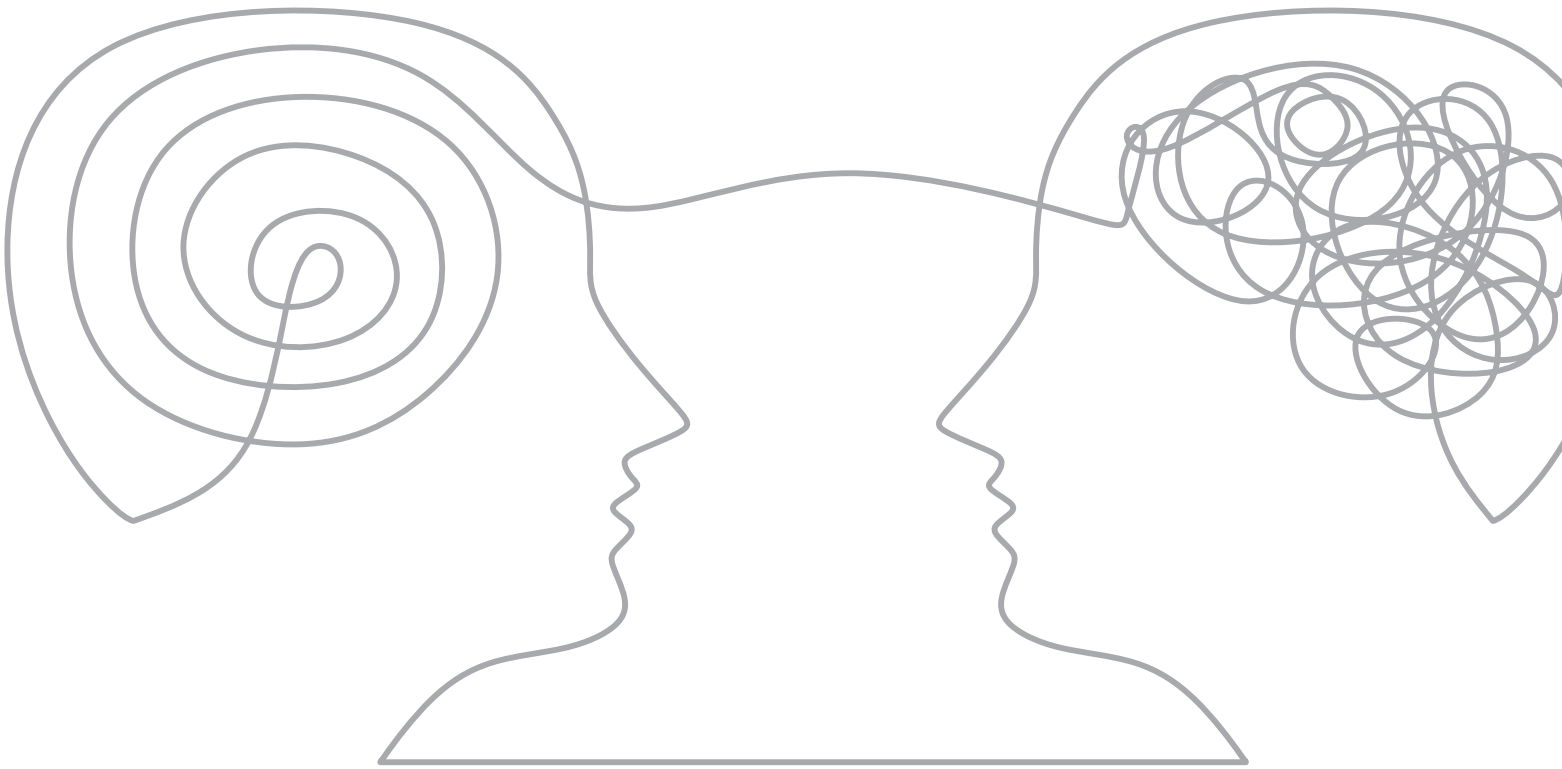
2 Teiseks, andmekogu põhimääruses peab kindlasti kirjas olema see, milline asutus millist rolli seoses andmekogu pidamisega täidab ning millised on tema rolliga seotud ülesanded. See tähendab, et tuleb kirjeldada, milliseid ülesandeid täidab andmekogu vastutav töötleja ja milliseid volitatud töötleja, kui ta on määratud (näiteks kes haldab kasutajaõigusi, kes vastab päringutele, kes arendab andmekogu jne). Siinjuures tuleb aga eristada IKÜM-ist tulenevat isikuandmete vastutava töötleja rolli ja AvTS-ist tulenevat vastutava töötleja ehk andmekogu haldaja rolli. Kui andmekogu kaudu täidavad seadusest tulenevat ülesannet mitu asutust, siis võib tegemist olla isikuandmete kaasvastutavate töötlejatega ning sellisel juhul tuleb isikuandmete kaasvastutavad töötlejad juba seaduse tasandil kindlaks määrata. Andmekogu põhimääruses tuleb sätestada, milliseid IKÜM-ist tulenevaid kohustusi milline kaasvastutav töötleja täidab. See on muu hulgas oluline nende ülesannete osas, mis puudutavad andmesubjektide õigusi ja nende teostamist (näiteks kes vastab IKÜM-i artiklis 15 kirjeldatud juurdepääsutaotlustele, kes teavitab vajadusel andmesubjekte andmelekkest jms).

3 Kolmandaks on meile silma jäänud, et tihti ei käi andmekogu arendamine käsikäes õigusloomega. Näiteks on 2025. aastast välja tuua juhtum, kus andmekogu varasemalt kehtivad sätted tühistati seoses uue andmekogu arendamisega, mis ei saanud aga tähtaegselt valmis. Kuna uut põhimäärust vastu ei võetud, toimus andmetöötlus edasi, sh andmevahetus teiste osapooltega, kuid mingil perioodil puudusid reeglid, kuidas ja millistel tingimustel andmevahetus toimub.

18

4 Neljandaks on täiesti omaette küsimus kõikide nende andmekogudega, mille põhimäärused on tehtud nii ammu, et need baseeruvad veel kunagi kehtinud andmekogude seadusel. Need põhimäärused ei ole tihti kooskõlas tänaste nõuetega, mis põhimäärustele ette on nähtud ja tuleks tegelikult andmekogu haldajatel uuendada.

Lõpetuseks toome välja veel üks markantse näite, kus just ühe sellise andmekoguga seotud muudatused jõudsid meie lauale, aga üllatuslikult ei olnud eelnõuga esialgu plaanis põhimääruses vananenud ja andmetöötluse tegelikkusele mittevastavaid sätteid muuta.



19

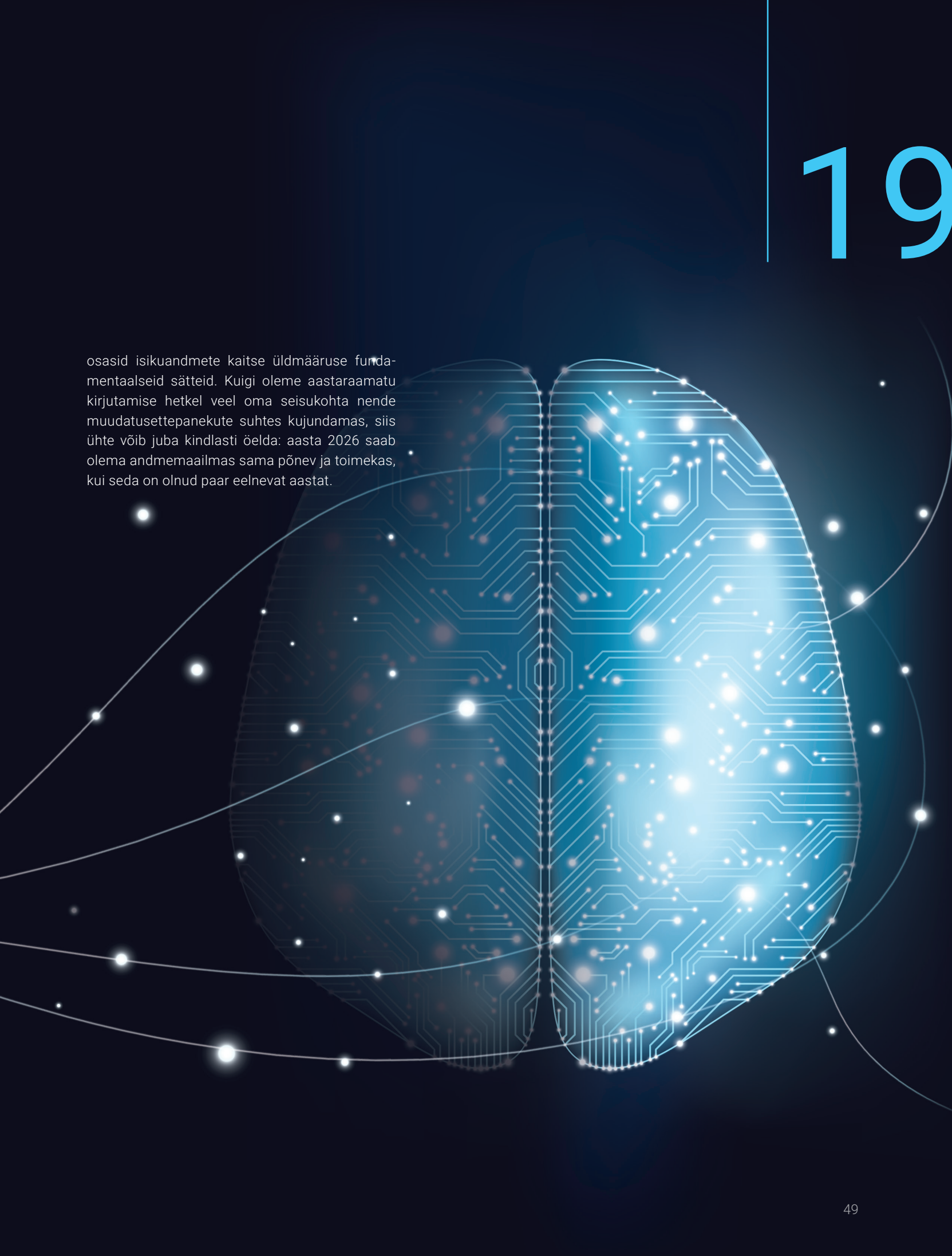
Privaatsust austava turvalise Euroopa andmemajanduse kujundamine

Andmed on tänapäeva majanduse vereringe, mis on oluline innovatsiooniks, konkurentsivõimeks ja parimate teenuste loomiseks pea igas sektoris. See, kui palju on meil praegu andmeid, milline on mahuline võimekus neid töödelda ja milleks kõigeks neid kasutada saab, oleks veel paar dekaadi tagasi kuulunud pigem ulmeklassika valdkonda. Andmeinnovatsiooniga käsikäes on käinud aga ka ohud, mis murendavad inimeste usaldust andmetöötlejate vastu – küberkurjategijad on pea sama nutikad kui parimad innovaatorid ja üksikisikul on juba pea võimatu pidada järge, kes, mida ja kui palju tema kohta teab ning mida selle alusel järeldada suudab. Seega peab andmetest suurima väärtuse loomiseks leidma tasakaalu, kus privaatsus ja innovatsioon käivad käsikäes, turvalisus on tagatud ja andmesubjektid teadlikud, kuidas nende andmeid töödeldakse. Üheks instrumendiks kõige eeltooduga tegelemiseks Euroopa Liidu tasandil oli õigusettepanekute pakett, mida tuntakse suure viisiku (big 5) nime all ning mis sisaldas endas (ettepanekute tegemise järjekorras) andmehalduse määrust, digiturgude määrust, digiteenuste määrust, tehisintellekti määrust ja andmemäärust. Praeguseks on kõik viidatud aktid läbinud edukalt Euroopa Liidu kaasotsustusmenetluse ning suurem osa neist ületanud ka rakendustähtaja finišijoone. Järgnevalt leiate lugemist nelja määruse kohta – eesmärgiks on aidata kaasa nende sisu ja mõju mõistmisele.

Lõpetuseks olgu mainitud, et Euroopa andmemajanduskeskkond ei ole veel kaugeltki valmis ja areneb tempokalt edasi. Selleks et kiiresti muutuva maailmaga sammu pidada, on Euroopa Komisjon eelmise aasta novembris tulnud välja digitaalse ja tehisintellekti omnibussi algatusega, mille eesmärgiks on ettevõtjate jaoks majanduskeskkonda lihtsustada ja innovatsiooni toetada. Muu hulgas on selle raames tehtud ettepanek muuta

19

osasid isikuandmete kaitse üldmääruse fundamentaalseid sätteid. Kuigi oleme aastaraamatu kirjutamise hetkel veel oma seisukohta nende muudatusettepanekute suhtes kujundamas, siis ühte võib juba kindlasti öelda: aasta 2026 saab olema andmemaailmas sama põnev ja toimekas, kui seda on olnud paar eelnevat aastat.



20 Digiteenuste määruse nõuete ja isikuandmete kaitse koosmõju

Üks õigusakt, mis kuulub hiljuti vastu võetud Euroopa Liidu andmealaste õigusaktide „suurde viisikusse“, on eelmisest aastast kohaldatav digiteenuste määrus. Digiteenuste määruse eesmärk on luua Euroopa Liidus tarbijatele ja ettevõtjatele turvalisem veebikeskkond. Selleks kehtestab määrus raamistiku ebaseadusliku sisuga võitlemiseks, andes kasutajatele suurema kontrolli selle üle, mida nad internetis näevad. Muu hulgas tagatakse kasutajatele võimalus ebaseaduslikku sisu (näiteks vihakõne ja desinformatsiooni) kergesti märgistada ning kehtestatakse kohustused seoses kauplejate jälgitavusega internetipõhistes kauplemiskohtades. Teatud olukordades võib digiteenuste määruse nõuete täitmine kaasa tuua ka vajaduse isikuandmeid töödelda. Sellisel juhul on vajalik täiendavalt arvesse võtta ka isikuandmete kaitse üldmäärusest (IKÜM) tulenevaid nõudeid. Euroopa Andmekaitsenõukogu (andmekaitsenõukogu) on digiteenuste määruse ning isikuandmete kaitse koosmõju käsitlenud 2025. septembris vastu võetud suunistes. Käesolevas artiklis avatakse olulisemaid suunistes käsitletud puutekohti, millele vahendusteenuste osutajad tähelepanu pöörama peaksid.

Ebaseadusliku sisu tuvastamine ja selle vastu meetmete võtmine

Digiteenuse määrus käsitleb vabatahtlikke meetmeid ebaseadusliku sisu tuvastamiseks. Andmekaitsenõukogu suunistes selgitatakse, et ebaseadusliku sisu tuvastamine ja sellega seonduvate meetmete võtmine võib hõlmata isikuandmete töötlemist. Igasuguseks isikuandmete töötlemiseks on vajalik aga IKÜM-i artikli 6 kohane õiguslik alus. Ebaseadusliku sisu modereerimise kontekstis võib olenevalt olukorrast sobivaks aluseks olla IKÜM-i artikli 6 lõike 1 punkt c või f.

Teavitus- ja meetmete võtmise mehhanismid ning ettevõttesisesed kaebuste menetlemise süsteemid

Digiteenuste määrus nõuab, et vahendusteenuse osutajad looksid süsteemid, mis võimaldaksid kasutajal lihtsal ja kasutajasõbralikul viisil teatada teenusekeskkonnas leiduvast ebaseaduslikust sisust. Teavituse esitajaid tuleb teavitada otsustest, mis on teates käsitletud teabega seoses tehtud. Digiplatvormidest vahendusteenuse pakkujad peavad lisaks tagama võimaluse sellised otsused ettevõttesisese kaebuste menetlemise süsteemi kaudu vaidlustada. Siinkohal on oluline silmas pidada võimalikult väheste andmete töötlemise põhimõtet ning koguda üksnes eelkirjeldatud toimingute jaoks vajalikke isikuandmeid. Teate esitaja isiku tuvastamine peaks olema nõutav üksnes juhul, kui see on vajalik, et teha kindlaks, kas teave kujutab endast ebaseaduslikku sisu. Lisaks on oluline tähele panna, et digiteenuste määruse kohaste kaebuste menetlemise süsteemide kasutuselevõtmine ei piira andmesubjektide IKÜM-ist tulenevaid õigusi digiplatvormide kui vastutavate töötlejate suhtes.

20

Kasutajaliides: petlikud kujundusmustrid, soovitussüsteemid, reklaamide läbipaistvus

Digiteenuste määrusega keelatakse petlike kujundusmustrite kasutamine, kuid erandina ei kohaldata seda tavadele, mis kuuluvad IKÜM-i kohaldamise alasse. Seetõttu on oluline analüüsida, kas kujundusmuster hõlmab isikuandmete töötlemist ja mõjutab andmesubjekti käitumist. Samuti keelatakse määruses eriliiki isikuandmete kasutamine profiilianalüüsil põhinevate reklaamide näitamiseks. Selline keeld täiendab IKÜM-i artikleid 9 ja 22, mis tähendab, et keeld kohaldub ka olukorras, kus vahendusteenuse osutajal võiks muul juhul olla IKÜM-ist tulenev õiguslik alus ning sobiv erand isikuandmete töötlemiseks. Sageli kasutatakse digiplatvormide kasutajaliideses ka isikuandmetel põhinevaid soovitussüsteeme, et kasutajale näidatava sisu järjekorda isikupärastada või kindlat sisu esile tõsta. Oluline on tähele panna, et sellise soovitussüsteemi kaudu sisu esitamine võib olla „otsus" IKÜM-i artikli 22 tähenduses siis, kui sellel on kasutajale märkimisväärne mõju. Kui pakutakse eri soovitussüsteeme, siis tuleks valikud esitada kasutajale neutraalselt, st kasutajat ei tohiks kallutada valima profiilianalüüsil põhinevat soovitussüsteemi.

Alaealiste kaitse

Digiteenuse määruses pööratakse eraldi tähelepanu ka alaealiste kaitsele. Määrus kohustab digiplatvormide pakkujaid kehtestama meetmeid, et tagada alaealistele kõrge kaitsetase, lisaks keelatakse alaealistele profiilianalüüsil põhineva reklaami esitamine. Andmekaitsenõukogu möönab oma suunistes, et digiteenuste määruse vastavad sätted võivad kvalifitseeruda isikuandmete töötlemise õiguslikuks aluseks IKÜM-i artikli 6 lõike 1 punkti c alusel. Selline töötlemine peab aga olema vajalik ning proportsionaalne, seejuures peab vastutav töötleja suutma tõendada nende tingimuste täitmist. Alaealiste kaitse vajadust tuleb tasakaalustada vajadusega kaitsta kõigi veebiplatvormide kasutajate eraelu puutumatust. Seetõttu tuleks vältida vanusekontrolli käigus kasutajate isiku täpset tuvastamist ning vanusekontrolli protsessi tulemusel kogutud andmete püsivat säilitamist.

Täpsema ülevaate saamiseks digiteenuste määruse ja IKÜM-i koostoime kohta soovitame tutvuda andmekaitsenõukogu suunistega.

[1] European Data Protection Board. Guidelines 3/2025 on the interplay between the DSA and the GDPR Version 1.1. Adopted on 11 September 2025.

[2] Tutvu ka Andmekaitsenõukogu suunistega 03/2022: Petuelemendid sotsiaalmeediaplatvormide kasutajaliidestes: kuidas neid ära tunda ja vältida. Versioon 2.0. Vastu võetud 14. veebruaril 2023. Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them | European Data Protection Board.

21 Euroopa Liidu digiandmeid reguleerivate õigusaktide ja isikuandmete kaitse koosmõju

Euroopa Liidu õigusruum on viimastel aastatel kiiresti kujunenud ühtseks ja mitmekihiliseks andmemajanduse raamistikuks. Kui isikuandmete kaitse üldmääruse (edaspidi IKÜM) rakendumine 2018. aastal tähistas murrangut andmekaitseõiguses, siis praeguseks on sellele lisandunud mitu uut õigusakti, mille eesmärk on kõikide digitaalsete andmete kasutamist ja haldamist reguleerida.

Selle artikli keskmeks on uutest õigusaktidest andmemäärus (Data Act, edaspidi DA) ja andmehalduse määrus (Data Governance Act, edaspidi DGA). Mõlemad õigusaktid mõjutavad ettevõtjate andmekäitlust ning loovad uusi kohustusi ja võimalusi, mis omakorda peavad olema kooskõlas isikuandmete kaitse üldpõhimõtetega. IKÜM on samal ajal oluliseks alusraamistikuks, millega uued õigusaktid horisontaalselt suhestuvad.

1 **Andmemäärus: õiglase andmete jagamise raamistik.** Andmemääruse peamine eesmärk on tagada õiglane juurdepääs andmetele ja nende jagamine digitaalses majanduses olukordades, kus andmed tekivad ühendatud seadmete või seotud teenuste kasutamisel. Määrus loob raamistiku, mis võimaldab andmesubjektidel (andmemääruse mõistes ka kui tarbija) kontrollida oma andmete kasutamist ja jagamist ning määrab andmevaldajatele selged kohustused andmete turvaliseks ja õiguspäraseks haldamiseks. Samuti toetab andmemäärus innovatsiooni ja konkurentsi, luues kindla ja läbipaistva aluse andmete jagamiseks kolmandate isikutega tarbija taotlusel. Määrus reguleerib lisaks (isiku)andmete jagamist avaliku sektori asutustega erakorralise vajaduse korral.

21

1.1

Kasutaja õigus ühendatud toote kasutamisel loodud andmetele. IKÜM reguleerib andmesubjekti juurdepääsu oma isikuandmetele. Andmemäärus reguleerib juurdepääsu ühendatud toodete kasutamisel loodud andmetele laiemalt, andes kasutajale võimaluse ligi pääseda ka isikustamata andmetele, mis on loodud kasutajaga seotud ühendatud toote või seotud teenuse kasutamisel. Selline juurdepääs andmetele peab kasutajal olema reaalajas või taotluse alusel masinloetaval kujul.

Ettevõtted peavad oma läbipaistvustingimustes juba enne ühendatud toote müüki või teenuselepingu sõlmimist selgelt teatama, milliseid andmeid on võimalik taotleda, et tagada kasutajale teadlik ligipääs oma andmetele.

Kasutajaks ei ole alati vaid tarbija. Näiteks võib tarbija kasutada ühendatud toodet rendilepingu alusel, kuid ühendatud toode ei kuulu talle. Sellisel juhul on kasutajaks nii tarbija kui ka toote omanik. Mõlemal kasutajal on õigus ühendatud toote kasutamise käigus tekkinud (isiku)andmetele.

1.2

Andmesubjekti õigus andmete jagamisele kolmandatele isikutele. Andmemääruse üks keskseid uuendusi on tarbija õigus nõuda oma andmete jagamist kolmandale isikule. Tarbija võib määrata, milliseid andmeid jagatakse ja kellele, ning andmevaldajal on kohustus need andmed kättesaadavaks teha. Selline jagamine kolmandale isikule toimub IKÜM-i mõistes nõusoleku alusel, kuna oluliseks faktoriks on tarbija taotlus andmete jagamiseks.

Jagatavad andmed peavad olema samaväärsed nendega, mida andmevaldaja jagaks otse tarbijale. Andmevaldaja saab andmed kolmandale isikule kättesaadavaks teha näiteks andmehalduse määruses reguleeritud turvalise andmevahendusplatvormi kaudu.

21

1.3 **Avaliku sektori vajadused ja erakorralised olukorrad.** Andmemäärus sätestab ka kohustuse jagada andmeid avaliku sektori asutustega vastava taotluse alusel erakorralise vajaduse korral, kui andmeid ei ole võimalik muul viisil õigel ajal ja tulemuslikult hankida. Määruse kohaselt peab selline erakorraline vajadus olema ajaliselt ja ulatuselt piiratud. Juhul, kui tegemist on eriolukorraga, on avaliku sektori asutusel õigus taotleda isikustatud andmeid. Ettevõtted peavad tagama, et selliste olukordade korral oleks loodud selged protsessid, mis võimaldavad isikuandmete turvalist ja kontrollitud edastamist, sealhulgas tehnilised ja korralduslikud meetmed, et tagada andmete terviklikkus, konfidentsiaalsus ja jälgitavus. Võimaluse korral tuleb isikuandmete edastamisel kohaldada kaitsemeetmeid, näiteks andmed pseudonüümida .

2 **Andmehalduse määrus: usalduse ja läbipaistvuse raamistik.** Andmehalduse määrus täiendab andmemäärust, luues mehhanismid andmete jagamise usaldusväärsuse suurendamiseks. Määrus reguleerib ettevõtjate poolelt andmete vahendajaid ja andmealtruismi organisatsioone ning avaliku sektori poolelt võimalust anda juurdepääsupiiranguga andmeid taaskasutamiseks.

2.1 **Andmevahendusteenuse osutajad ning andmealtruismi organisatsioonid.** Andmevahendusteenuse osutajad tegutsevad sõltumatute vahendajatena, kelle ülesanne on luua ettevõtjatele ja üksikisikutele usaldusväärsed ning turvalised andmete jagamise mehhanismid. Andmealtruismi organisatsioonid võimaldavad seevastu isikuandmete loovutamist näiteks nõusoleku alusel, eeskätt teadusuuringuteks, innovatsiooniks või avalike teenuste arendamiseks. Nõusoleku standardvormi kehtestab Euroopa Komisjon.

Isikuandmete kontekstis tähendab see, et andmete vahendamine ega altruistlik kasutamine ei tohi toimuda väljaspool IKÜM-i raamistikku ning isikuandmete töötlemisel peab andmetöötleja olema veendunud õigusliku aluse olemasolus.

2.2 **Avaliku sektori juurdepääsupiiranguga andmete taaskasutamine.** Andmehalduse määruse avaliku sektori andmete taaskasutamise regulatsioon kujutab endast sisulist täiendust avaandmete direktiivile. Kui avaandmete direktiivi eesmärk on tagada, et avaliku sektori valduses olevad juurdepääsupiiranguta andmed oleksid ühiskonnale võimalikult laialdaselt kättesaadavad, siis andmehalduse määrus laiendab seda lähenemist valdkondadesse, kus andmete täielik avalikustamine ei ole lubatud ärisaladuse, intellektuaalomandi kaitse, statistilise konfidentsiaalsuse või isikuandmete kaitse tõttu.

Andmehalduse määrus reguleerib piiratud juurdepääsuga andmestike kasutamise võimalust juhul, kui avaliku sektori asutus on selle andmestiku taaskasutamise tingimused ette näinud. Taaskasutaja võib taotleda, et avaliku sektori asutus annaks andmed taaskasutamiseks pseudonüümitud kujul, kui taaskasutaja on teinud IKÜM-i kohase mõjuhinnangu, konsulteerinud inspektsiooniga ning isikuandmete töötlemiseks on olemas õiguslik alus.

3 **Pilk tulevikku.** Digitaalsete õigusaktide rägastikus orienteerumine nõuab ettevõtjatelt olulist ressurssi. Selle lihtsustamiseks avaldas Euroopa Komisjon 19. novembril 2025 digitaalsete õigusaktide lihtsustamise ettepaneku, mis pakub välja muudatused muu hulgas andmemääruse, andmehalduse määruse ja isikuandmete kaitse üldmääruse muutmiseks.

[1] Alates 2019. aastast on lisandunud üle 100 digitaalsete andmete käsitlemist reguleeriva õigusakti. Andmemäärus, andmehalduse määrus ja digiteenuste määrus on omavahel tihedalt seotud.

[2] Pseudonüümimise kohta on Euroopa Kohus 04.09.2025 öelnud lahendis SRB vs EDPS, kui saaja ei oma ligipääsu lisateabele ega tehnilisi ega õiguslikke võimalusi isikuid taasidentifitseerida, võib pseudonüümne teave tema jaoks muutuda selliseks, et andmesubjekti ei peeta enam identifitseeritavaks (st tegemist oleks anonüümsete andmetega).

22 Andmekaitse ja konkurentsiõiguse põimumine digimaastikul: Isikuandmete kaitse üldmääruse ja Digiturgude määruse koosmõju suunised

2025. aastal kulmineerus Euroopa Andmekaitsenõukogu (EAKN) ja Euroopa Komisjoni ühine projekt Digiturgude määruse (DMA) ja Isikuandmete kaitse üldmääruse (IKÜM) koosmõju suuniste alal. Ühised suunised selgitavad, kuidas pääsuvalitsejad saavad DMA sätteid kooskõlas EL-i andmekaitseõigusega rakendada.

Suunised kirjutati algselt ainult EAKN-i siseselt selle konkurentsiõiguse ja tarbijakaitse õiguse alagrupis ja selle liikmete panustel, kuid kahe aasta jooksul ühines kirjutamisega Euroopa Komisjon. Suuniste kirjutamisse panustas ka Andmekaitse Inspektsioon. Kuna õigusakt puudutas üksikasjalikult nii andmekaitseõigust ja selle mõisted, mis on EAKN-i pädevuses, kui ka konkurentsiõigust, mis on Komisjoni pädevuses, otsustati, et ühiste koosmõju suuniste valmistamine, kus üksmeelt ja vastastikust mõistmist leitakse võimalikult vara, on õige tee.

DMA on eelkõige konkurentsiõiguse instrument, mille eesmärk on tagada Euroopa Liidu digisektoris konkurentsile avatud ja õiglased turud, millest saavad kasu füüsilistest või juriidilistest isikutest tavalised kasutajad (lõppkasutajad) ja ettevõtted, kes kasutavad digiplatvorme ärilistel eesmärkidel (ärikasutajad). DMA seab kohustusi suurtele tehnoloogiaettevõtetele, kes haldavad digiplatvorme ja pakuvad põhiplatvormiteenuseid nagu sotsiaalmeediateenused, veebibrauserid, sõnumiteenused, otsingumootorid ja muud veebipõhised teenused. Põhiplatvormiteenused on suurte kasutajaskondadega platvormid, mille kaudu pääsuvalitsejad on saanud digiturge oma huvides mõjutada.

Pääsuvalitsejate hulka kuulub näiteks selline ettevõtte nagu Meta, kes pakub muuhulgas põhiplatvormiteenuseid nagu sotsiaalmeediateenused (Facebook, Instagram), sõnumiteenuseid (Messenger, Whatsapp) ja internetireklaamteenused (Meta Ads). Teiselt poolt on pääsuvalitsejate hulgas ka ettevõtteid, kes pakuvad ainult ühte põhiplatvormiteenust – näiteks Booking.com, kes pakub ainult veebipõhist vahendusteenust (vahendusteenust majutuste leidmiseks).

Uued õigused ja kohustused

Uus määrus lisab kohustusi digihiiglastele ning pakub ka tarbijatele ehk lõppkasutajatele hulga uusi õiguseid, mis täiendavad nende IKÜM-ist tulenevaid õigusi. Üks olulisemaid sätteid DMA-s on artikli 5 lõige 2, mis keelab pääsuvalitsejal lõppkasutajate isikuandmetega teatud töötlemistoiminguid teha, sealhulgas:

- töödelda kolmandate isikute teenustelt saadud lõppkasutajate isikuandmeid reklaamide pakkumiseks;
- kombineerida isikuandmeid eri põhiplatvormiteenuste vahel või kolmandate isikute teenustelt saadud andmetega;
- ristkasutada põhiplatvormiteenuse kaudu saadud isikuandmeid muude teenuste puhul, mida pääsuvalitseja eraldi osutab;
- logida lõppkasutajaid automaatselt sisse pääsuvalitseja muudesse teenustesse, et isikuandmeid kombineerida.

22

Kohustus nendest toimingutest hoiduda aga ei kehti, kui kasutajale on antud selge valikuvõimalus ja ta annab oma nõusoleku, mis vastab IKÜM-i nõuetele (vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus). Suunistes täpsustatakse üksikasjalikumalt, kuidas pääsuvalitsejad peaksid neid elemente arvesse võtma, et IKÜM-ist tulenevaid nõudeid täita.

DMA on seadnud eesmärgiks tagada, et isikuandmete töötlemisest keeldumisel ei pea kasutajad siiski loobuma mõne teenuse kasutamisest. Kui lõppkasutaja keeldub oma isikuandmetega nimetatud toimingute tegemisest, peab pääsuvalitseja pakkuma oma platvormil vähem isikustatud, kuid samaväärset alternatiivi ilma, et teenus või selle funktsioonide kasutamine lõppkasutaja nõusolekust sõltuks. IKÜM-i vaatest on see hea eesmärk ja tervitatav areng, et teenuse kasutamise võimalus ja kvaliteet ei sõltuks isikuandmete töötlemisest.

DMA tutvustas ka uut õigust andmete ülekantavusele DMA alusel, mis on mõeldud täiendama IKÜM-ist tulenevat õigust andmete ülekantavusele. Selle kohustuse eesmärk on võimaldada lõppkasutajal tõhusalt platvorme vahetada või samal ajal mitut platvormi kasutada. Taotluse ülekantavusele võib teha nii lõppkasutaja kui ka tema volitatud kolmas isik selliste andmete kohta, mida kasutaja on esitanud või mis on loodud tema platvormi kasutamise tulemusena.

DMA täitmine

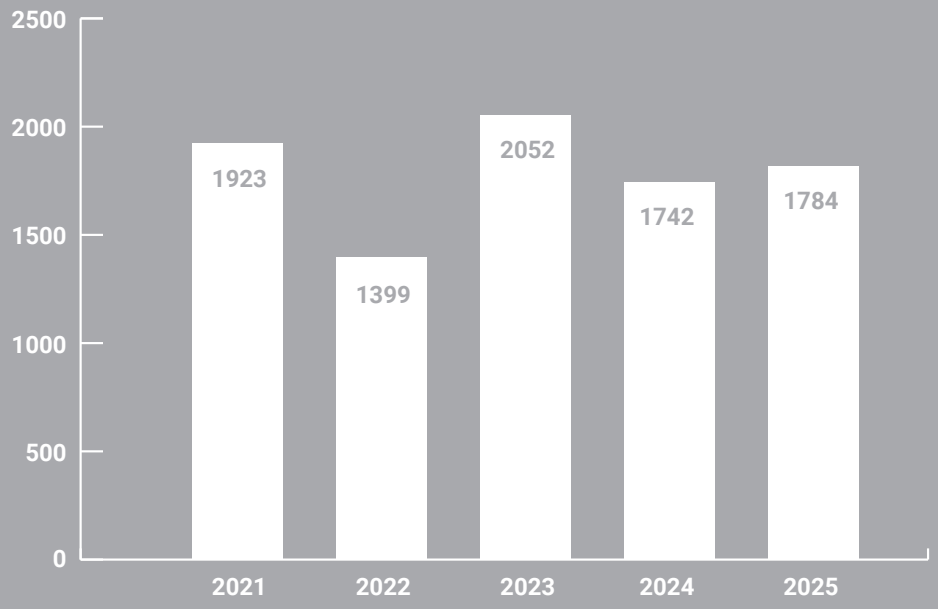
Komisjon on valvanud pääsuvalitsejate kohustuste täitmist põhiplatvormiteenustel ning 2025. aasta jooksul kuulutanud välja paar DMA täitmata jätmist käsitlevat otsust. Märkimisväärne otsus 2025. aprillist puudutab Meta nõustu-või-maksa-mudelit. Meta tutvustas 2024. aasta märtsis Facebookis ja Instagramis mudelit, kus kasutajad pidid kas andma nõusoleku oma isikuandmete kombineerimiseks isikupärastatud reklaamide pakkumise eesmärgil või maksma reklaamivaba teenuse eest tasu. Komisjon leidis, et sellise mudeliga ei pakkunud Meta lõppkasutajatele piisavat valikuvõimalust ning trahvis ettevõtet 200 miljoni euroga. Sarnase kriitilise hinnangu andis ka EAKN oma 2024. aprilli arvamuses, kus järeldas, et enamikul juhtudel ei ole suurtel digiplatvormidel võimalik kehtiva nõusoleku nõudeid täita, kui nad seavad kasutajad vaid kahe valiku ette: kas nõustuda isikuandmete töötlemisega käitumispõhise reklaami eesmärgil või maksta tasu.

Piisava valikuvõimaluse andmine on ettevõtetele kohustuslik nii IKÜM-i kui ka DMA kontekstis. Sarnased otsused näitavad, et lõppkokkuvõttes seistakse kahes asutuses sarnaste eesmärkide eest, kuid kasutades erinevaid õigusinstrumente.

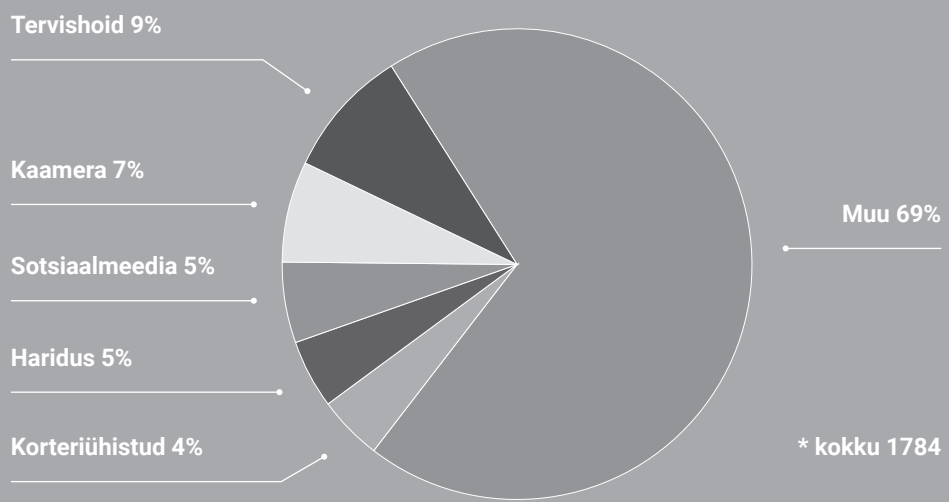
Need ühised suunised rajavad teed ka teistele koostööprojektidele andmekaitseasutuste ja komisjoni vahel tänapäeva õigusmaastikul, kus õigusvaldkonnad kattuvad aina tihemini. Andmekaitsenõukogu ja komisjon on hetkel välja töötamas ka ühiseid tehisintellekti määruse ja andmekaitseõiguse koosmõju suuniseid.

Tegevusnäitajad 2025

Selgitustaotlused, märgukirjad, nõudekirjad, teabenõuded, sh meediapäringute arv viie aasta võrdluses

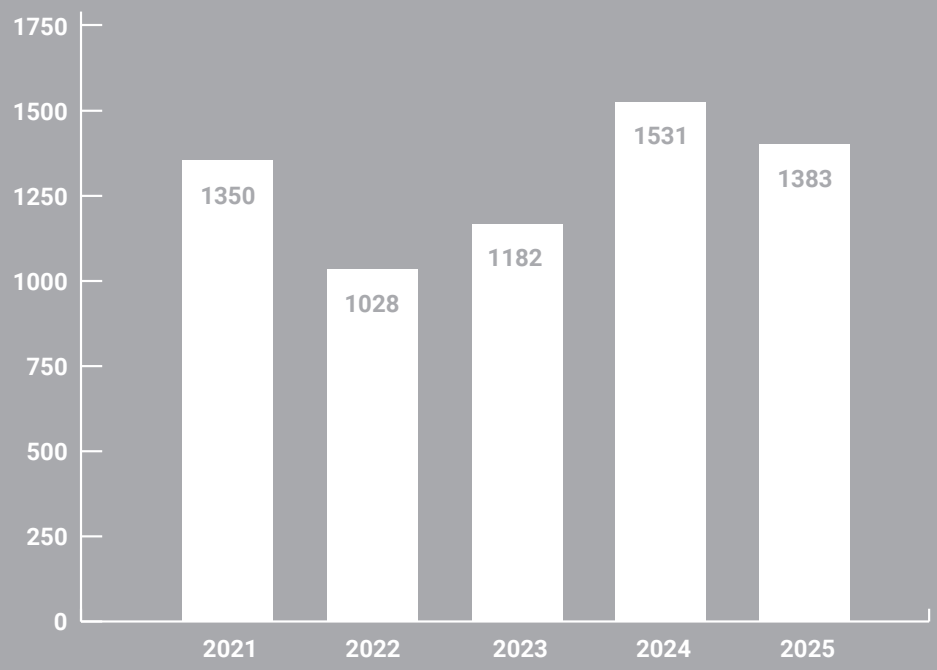


2025. aasta sissetulnud selgitustaotluste (selgitustaotlused, märgukirjad, nõudekirjad, teabenõuded, sh meediapäringute arv) sisuline jaotus

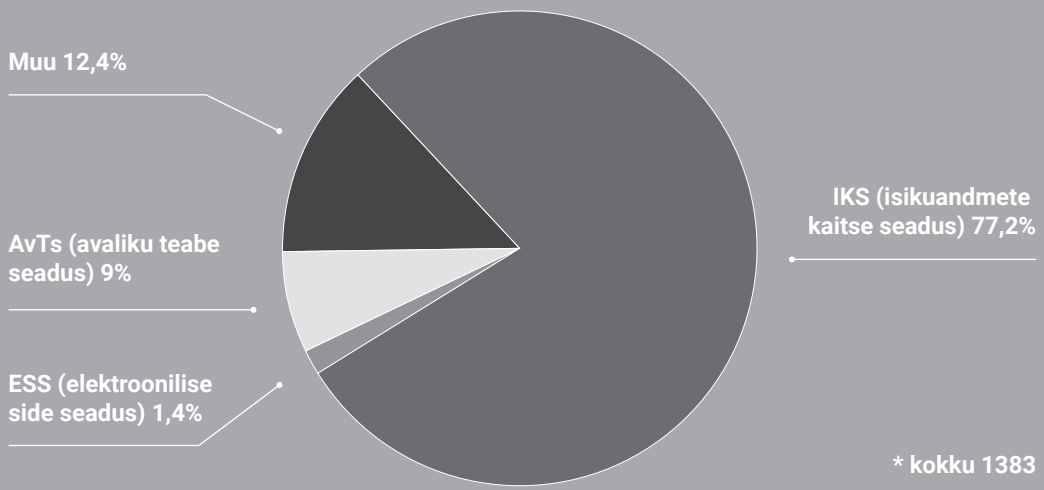


2025

Nõuandetelefonile tulnud kõned viie aasta võrdluses

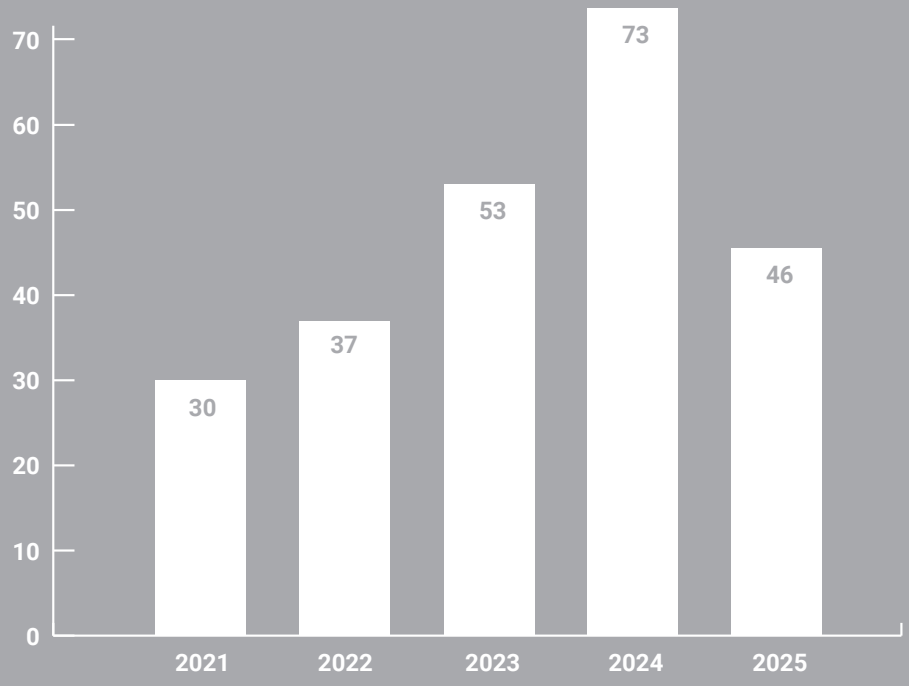


Nõuandetelefonile tulnud kõned

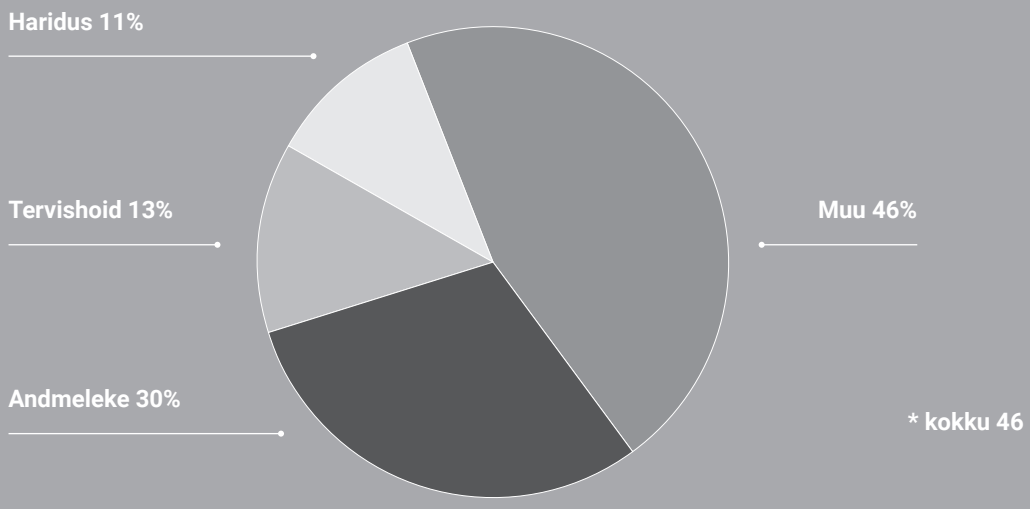


* kokku 1383

Omaalgatuslikud järelevalvemenetlused viie aasta võrdluses



2025. aasta omaalgatuslike järelevalvemenetluste valdkondlik jaotus

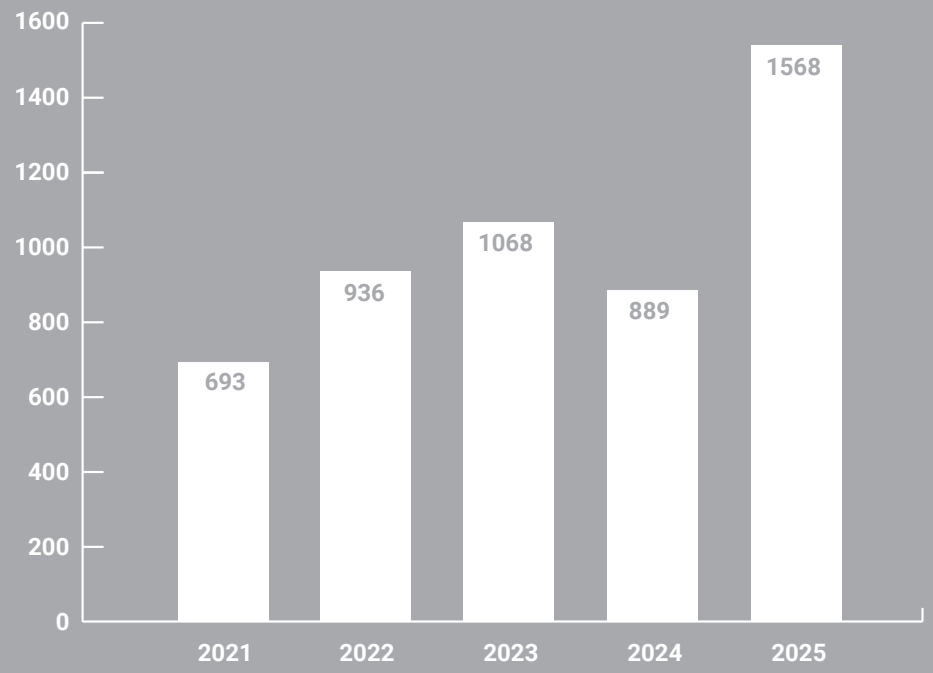


* kokku 46

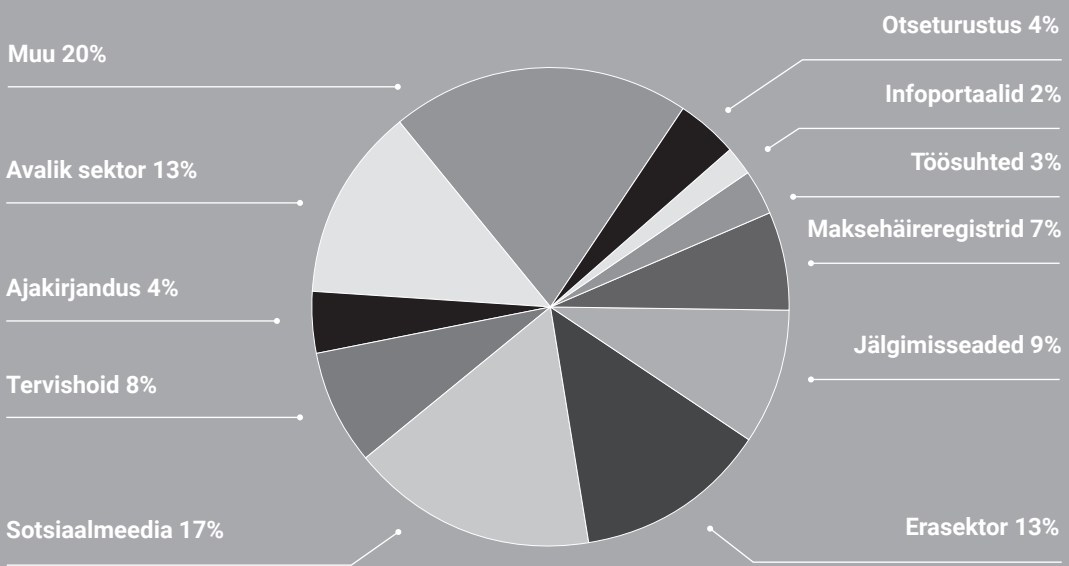
2025

2025

Kaebuste ja vaiete (sh AKI otsuste osas) arv viie aasta võrdluses

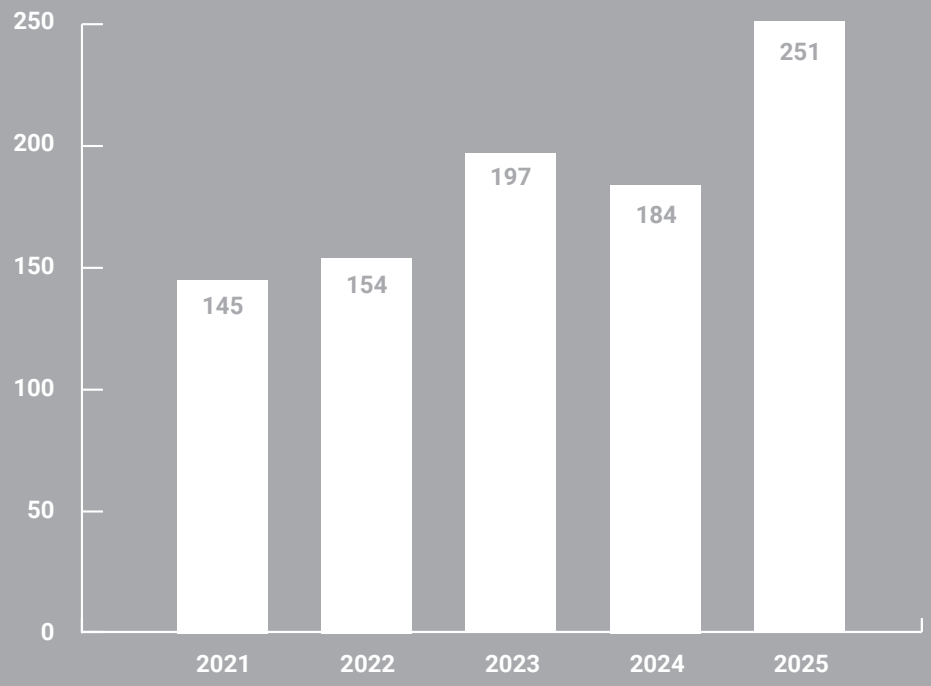


2025. aasta kaebuste sisuline jaotus

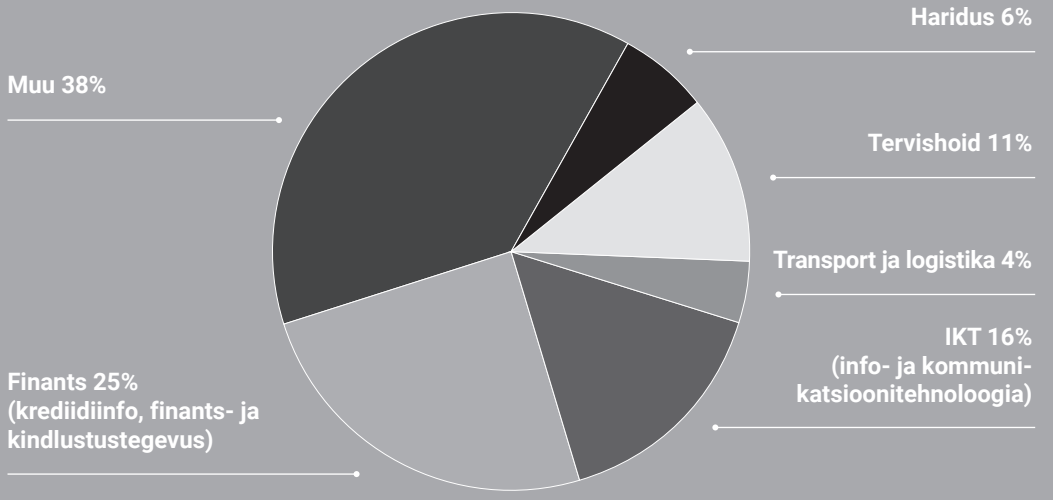


*** kokku 1380**

Rikkumisteadete arv viie aasta võrdluses



2025. aasta enim rikkumisteateid edastanud valdkondade jaotus



*** kokku 251**

Puudutatud isikute arv Eestis ja välismaal kokku 3 030 325

2025

2025. aasta järelevalve otsused arvudes

Kirjeldus	Arv
noomitus	**31**
tähelepanujuhtimine	**135**
ettepanekud	**74**
hoiatus	**4**
ettekirjutused	**13**
väärteomenetlused	**6**
määratud trahvid ja sissenõutud sunnirahad	**5**
määratud trahvid ja sissenõutud sunnirahad kokku summas	**3 088 100 €**

Noppeid numbrites

Oleme oma arvamust avaldanud 56 õigusakti eelnõu osas.

2025. aastal sai tegeletud 50 kohtuasjaga.

Oleme olnud Euroopa Andmekaitsenõukogu juhendiloome kaasautorid 3 korral.

Sellel aastal oleme produtseerinud 11 Andmehäälingu episoodi.

Sellel aastal oleme läbi viinud 58 koolitust ja nõustanud 74 korral.

Täname!

Aari Helmelaid
Agnes Järvela
Andra Kask
Andres Kudrjavtsev
Annika Kaljula
Eleri Karu
Elve Adamson
Geili Keppi
Grete-Liis Kalev
Irina Meldjuk
Jaana Sahk-Labi
Jekaterina Aader
Katrin Haug
Kirsika Kuutma
Kirsika Nigul
Liina Kroonberg
Maarja Kirss
Maire Iro
Mari-Liis Uprus
Mona-Reti Pavlov
Pille Lehis
Urmo Parm
Virve Lans

Toimetaja
Marilis Ehvert

Küljendus, illustratsioonid, trükk
Ain Kaldra, Andre Poolma, Iconprint OÜ

Fotod
Inga Mattiesen (Pille Lehis foto), Shutterstock, Iconprint

Andmekaitse Inspektsioon
2025