Aastaraamat

2023

Andmekaitse Inspektsioon

Sisukord

01 Peadirektori Pille Lehise eessõna

Tähtis aeg

Andmekaitse Inspektsioonil on sel aastal sünnipäev – täitub 25 aastat. Tegelikult on andmekaitse Eestis aga pisut vanem kui 25 aastat. Esimene isikuandmete kaitse seadus Eestis võeti vastu juba 1996. aastal ja osakond isikuandmete kaitsega tegelemiseks loodi Siseministeeriumisse aastal 1997. Iseseisva asutusena alustas Andmekaitse Inspektsioon aga tõesti tegutsemist aastal 1999, mistõttu me just 25. sünnipäeva sel aastal tähistame, ehkki tinglikult võiksime tähistada ka isikuandmete kaitse 27. aastapäeva.

Nii nagu tihti sünnipäevi – aga ka uue aasta saabumist – tähistatakse ilutulestiku ja mölluga, juhtus ka meiega. Seekord ei olnud aga möllu tellijaks meie ja meeliülendavast ilutulestikustki jäi asi kaugele. Selle suure mürtsu all pean silmas aastalõpu uudist sellest, kuidas suur hulk terviseandmeid võõrasse valdusse sattus.

Kuigi nagu öeldud, on isikuandmete kaitse Eesti õiguses teada juba aastast 1996, tuli see ikkagi paljudele üllatusena, mis võib olla tagajärg või kuidas saab inimest puudutada see, kui andmed piisavalt kaitstud pole. Ühelt poolt paneb see meid peeglisse vaatama, sest kõneleb see ju sellestki, et meie enda töö inimeste teadlikkuse tõstmisel on nõrgaks jäänud. Teisalt räägib see üllatus aga sellest, et vaatamata andmete kaitsmise vajadusest rääkimisele pole paljud seda tõsiselt võtnud.

Tõsi on ka see, et andmekaitse tundub paljudele keeruline, ja ei saa salata, et tihtilugu neist reeglitest arusaamine seda ongi. Kuna teema on mitmetahuline, pannakse vastutus ja otsustus paljuski andmete töötleja enda õlule ja talle ei ole abiks anda käsiraamatut, et tee nii või naa. Seetõttu jäävad avalikus ruumis andmekaitsest rääkides tihti kõlama teemad, mis tegelikult on meie vaatest teisejärgulised. Nii näiteks võib valele meiliaadressile saadetud e-kiri panna n-ö korralikus organisatsioonis käima tohutu protseduuride jada ja menetluse, kuid samas võivad olla täitmata andmete turvalisele hoidmisele seatud nõuded.

Andmekaitse kui andmetöötleja keskne ülesanne

Ajakirjanduseski saavad andmekaitsest rääkides suuri pealkirju pigem olümpiaaditulemuste avalikustamine, laste spordivõistluste tulemused, Facebooki postitused või sünnipäevaõnnitlused kohalikus lehes. Need teemad on lihtsad, neist rääkida ja nendega samastuda on lihtne. Kui aga hakata rääkima andmetöötleja kohustusest tagada andmete konfidentsiaalsus ja terviklus, töödelda andmeid minimaalselt ja kooskõlas eesmärgiga, tagades seejuures andmete õigsus, läheb juba keeruliseks.

Tavalisele inimesele ei ütle see lause mitte midagi. Küll aga ütles midagi detsembris avalikuks tulnud juhtum geeniandmete kurjategija kätte sattumisest.

01

Sel hetkel said inimesed aru – ma vähemalt loodan, et said – mida tähendab see, kui ka andmetöötlejad, kes peaksid olema professionaalid, ei mõista selle lause sisu.

Ühes hiljutises raadiosaates, kus analüüsiti sedasama teemat, öeldi väga hästi, et andmekaitse peab saama andmetöötlejate (olgu need siis eraettevõtjad või riigiasutus) keskseks ülesandeks. See tähendab, et andmekaitse ei ole midagi sellist, mis tuleb siis, kui äriprotsessid on kõik püsti pandud, vaid sellest tuleb alustada. Eriti kui tegeletakse erilliki ehk tundlike andmetega nagu terviseandmed. Kui äriprotsesse luues ei ole kohe andmekaitset keskseks ülesandeks seatud, vaid peetud seda üksnes tülikaks protseduuri- ja bürokraatiareegliks, võib see ühel päeval paraku ärile saatuslikuks saada.

Loodan, et kõnealune juhtum, aga mitte ainult, vaid ka meie selleaastane esimene juriidilisele isikule Ida-Tallinna Keskhaiglale määratud trahvivaidlus kohtus ja miks ka mitte ajakirjandusse jõudnud juhtum Tallinna Kiirabist paneb kõiki inimesi andmekaitsesse tõsisemalt suhtuma. Nii neid, kes selliste juhtumite tulemusel avalikuks saanud andmetest puudutatud said kui ka neid, kelle tegematajätmise või vääriti käitumise tulemusel andmete võõrale silmale nähtavaks saamine võimalikuks sai. Ehk aitasid need juhtumid mõista ka seda, et andmed ei ole abstraktne numbrite või tähtede rida, vaid nende taga on päris inimesed, oma päris elude ja tundliku infoga.

01

Kuna on sünnipäeva-aasta, ikkagi veerand sajandit, siis on paslik ka pisut tagasi vaadata. Isiklikult minu teadmised inspektsiooni ajaloost ei ole ülearu pikad – vaid 4 aastat, mistõttu saan ka üksnes neist rääkida. Selle võrra põnevam on lugeda eelmiste peadirektorite meenutusi ja nägemust sellest, kuhu inspektsioon peaks nende hinnangul lähiaastatel suunduma. Eriti huvitav on seejuures, et mõlemad näevad tulevikku täiesti erinevalt. Vaadates ise tagasi viimasele neljale aastale, siis mõlemad stsenaariumid on võimalikud – nii see, et inspektsioon lakkab iseseisva asutusena olemast ja ta liidetakse mõne teisega, et teenus oleks veelgi paremini tagatud, kui ka see, et inspektsioon on veelgi sõltumatum ja iseseisvam kui ta praegu on ehk väljaspool ministeeriumite haldusalasid. Küll aga räägivad need nägemused üht, ja sellega ka nõustun: see, mis on toonud meid siia, ei vii meid enam edasi.

Nii nagu eespool juba arutlesin, mida näitasid meile 2023. aasta lõpu sündmused ja juhtumid, ning kuidas inimesed samal ajal andmekaitset tajuvad ja sellest aru saavad, on selge, et andmekaitseküsimused koosmõjus tehnoloogia arenguga peavad veelgi rohkem fookusesse tõusma. Nagu üks partnerasutuski pidevalt rõhutab: küsimus ei ole mitte selles, kas organisatsioonide infosüsteeme ja andmekogusid rünnatakse, vaid millal see juhtub. Ja sealt edasi on küsimus, kui hästi selleks valmis ollakse ja andmekaitse olulisust mõistetakse. Seepärast on nüüd, 27 aastat pärast esimese isikuandmete kaitse seaduse väljaandmist, 25 aastat pärast Andmekaitse Inspektsiooni loomist ja 5 aastat pärast isikuandmete kaitse üldmääruse kehtima hakkamist, vaja ühiskonnas fookusesse tõsta andmekaitse teemad, mis ulatuvad kaugemale lahtise loeteludega e-kirjadest, laste joonistuste avaldamisest kooli veebilehel või naabritevahelistest tülidest valvekaamera üle.

Nagu ennist isegi ütlesin, on põhjust endalgi peeglisse vaadata, miks seda muutust pole nende aastatega suudetud ellu viia. On kõlanud ka etteheited, et järelevalve ei ole piisavalt tõhus. On ressursipuudus ja seadusandlus logiseb. Sel kõigel on kindlasti oma osa, aga ma ei poeks ei ühe ega teise taha.

Tugevam järelevalve vs ressursipuudus

Ressursipuudus näiteks on tõde. Kui isikuandmete kaitse üldmäärus 2018. aastal Euroopas kehtima hakkas, siis suurenes põhimõtteliselt kõigi Euroopa Liidu ja majandusühenduse riikide andmekaitseasutuste eelarve, kuna oli vaja värvata täiendavat tööjõudu. Eestis see aga nii polnud. Siin oleme me huvitava paradoksi ees – nimelt soovime ühelt

poolt õhukest riiki, st vähem ametnikke, kuid teisalt, kui aset leiavad suuremad kriisid, on ühiskond esimese asjana nõudmas tugevamat järelevalvet. Kahjuks need kaks asja koos ei käi.

Tõhusam ja tugevam järelevalve nõuab ressurssi, st inimesi, kes seda tööd teevad. Ametniku tööd ei saa AI veel üle võtta, uskuge mind. Ja kui ka mingil määral ühel päeval saaks, siis nõuavad sellised infotehnoloogilised lahendused esmalt väga palju raha. Seega ei saa me üle ega ümber sellest, et järelevalve on aeglane ja kallis. Sellepärast usun mina ennetusse ja teadlikkuse kasvatamisse. Ent see võtab aega. Kui kaua on võtnud aega see, et me enne sõitma asumist automaatselt autos turvavöö kinnitame? Mina mäletan veel aegu, kus see ei olnud norm. Ja mis seejuures kõige markantsem – et inimeste harjumust lõplikult muuta, pidid turule tulema autod, mis lihtsalt ei lase rahus sõita, kui turvavöö peal pole. Seega, nagu me sellest näitest õppinud oleme, on inimestes küll võimalik pikaajalise teavitustööga mõttelaadi muutust esile kutsuda, kuid lõpuks tuleb ikkagi pisut ka keeldude ja käskudega kaasa aidata.

Õigusloome pool

Siit jõuamegi teema juurde, millel ma küll pikalt peatuda ei tahaks, aga vaadates tagasi inspektsiooni ajaloole, on see keskne teema ja vajab põgusat äramärkimist. See on siis õigusloome pool. Saladus ei ole see, et neid üldmääruse kehtima hakkamisel kirgi kütnud hiigeltrahve pole Eestis tänaseni tulnud. Siin on tõesti puudujääk olnud meie enda siseriiklikus õiguses. Eespool mainisin, et aastasse 2023 jäi ka meie esimene juriidilisele isikule määratud väärteotrahv, täiesti arvestatavas suuruses – 200 000 eurot. Paraku on kohtuvaidlus selle õiguspärasuse üle kardetavasti fiaskoga lõppemas, mida üldmääruse ega ka kehtiva Euroopa Kohtu praktika kohaselt juhtuda ei tohiks. Tõe huvides olgu öeldud, et kohtuasi ei ole veel lõpuni jõudnud, viimaseid jõupingutusi on veel võimalik teha, kuid ma ei ole ülearu optimistlik. Milles siis mure?

Kohtulahend viidatud trahviasjas kirjeldab küll üksiksasjaliselt, kuidas haigla on andmekaitseliselt kõik tegemata jätnud ja eksimus isikuandmete töötlemisel eksisteeris, aga meie siseriiklik õigus lihtsalt ei võimalda haiglat süüdi mõista, sest sellist füüsilist isikut, kes peaks täitma täpselt samu norme, mida juriidiline isik, ja neid siis ka süüliselt rikkuma, pole võimalik tuvastada. Samas ütleb Euroopa Kohtu praktika, et sellise tulemuseni ei tohiks siseriiklik õigus viia. Nagu ma ütlesin, on veel väike lootus kohtust mingi õigusselgus saada, aga minu pessimism seisneb selles, et lisaks muudele puudujääkidele kehtib Eestis väärteoasjadele, sh andmekaitse asjadele ääretult lühike aegumistähtaeg ja kardan, et see saabub enne kui selgus kohtust.

01

Novembrist hakkas küll kehtima siseriiklik õigusmuudatus, mis võiks tekkinud frustratsioonile (st võimatus trahvida olukorras, kus rikkumine seda nõuab) pisut leevendust tuua. Kui aga trahvi temaatika kõrvale jätta, siis ka kõigis muudes olukordades on õigusloome meie töös kesksel kohal. Selged ja üheselt arusaadavad siseriiklikud normid on meie töös A ja O. Ja mitte ainult selged ja üheselt arusaadavad normid, vaid teatud juhtudel see, et need siseriiklikud normid üldse eksisteeriksid. Nimelt ei olda tihtipeale võib-olla aru saadud ka sellest, et isikuandmete kaitse üldmäärus on ikkagi paljudel juhtudel kõigest raamseadus, mis annab suuna, kuidas teha, kuid täpsed reeglid ja normid on liikmesriigi kätes.

Üsna tihti saame kriitika osaliseks, kui viitame mingis olukorras näiteks sellele, et selline tegevus nõuab siseriiklikku volitusnormi ja ilma selleta edasi minna ei saa. Siis kuuleme ikka ja jälle, kuidas andmekaitse takistab kiireid lahendusi, innovatsiooni ja mida kõike veel. Kuid lisaks andmekaitsereeglistikule peitub nõue, et meie eraelu puutumatust, mida just meie andmete kasutamine ongi, saab riivata üksnes seaduse alusel.

Pisut läbimõeldum ja läbipaistvam tegevus on see, mida riigilt selles olukorras oodatakse, ei muud. Seadusandja võiks õigusloome käigus selle tüütu andmekaitsega taaskord kokku puutudes mõelda, millist hüve selge ja läbipaistev andmetöötlus pakub ja kes on selliste normide adressaat. Seadused on ju inimestele, st meile kõigile ja igaühele meist, sõltumata hariduslikust taustast või ühiskondlikust positsioonist. Kõik need inimesed peavad aru saama, millal, miks ja kuidas riik tema andmeid töötleb ja hoiab.

Andmekaitse ja avaliku teabe kättesaadavus

Eks meie nimestki tulenevalt, aga ka viimaste aegade sündmustest tingituna, on nii meie töö fookus kui ka avalik tähelepanu inspektsioonile seotud peamiselt isikuandmete kaitsega, ent meil on ju ka n-ö teine pool. Teine pool tagab avaliku teabe kättesaadavuse. Paljudes Euroopa riikides ei ole need kaks rolli ühes asutuses ja põhjus on selles, et eks neil ongi pisut üksteisele vastanduv roll. Ühelt poolt teeme järelevalvet, et isikuandmed kaitstud oleks ja teisalt, et teave avalik oleks. Samas on neil kahel teemal ka palju kokkupuutepunkte – näiteks avaandmete temaatika ja andmekogud. Neid mõlemat reguleerib just avaliku teabe seadus. Mõlemad teemad on meil viimastel aastatel ka fookuses olnud ja mis seal salata, tekitanud mitmeid küsimusi. Riigi andmekogud, nende loomine ja järelevalve on ääretult oluline, sest riik ise on üks suuremaid andmetöötlejaid Eestis. Seega kõik see, mida ma ütlen andmetöötleja vastutuse ja teadlikkuse ning prioriteetide seadmise kohta, on mõeldud ka riigile.

Küll aga on siin veelgi olulisem õigusnormide läbipaistvus. Inimene, kes viimaste sündmuste valguses on nüüd ka ettevaatlikuks muutunud, peab saama vastused sellele, kuidas riik tema andmeid töötleb, just andmekogusid reguleerivatest õigusaktidest. Seepärast on ääretult oluline, et need oleksid lihtsas keeles, selged ja arusaadavad ega teeks sadu ristiviiteid eri normidele, kus isegi kõrgelt haritud juristid arusaamisega hätta jäävad, rääkimata muu eriala inimestest.

01

Lisaks andmekogudele on kindlasti oluline avaliku teabe valdkonnas edasi tegeleda juurdepääsupiirangutega. Ka siin on esmalt ääretult oluline teadlikkuse kasv, seda siis eelkõige ametnikkonna enda seas. Et iga ametnik, kes oma tööd teeb ja selle käigus dokumente loob, saaks aru, kas, millal ja millise juurdepääsupiirangu ta loodud teabele seab või seadmata jätab. Selline igaks juhuks piirangute seadmine peab lõppema. Küll aga peab siin kaasa tulema ka infotehnoloogia ehk siis dokumentide töötlemise ja haldamise programmid, mis peaksid tänapäeval võimaldama juba loomise käigus märkida, milline osa loodavast teabest on asutusesiseseks kasutamiseks ja milline mitte. Et ei oleks nii nagu praegu, et kui dokument sisaldab sellist teavet, siis on kogu dokument n-ö suletud ja üksnes teabenõudega välja nõutav, vaid et meil oleksid ikkagi kõik dokumendid avaldatud ja avalikud, lihtsalt juurdepääsupiiranguga osa ei ole nähtav.

Lõpetuseks, mida siis sünnipäevalapsele soovida?

Soovin, sõltumata sellest, kas inspektsioon on tulevikus eraldiseisev või kellegagi koos, suur või väike, et sünnipäevalapse enda soovid täituksid.

Andmekaitse Inspektsioon soovib, et isikuandmete kaitse roll ühiskonnas kasvaks ja et meie riik oleks läbipaistev, ja panustab sellesse nii palju, kui meie väike kollektiiv suudab.

Et meie inimesed oleksid teadlikud oma õigustest ja oskaksid ise enda õigusi kaitsta, esmajärjekorras ise nõudlik olles nende suhtes, kes nende andmeid töötlevad.

Et inimesed küsiksid õigeid küsimusi ja teeksid valikuid selle põhjal, kes nende andmetega vastutustundlikult ümber käivad.

Soovin, et meie kohtupraktika võtaks eeskuju Euroopa omast ja et meie inimesed tunneksid, et kui muud moodi enam ei saa, siis kohus mõistab õigust, ja õigusaktidest tulenevalt saab seda teha, lähtudes samadest printsiipidest nagu Euroopa teise riikide kohtud ja Euroopa Kohus. Soovin, et meie riik oleks läbipaistev, õigusnormid selged ja arusaadavad ning inimesed usaldaksid riiki – sealhulgas andmetöötluse valdkonnas. Seda usaldust saab läbi lihtsate ning selgete normide kontrollida.

Kõige lõpuks, nii nagu mitmel rahvusvahelisel andmekaitsekonverentsil on rõhutatud, soovin, et me mõistaksime, et andmekaitse, sellest arusaamine ja teadlikkuse kasvatamine meis kõigis ei ole ainult andmekaitseasutuse roll, vaid kõigi ülesanne – eriti aga kogu riigi ja tema asutuste ülesanne.

peadirektor

02

Viljar Peep

AKI peadirektor aastatel 2008 - 2018

Töötasin AKI-s 10 aastat. Arusaadavalt tundsin pärast lahkumist kõige enam puudust vanadest kolleegidest. AKI oli väike kompaktne meeskond, kus igaühel oli oma vastutusportfell. Formaalsetele juhtimistasanditele ja struktuuriüksustele eelistasime mitteformaalseid töörühmi ja isiklikku vastutust. Niivõrd paindlikku ja tõhusat hajusjuhtimise mudelit ja tugevat meeskonnatunnet ei ole ma enne ega pärast näinud.

Olen AKI-st 5 aastat eemal olnud ja loomulikult on mu visioon veidi kuhtunud. Aga usun, et aastaks 2035 on AKI-st saanud osa mõnest suuremast asutusest. Tehnoloogia ja õigus muutuvad üha keerukamaks. Väga väikeses asutuses on raske kõiki vajalikke kompetentse hoida ja arendada, eriti kui tuleb tegemist teha endast suuremate asutuste ja ettevõtetega nii Eestis kui Euroopas. Sellise ühendasutuse loomiseks on mitu võimalust, näiteks liita andmekaitse, tarbijakaitse ja konkurentsijärelevalve. Või siis viia andmekaitse ja avaliku teabe järelevalve riigi IT ja küberturbe osaks. Vajalikku sõltumatust saab tagada ka suuremas asutuses. EL-i õiguses ette nähtud andmekaitseasutuse sõltumatust ei ole ju seganud näiteks avaliku teabe ja andmekogude järelevalvega tegelemine. Loodan, et aastal 2035 on andmekaitse ja avaliku teabe alane proaktiivne töö suurema mahuga kui reaktiivne kaebuste ja kirjavahetusega tegelemine.

Kui tulin AKI-sse, oli asutuse maine päris kehv – meid teati peamiselt sünnipäevaõnnitluste ärakeelajana. Püüdsin vähendada kolleegide juriidilist ülemõtlemist, kaasata meie töösse oponente ja eksperte väljastpoolt (asutasime nõukoja) ning parandada teavitustööd. Seadsin eesmärgiks, et vähemalt 1/3 asutuse töömahust oleks proaktiivne (juhendiloome, võrgustikud, seired, auditid, ringkirjad jne). See oli pagana raske, sest töölaual kipub ikka domineerima see töövoog, kus on palju väikesi asju (kaebused, kirjad), millel on seadusega määratud tähtajalipik küljes. Mu teine viisaastak AKI-s läks EL-i andmekaitsereformi tähe all. Töömaht oli tohutu. Ise käisin Brüsselis kokku kolmes grupis (nii juhi, asejuhi kui eksperdi tasandil). Mäletan, et näiteks andmekaitse-ametnike juhise lõpphääletusele tuli eelnõu 43. versioon.

Foto: Postimees

Urmas Kukk

AKI peadirektor aastatel 2003 - 2008

03

Asudes Andmekaitse Inspektsiooni peadirektori ametisse, oli mul päris hea ettekujutus, millised on peamised kitsaskohad andmekaitse ja riikliku järelevalve vallas. Kõige olulisemaks ja suuremaks probleemiks oli enamiku suuremate (et mitte öelda kõigi) isikuandmete töötlejate seisukoht, et igasugune Euroopa Liidust tulnud nõue on „üks Euroopa Liidu värk, mis meie kohta ei käi". Teiseks suureks probleemiks oli ettevõtete ja asutuste suhtumine õigusnormi (seadusesse) selliselt, et õigusnormi ainuke eesmärk oli nende arvates takistada eesmärkide saavutamist väljakujunenud ja harjumuspärasel viisil. Sellest tulenevalt oli iga uue õigusnormi lisamisel kohustatud isikute esimeseks tegevuseks võimaluse otsimine lisatud õigusnormi mittetäitmiseks.

Tõele au andes ei puudutanud see kitsalt isikuandmete töötlejaid, vaid oli laialt levinud ja seda eriti avaliku võimu teostamisel. Selline suhtumine on säilinud tänini ja sellest ei ole vaba ka Andmekaitse Inspektsioon. Märksõnadeks on „haldusorgani piiramatu kaalutlusõigus" ja „nõustav järelevalve".

Kaalutlusõigus on muutunud bürokraatliku õpitud abituse (haldusorgani tegevus on suunatud esmajärjekorras nende õigusnormide otsimisele, miks oma ülesandeid ei pea täitma / ei saa täita) kilbiks.

Nõustamine ja (riiklik) järelevalve on siiski oma olemuselt nii erinevad, et nende vägisi kokku sobitamine ei anna head tulemust. Sisuliseks tulemuseks on see, et nõustava järelevalve puhul on õigusnormi täitmine soovituslik isegi juhul, kui rikkumise eest on ette nähtud sanktsioon. Kui isikuandmete töötleja tegevus on vastuolus kehtestatud nõuetega, siis järelikult on nõustamine olnud olematu või puudulik.

Loodan, et Andmekaitse Inspektsioon hakkab võimalikult kiiresti teostama järelevalvet Isikuandmete kaitse üldmääruse nõuete täitmise üle ka täidesaatva võimu ja riigiasutuste osas. Põhjendus, et riigiasutuse kohta esitatud kabust ei ole mõtet menetleda, sest trahvida nagunii ei saa, on intellektuaalselt huvitav, kuid ei aita kaasa isikuandmete töötleja suunamisele õiguspärasele käitumisele. Pigem annab see rikkujale AKI-poolse kinnituse, et õigusnormi täitmine ongi soovituslik. Ei ole vaja oodata aastani 2035, vaid sellega võib alustada juba täna.

Arvestades seda, et suurimad isikuandmete töötlejad on täidesaatev võim ja riigiasutused, võiks Andmekaitse Inspektsioon olla eraldiseisev asutus ning mitte asuda mõne ministeeriumi haldusalas. Kas see välistab täielikult Andmekaitse Inspektsiooni tegevuse mõjutamise täidesaatva võimu poolt, seda ei tea. Tasub kindlasti vaadata seda, kuidas kujunevad praegu põhiseaduslike institutsioonide eelarved. Aga mõjutusvõimalusi jääks kindlasti vähemaks.

04

Tähelepanekuid terviseandmete töötlemise osas

Kuigi tööandjad ei peaks töötajate terviseandmeid üldse töötlema, siis on mõned teemad siiski meile menetlustesse jõudnud. Nii jõudis meie lauale kaasus, milles üks suur Eestis tegutsev ettevõte pakkus töötajatele töötervishoiuteenuse raames lisaks ka eri lisateenuseid (nt kardioloog, psühholoog, vaktsineerimine jms). Tegemist on väga tänuväärse algatusega, mis näitab tööandja hoolivust oma töötajatesse. Küll aga tekkis probleem, kui ettevõte hakkas raviarvete kontrollimise eesmärgil töötervishoiuteenuse osutajalt küsima välja tabeleid, milles kajastus nimeliselt, kes ja millise teenuse on saanud. Seeläbi oli tööandjal täpne ülevaade, kes ja kui palju on käinud psühholoogi juures, kes lasi teha mingi vaktsiini jne.

Rõhutame, et terviseandmed on oma olemuselt kõige delikaatsemad andmed, mida tuleb kaitsta oluliselt hoolikamalt kui tavalisi isikuandmeid. Terviseandmed on isiku füüsilise ja vaimse tervisega seotud isikuandmed, sealhulgas tervishoiuteenuste osutamist käsitlevad andmed, mis annavad teavet tema tervisliku seisundi kohta. Seega kuulub terviseandmete alla mh ka informatsioon selle kohta, millist lisateenust pidas töötervishoiuarst töötajale vajalikuks. Näiteks kui arst on pidanud vajalikuks suunata töötaja tööpsühholoogi juurde, ei tähenda see kohe, et töötajal on probleemid vaimse tervisega, kuid loob eelarvamuse, et inimesel võib sellele kalduvus olla (potentsiaalne terviserisk).

Selguse mõttes on oluline välja tuua, et tööandjal on seaduse järgi üsna palju kohustusi seoses töötervishoiu ja tööohutuse eri nõuetega, mh on tööandjal kohustus suunata töötajad tööalasesse tervisekontrolli. Seaduse eesmärk ei ole aga anda tööandjale õigust saada infot töötajate terviseandmete kohta ja talle ei avaldata ka ühtegi töötajat puudutavat diagnoosi vm terviseandmeid. Töötervishoiu ja tööohutuse seadus näeb küll ette teatud juhud, millal tööandjal terviseandmete töötlemise õigus on, kuid need reguleerivad väga kitsalt konkreetseid olukordi ning neid ei saa tööandja omavoliliselt laiendada. Seega, saab tööandja töötervishoiuarstilt teada vaid selle, kas töötaja sobib või ei sobi töötama või sobib töötama teatud lisatingimustega (nt prillid) ning üldised soovitused, mida tööandja peaks parendama.

Menetluse käigus ilmnes, et tegemist on laialt levinud praktikaga, kus tööandjad küsivad ja töötervishoiuteenuse osutajad väljastavad küsitud andmeid eriarstile suunamise osas. Selle parktika muutmiseks on inspektsioonil plaanis teha töötervishoiuteenuse osutajatele ringkiri ning juhtida tähelepanu, milliseid andmeid ja mis ulatuses tohib välja anda.

Soovitus tööandjale – mõtle läbi, kuidas töötajale lisateenuseid pakkuda ilma selle kohta infot saamata. Näiteks lepi töötervishoiuteenuse osutajaga kokku, millises ulatuses võib töötajat eriarstile suunata.

Pane tähele! Terviseandmed on ka need andmed, mis konkreetset diagnoosi ei sisalda. Seega võib ka muu info muutuda terviseandmeteks ristviitamise teel muude andmetega, tehes seega avalikuks tervisliku seisundi või terviseriskid. Nt arsti ettepanek jälgida vererõhku ja toituda tervislikumalt loob eelduse, et isikul on südameprobleemide risk või soovitus minna psühholoogi juurde loob eelduse, et isikul on kalduvus vaimse tervise probleemidele.

04

Sama loogika on seotud ka joobe kontrollimisega, mis on samuti käsitletav terviseseisundina, olgu selleks siis alkoholi- või narkojoove või psühhotroopse aine mõju. Ka see teema tõusis nii mitmeski menetluses ja selgitustaotluses. Tööandjal on küll kohustus joobes töötaja töölt kõrvaldada, kuid ise ta seda kontrollida ei või, sh ka mitte sellise seadmega, mis promille ei näita. Kontrolli võib teostada ainult tervishoiuteenuse osutaja, kellel on seadusest tulenev saladuse hoidmise kohustus. Järelikult oleks võimalus, et tööandja saadab töötaja arsti või õe juurde kontrolli, kes saab teha otsuse töötaja tööle lubamise või töölt kõrvaldamise kohta. Ühtlasi on oluline juhtida tähelepanu, et tööandjal on oluline teada isiku töövõimet, mitte milline joove ja millises ulatuses on tuvastatud. Töövõimetu võib olla ka isik, kellel on mõni terviserike ja seda ei tuvasta ükski tööandjale käepärane masin.

04

Alkoholi kõrvale on paratamatult tekkinud järjest enam erinevaid muid aineid, mis võivad mõjutada töötajate töövõimekust. Seega ei tohiks tekkida olukorda, kus tööandjad hakkavad n-ö võidurelvastuma ehk kes saab võimalikult palju erinevaid joobetuvastamise vahendeid. Oluline ei olegi mitte joobe täpse liigi ja suuruse tuvastamine, vaid veendumine, kas töötaja saab töö tegemisega hakkama või mitte.

Soovitus tööandjale – kui mõni konkreetne töökoht eeldab igapäevast joobekontrolli (nt bussijuhid, tõstukijuhid jne), tuleb esmalt töökoha riskianalüüsis see vajadus kaardistada ning töötajad tervishoiuteenuse osutaja juurde saata või vastav meditsiinilise haridusega inimene asutusse kohapeale kutsuda.

Joovet ei tohi kontrollida ka siis, kui isik on sellega vabatahtlikult ise nõus, sest nõusolek peab olema antud vabatahtlikult, konkreetselt, teadlikult ja ühemõtteliselt. Töösuhetes on tööandja aga jõupositsioonil ning nõusoleku tegelikku vabatahtlikkust pole võimalik garanteerida. Ka selliseid menetlusi on inspektsiooni laualt läbi käinud, kus tööandja on töötajate terviseandmeid töödelnud, tuginedes töötajate vabatahtlikule nõusolekule, kuid töötajad ise seda tegelikult ei tunne ning kardavad töösuhte lõppemist, kui nad nõus pole.

AKI sõnumid tervishoiuteenuse osutajatele

1. Pea kinni oma ametisaladuse hoidmise kohustusest ja ära väljasta rohkem andmeid, kui seaduses on lubatud. Ükski säte ei kohusta sind tööandjale töötaja terviseandmeid väljastama suuremas ulatuses, kui on seaduses ette nähtud.

2. Pea meeles, et terviseandmed on ka need, mis esmapilgul seda ei tundu olevat (nt soovitus mõõta vererõhku), sest see viitab isiku potentsiaalsele terviseriskile.

3. Dokumenteeri kõik andmete töötlemised. Nt on ka kogemata tehtud päring tervise infosüsteemi rikkumine. Kaebuste korral aitab see tõendada sinu tegevust ja asjad laheneb kiiremini.

4. Soovituste ja nõu saamiseks pöördu Andmekaitse Inspektsiooni poole.

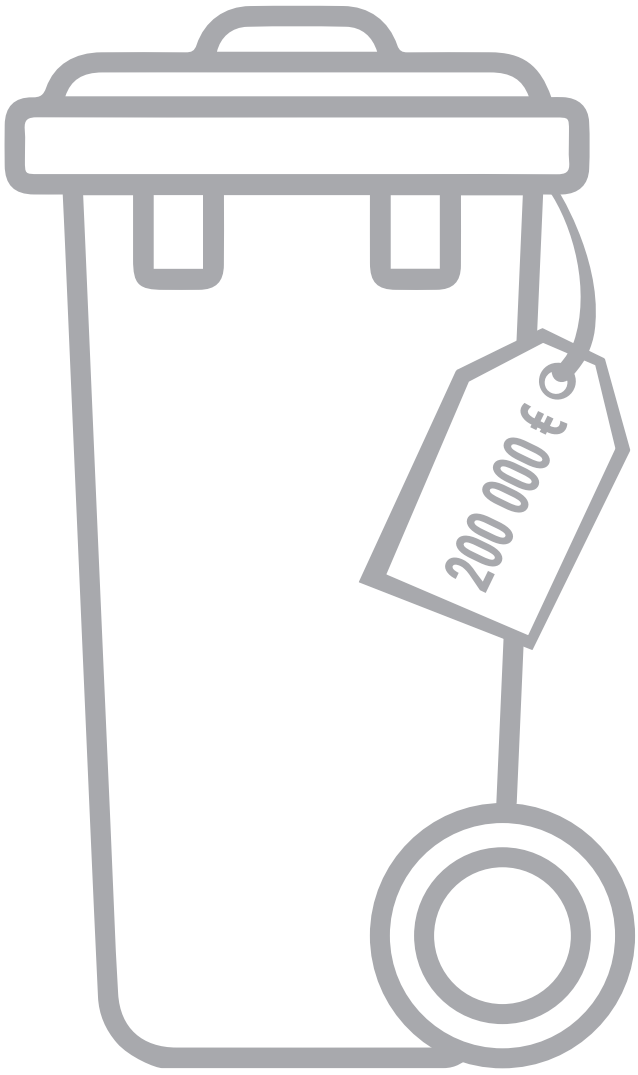
Muutused õigusruumis

05

2023. alguses määras AKI väärteotrahvi summas 200 000 eurot Ida-Tallinna Keskhaiglale (ITK) põhjusel, et patsientide hävitamisele suunatud tervise-andmeid ladustati Magdaleena polikliiniku peaukse kõrval pealt avatud ehitusjäätmete konteineris, mille väravad olid avatud ja konteiner oli järelevalveta. Iga möödakäija sai segamatult konteinerisse astuda, paberites sorida ja neid pildistada. Juhtum viitas isikuandmetega seotud protsesside läbimõtlematusele terves asutuses.

ITK vaidlustas väärteootsuse kohtus ning kohus leidis 2023. suve lõpul, et ITK tegevus isikuandmete töötlemisel oli kahetsusväärne, kuid väärteootsus ja trahv tuleb tühistada põhjusel, et karistusseadustik nõuab juriidilise isiku karistamiseks ka konkreetset füüsilist isikut, kes talle pandud kohustust on rikkunud.

Novembris 2023. jõustusid seadusemuudatused, mis selle juriidilise lünga kõrvaldavad ja edaspidi ei ole vaja juriidilise isiku tegevusetuse korral otsida enne karistamist füüsilist isikut.



06

Kasulikud soovitused

andmete turvaliseks töötlemiseks

Viimase aja paljude andmelekete ja isikuandmete kaitse alaste rikkumiste valguses on mõistlik tuletada meelde mõningaid lihtsaid, kuid olulisi soovitusi, kuidas igapäevatöös andmetega turvaliselt ümber käia. Küberrünnakud on paraku pigem millal- kui kas-küsimus. See ei tähenda aga, et me ei saaks võtta ennetavaid samme, et oma andmeid kaitsta ja kiirelt reageerida, kui midagi juhtuma peaks. Asutus, kes võtab tõsiselt turvameetmeid, ei suuda mitte ainult kaitsta oma andmeid, vaid on ka usaldusväärne partner ja eeskuju teistele.

1. **Andmete krüpteerimine ja pseudonümiseerimine.** Hoolitsege selle eest, et isikuandmetega tegelemisel kasutatakse tugevat krüpteerimist. Eriti tundlike andmete pikaajalisel säilitamisel võiks kaaluda pseudonümiseerimist, mis muudab isikute tuvastamise isegi andmelekke korral keerukamaks.

2. **Autentimine.** Kasutage süsteemides tugevaid paroolireegleid või vähemalt kaheastmelist autentimist, et raskendada volitamata ligipääsu oma süsteemidesse.

3. **Logimine ja avastamine.** Kasutage tõhusaid jälgimissüsteeme ja logisid süsteemis toimuvate tegevuste jälgimiseks, võimaldades avastada ebatavalist tegevust või päringuid.

4. **Intsidentidele reageerimise plaan.** Koostage mõistlik ja selge plaan reageerimiseks, kui isikuandmetega peaks midagi juhtuma. See on sama tähtis kui tulekahju korral evakuatsiooniplaan.

5. **Töötajate teadlikkuse tõstmine.** Korraldage regulaarseid koolitusi või teste, et töötajad tunneksid ära petuskeemid ja õngitsuskirjad ning mõistaksid, kui oluline on turvalisuse tagamine.

6. **Turvaauditid, testimised või auditid.** Viige läbi regulaarseid teste ja auditeid, et tuvastada võimalikke puudusi süsteemides ning tagada, et turvameetmed vastavad kõrgetele standarditele.

7. **Andmekaitsespetsialisti kaasamine.** Kaasake andmekaitsespetsialist juba varakult andmeturbe küsimuste lahendamisse, pakkudes talle regulaarselt ülevaateid andmeturbe seisust.

8. **Standardi rakendamine.** Rakendage tunnustatud standardeid, näiteks Eesti infoturbestandardit või ISO 27001, et hinnata riske ja valida sobivaid meetmeid riskide maandamiseks.

9. **Dokumenteerimine ja reguleerimine.** Dokumenteerige kõik rakendatud meetmed, intsidentide juhised ja arendused, tagamaks töö sujuvat jätkumist ka oluliste inimeste vahetumise korral. Juhul kui kasutate andmeturbe tagamiseks mõnda teist ettevõtet volitatud töötlejana, sõlmige põhjalikud kokkulepped ja veenduge, et tagatud on just teie süsteemidele sobivad turvanõuded.

07

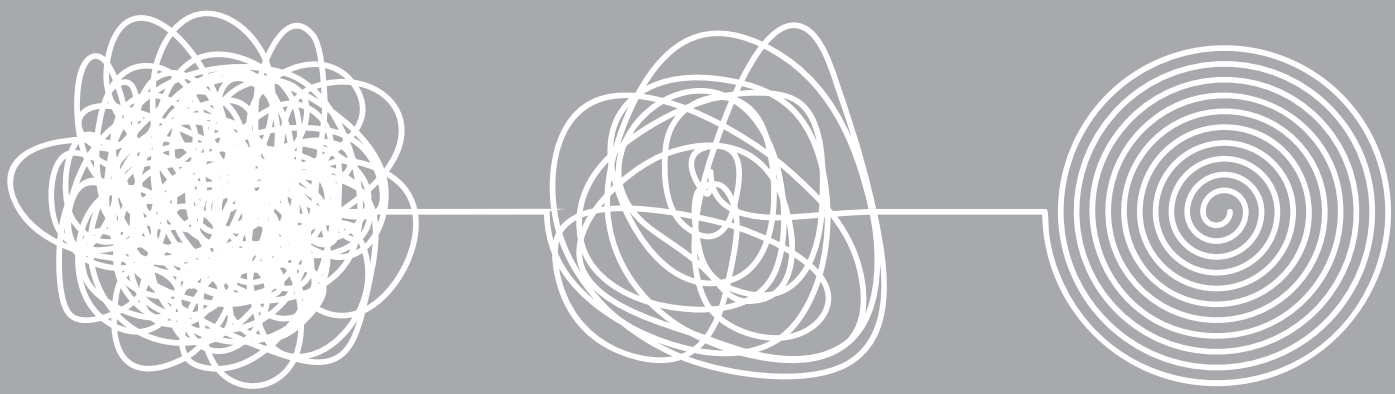
Probleemkohad avaliku teabe seaduse täitmisel

Avaliku teabe seadus (AvTS) pärineb aastast 2000 ja on kirjutatud pidades silmas eelkõige asjaajamist paberil. Seetõttu on paljud AvTS-i nõuded täitmiseks väga ajamahukad või suisa võimatud. Näiteks võib tuua § 42 nõude, et juurdepääsupiirangu kehtetuks tunnistamise kohta tehakse märge dokumendile – tänaseks on enamik dokumente digitaalsel kujul ja ka digitaalselt allkirjastatud ning neile ei saa seetõttu lihtsa vaevaga mingit märget lisada ilma, et algsest dokumendist kujuneks uus versioon.

Lisaks on juurdepääsupiirangu seadmise aluseid hulgaliselt ja nii mõnedki neist tekitavad peavalu otsustamaks, kas on alust juurdepääsupiirang seada või mitte, näiteks § 35 lg 1 p 12, mis kohustab kaitsma teavet, mis sisaldab isikuandmeid, mille avalikuks tulek kahjustaks oluliselt eraelupuutumatust. Mille alusel aga otsustada, kas kahjustab oluliselt? Kardetavasti kulub igal haldusorganil aastas selle punkti hindamise peale vähemalt ühe töötaja täistööaeg.

Aeg oleks teha oluline samm ja arendada välja dokumendihaldussüsteem, kus juba dokumendi loomise käigus märgistab selle kirjutaja juurdepääsupiiranguga osa dokumendist ning ülejäänud osa dokumendist läheb automaatselt avalikuks. See vähendaks oluliselt teabe otsijate vaeva ja säästaks asutusi teabenõuetele vastamisest.

Justiitsministeerium on hakanud AvTS-i muutmise vajadust analüüsima ja kogunud juba ka teiste ministeeriumite sisendit muudatusteks. AKI on arvamusel, et üle oleks vaja vaadata seaduse kogu kontseptsioon.



2000 2023 ...

08

Levinud

müüdid ja legendid

andmekaitses

1 Isikuandmed on kõik andmed, mis on seotud füüsilise isikuga.

Mitte alati. Isikuandmed on kõik andmed üksikuna või kogumis, mille kaudu füüsiline inimene on otseselt või kaudselt äratuntav, näiteks nimi, isikukood, asukohateave. Oluline on rõhutada, et ka isikukood on tavaline isikuanne ja selle kasutamisele ei ole seatud rohkem piiranguid kui inimese nime või sünniaja kasutamisele.

Jätkuvalt aetakse aga segamini isikuandmeid ja teisi andmeid. Isikuandmed ei ole andmed, mis käivad loomade, aga näiteks ka liiklusvahendite, ehitiste või muude asjade kohta. Lisaks ei ole isikuandmed ka andmed, mis puudutavad juriidilise isiku nime, vormi ja kontaktandmeid. Samas on isikuandmed kõigi äriühingutega seotud füüsiliste isikute andmed (nt nimi, isikukood, sünniaeg). Siiski peab meeles pidama, et kuna juriidilised isikud saavad tegutseda vaid füüsiliste isikute kaudu ning sel määral, mil füüsiliste isikute tegevus kvalifitseerub juriidilise isiku tegevuse alla, ei kuulu see isikuandmete kaitse üldmääruse kohaldamisalasse.

Inspektsioonil oli aastaid tagasi menetlus, kus teabevaldaja keeldus teabenõude täitmisest, sest tema hinnangul sisaldasid hobuste põlvnemist kinnitavad geneetilised ekspertiisid eriliigilisi isikuandmeid ja tegemist oli seetõttu juurdepääsupiiranguga teabega. Tol korral pidi inspektsioon selgitama, et hobuste põlvnemise andmed ei ole isikuandmed ja isikuandmete kaitse seadus laieneb siiski ainult füüsilistele isikutele ja nende andmetele.

2 Olümpiaadide tulemuste avalikustamine on keelatud.

Päris nii see siiski pole. 2023. aastal oli Andmekaitse Inspektsiooni menetluses juhtum, mille üheks küsimuseks kujunes olümpiaaditulemuste avalikustamise lubatavus ja tingimused. Ka avalikkuses tekkis diskussioon selle üle, kui kaua peaksid olümpiaaditulemused internetis nähtavad olema ja ekslikult võis jääda mulje, justkui oleks eri võistluste ja olümpiaadide tulemuste avalikustamine nüüd täiesti keelatud.

Tulemuste avalikustamisel tuleb lihtsalt silmas pidada seda, et selleks peab olema õiguslik alus ning kui õiguslik alus selliseks avalikustamiseks on olemas, siis tuleb seda teha kooskõlas isikuandmete kaitse üldmäärusest tulenevate põhimõtetega, milleks on muuhulgas minimaalsuse ja eesmärgipärasuse põhimõte. Olümpiaadi tulemuste avalikustamisel saaks selleks olla isikute nõusolek, õigustatud huvi või siis peaks see õigus tulema seadusest.

Lisaks peaks läbi mõtlema, kuidas ja kui kaua tulemusi avalikustatakse. Näiteks kas alati on vajalik kuvada ka konkreetset punktisummat või piisab saavutatud koha kuvamisest, või ehk saaks hoopis isikustatult kuvada neid õpilasi, kelle punktisumma on võimalikust saadavast kuni 50%. Peale selle peaks veel mõtlema läbi, milline on konkreetse eesmärgi täitmiseks vajalik andmete säilitamise tähtaeg. Aastakümnete pikkune säilitamine ja avalikustamine ei ole üldiselt esialgse eesmärgiga kooskõlas.

Esimene isikuandmete kaitse seadus võeti vastu juba 1996. aastal. Mõned aastad peale seda, täpsemalt 2001. aastal, jõustus avaliku teabe seadus. Kuigi vahepeal on seadused muutunud – 2018. aastal alustati isikuandmete kaitse üldmääruse rakendamist ning 2019. aastal jõustus uus isikuandmete kaitse seadus – on siiski läbi aja levinud nii isikuandmete kaitse, teabe avalikkuse kui ka Andmekaitse Inspektsiooni tegevuse kohta teatud müüte ja väärarusaamu. Toome mõned neist järgnevalt välja.

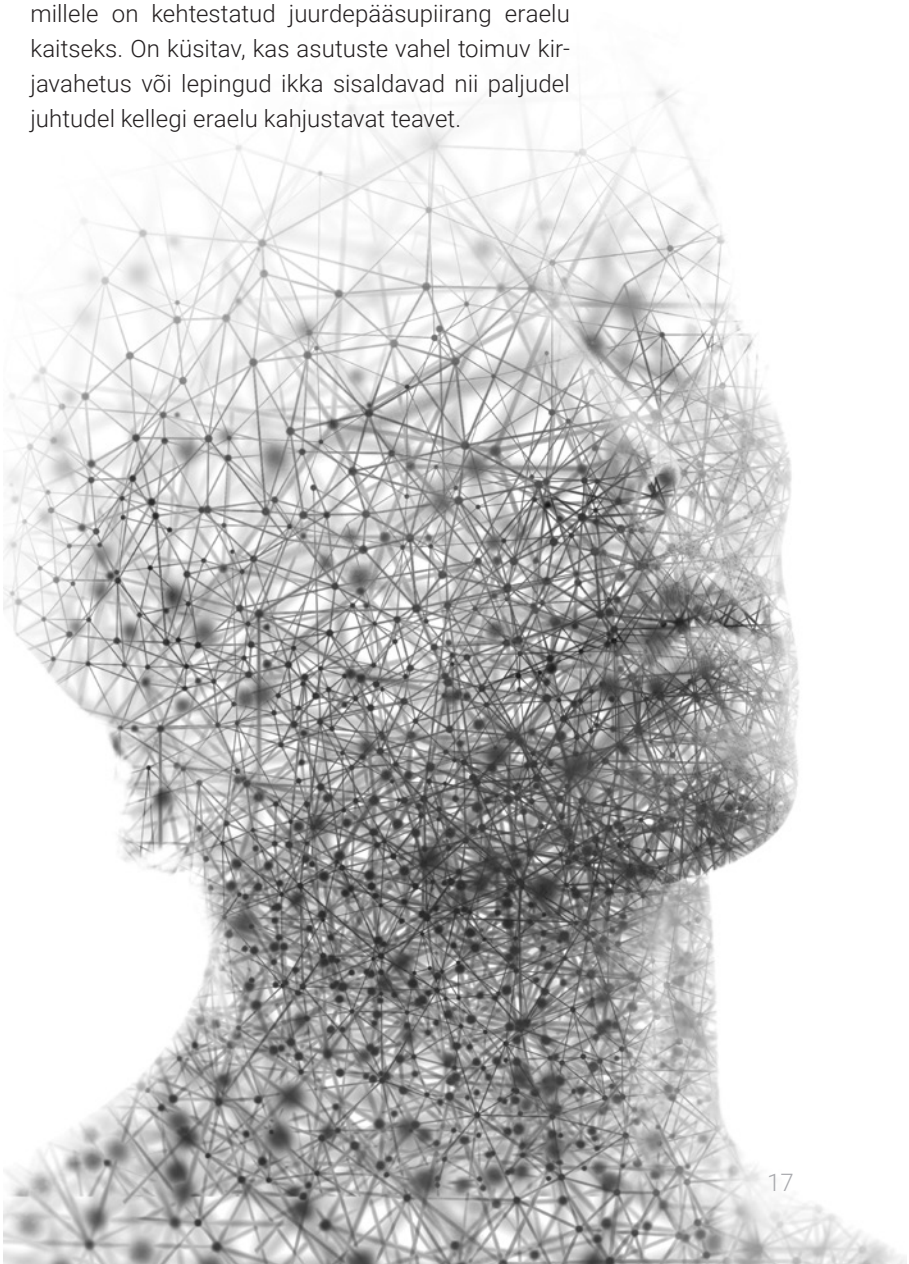
08

3 Kui dokument sisaldab isikuandmeid, siis tuleb sellele kehtestada juurdepääsupiirang avaliku teabe seaduse § 35 lõike 1 punkti 12 alusel, sest selle sätte kohaselt tuleb teave, mis sisaldab isikuandmeid ja millele juurdepääsu võimaldamine kahjustaks oluliselt andmesubjekti eraelu puutumatust, tunnistada asutusesiseseks kasutamiseks mõeldud teabeks.

See pole alati päris nii. Üksnes inimese nime olemasolu dokumendis ei ole alati piirangu seadmise põhjuseks avaliku teabe seaduse § 35 lg 1 p 12 alusel, kui dokument ise ei sisalda eraelu puutumatust oluliselt kahjustavat teavet. Ka sünniaja või isikukoodi lisamine nimele ei saa alati olla iseenesest piirangu seadmise aluseks. Näiteks ei saa avaliku teabe seaduse § 35 lg 1 p 12 alusel piirangut kehtestada dokumendi sisule ega ka dokumendi saaja/saatja isikule, kui dokument ei käsitle inimese eraelu, vaid üksnes avalikku tegevust ja ühiskondlikke küsimusi. Seda, kas dokument sisaldab inimese eraelu puutumatust kahjustavat teavet, tuleb hinnata iga dokumendi puhul eraldi ning vastavalt selle sisule.

Siiski tuleb rõhutada ja meeles pidada seda, et isikliku kontaktteabe (kodune aadress, isiklik e-postiaadress ja telefoninumber jms) sattumine piiramatu hulga võõraste isikute kätte võib oluliselt kahjustada tema eraelu puutumatust. See võib põhjustada rämpsposti adressaadiks sattumist ja muud soovimatut kontaktivõtmist. Seetõttu tuleb isiklikule kontaktteabele dokumendis seada piirang avaliku teabe seaduse § 35 lg 1 p 12 alusel. Kui dokumendile on selline piirang seatud, ei tähenda see siiski seda, et dokumenti poleks võimalik teabenõude korras väljastada.

Paraku näeb aga Andmekaitse Inspektsioon praktikas veel neid olukordi, kus piirangu kehtestamist põhjendatakse näiteks sellega, et dokument sisaldab eraelu oluliselt kahjustada võivaid andmeid, tegelikkuses aga on dokumendi pealkirjaks näiteks "Biojäätmete kogumist toetav meede". Pealkirja järgi otsustades tekib kahtlus, kas sellised dokumendid ikka sisaldavad isikuandmeid. Samuti on üsna palju asutustevahelist kirjavahetust ja lepinguid, millele on kehtestatud juurdepääsupiirang eraelu kaitseks. On küsitav, kas asutuste vahel toimuv kirjavahetus või lepingud ikka sisaldavad nii paljudel juhtudel kellegi eraelu kahjustavat teavet.



08

4 **Kui dokumendile on seatud juurdepääsupiirang**, siis polegi võimalik teabenõude korras teavet saada ega seda ka väljastada.

Ei, see pole tõsi. Kokkuvõtlikult võib öelda, et kui soovitud dokument sisaldab juurdepääsupiirangulist teavet, siis igaühel on õigus avaliku teabe seaduse alusel saada seda osa teabest või dokumendist, millele juurdepääsupiirangud ei kehti. Isegi kui teabevaldaja on kohustatud juurdepääsupiiranguga teavet sisaldava dokumendi tunnistama asutusesiseseks kasutamiseks, ei tähenda see, et kogu dokumendi sisu on juurdepääsupiiranguga.

Ka avaliku teabe seaduse § 38 lg 2 sätestab, et kui teabele juurdepääsu võimaldamine võib põhjustada juurdepääsupiiranguga teabe avalikuks tulemise, siis tagatakse juurdepääs üksnes sellele osale teabest või dokumendist, mille kohta juurdepääsupiirangud ei kehti. See tähendab, et teabenõudjale antakse välja dokument, milles üksnes kaitset vajav juurdepääsupiiranguga teave on kinni kaetud.

5 **Andmekaitsetingimused ei anna täielikku ülevaadet või puuduvad sootuks.**

Isikuandmete töötlemise üheks põhimõtteks, mida kõik andmetöötlejad peavad järgima, on läbipaistvuse põhimõte. Läbipaistvus tähendab usaldusväärsust ja tänapäeva ühiskonnas võib seda põhjendatult pidada digivisiitkaardi osaks.

Läbipaistvuse põhimõtte kohaselt peavad isikuandmete töötlemisega seotud teave ja sõnumid olema lihtsalt kättesaadavad (näiteks veebilehel), arusaadavad ning selgelt ja lihtsalt sõnastatud, ehk teisisõnu – koostatud peavad olema andmekaitsetingimused. Andmekaitsetingimused peavad olema sihtgrupile arusaadavas keeles ja vormis. Näiteks kui sihtgrupiks on lapsed või vanurid, siis peavad andmekaitsetingimused olema lihtsasti ja kergesti mõistetavad ka neile. Samamoodi peab arvestama, et kui ettevõtte põhisihtrühmaks on Eesti kliendid, siis peavad ka andmekaitsetingimused eesti keeles koostatud olema. Andmekaitsetingimuste sisu reguleerivad isikuandmete kaitse üldmääruse artiklid 12–14.

Ülioluline on aru saada, et andmekaitsetingimusi ei looda lihtsalt linnukese kirja saamiseks, vaid need peavad lähtuma just vastutava töötleja andmetöötlusest, mis eeldab, et andmetöötlus on täpselt kaardistatud ning ka andmekaitsetingimuste koostajale endale arusaadav.

Praktikas kipuvad andmetöötlejad andmekaitsetingimusi väga üldiselt sõnastama. Tegelikult peaks välja tooma kõik tõelised eesmärgid, õiguslikud alused ja selle, kellele andmeid edastatakse. Näiteks kasutatakse klausleid, et „võime teie andmeid edastada kolmandatele isikutele“, mis pole aga piisav, sest ei anna reaalset ülevaadet. Ka sõnade „näiteks, eelkõige, muu hulgas“ kasutamine ei ole hea tava. Samas ei tasuks ka ülemäära juriidilist, tehnilist ega erialast keelt või terminoloogiat kasutada.

Andmekaitsetingimused võiksid asuda lehe jaluses ja olla koostatud võimalikult lühidalt ning lihtsas sõnastuses, vältides seaduste kopeerimist. Samuti tuleks vältida kunstlikult loodud lauseid, mis ei anna tegelikult mingit lisainfot. Näiteks ei ole hea lause „klientide isiklikud andmed ning andmed nende poolt sooritatud tellimuste kohta on rangelt konfidentsiaalsed ja nende sattumine kolmanda osapoole kätte on välistatud“, sest see ei anna tegelikult mingit lisainfot.

08

6 Andmetöötlejal on õigus keelduda koopia väljastamisest isikule, kui failis on kolmandate isikute isikuandmeid, sest nende andmeid peab ka kaitsma.

Päris nii see siiski pole. Igal inimesel on õigus tutvuda enda kohta kogutud isikuandmetega ja saada selgitusi töötlemise asjaolude kohta. Seda õigust võib piirata üksnes siis, kui andmete edastamine kahjustab teiste isikute õigusi ja vabadusi. See aga ei tähenda seda, et olukorras, kus näiteks mõni dokument sisaldab kolmandate isikute andmeid, ei peaks üldse väljastama inimesele koopiat tema andmetest. Teiste isikuandmed tuleb lihtsalt kinni katta, sest koopia saamise õigus tähendab seda, et igal inimesel on õigus nõuda koopiat enda kohta käivatest isikuandmetest, mitte teiste inimeste andmetest.

Näiteks olukorras, kus isikuandmeid sisaldav videosalvestis sisaldab ka teiste isikute isikuandmeid, ei saa pidada isikuandmete kaitse üldmääruse või isikuandmete kaitse seaduse alusel teabe edastamisest keeldumise õigustatud põhjuseks. Tõepoolest, koopia saamise õigus ei tohi ju kahjustada teiste salvestisel olevate isikute õigusi ja vabadusi. See tähendabki, et juhul, kui andmesubjekti taotletava videosalvestise vaateväljas on nähtavad ka teised isikud, tuleb enne salvestise väljastamist teised inimesed salvestisel udustada.

Kui tema enda kohta käivate isikuandmete väljastamisest isikule siiski keeldutakse, siis tuleb ka põhjendada, kuidas isiku enda andmete talle väljastamine kahjustaks kolmandaid isikuid.

7 Kõige parem ja lihtsam on isikuandmete töötlemiseks võtta isiku nõusolek.

See on väärarusaam. Isikuandmete kaitse üldmääruses on välja toodud mitu võimalikku isikuandmete töötlemise õiguslikku alust. Näiteks saab selleks olla inimese nõusolek, töötlemine võib olla vajalik lepingu täitmiseks, andmete töötlemine on vajalik mõne juriidilise kohustuse täitmiseks või hoopiski on selleks andmetöötlejal õigustatud huvi. See loetelu siin pole muidugi ammendav.

Nõusolekut kui ühte isikuandmete töötlemise võimalust soovitakse aga tihti kasutada olukordades, kus üldmäärus muud alust selleks ei anna või kus see tundub kõige lihtsam. Tegelikult ei ole nõusolek aga mingi võluvits, mis võimaldaks igas olukorras ja igasugust andmetöötlust.

Nõusoleku puhul peab arvestama, et see peab olema vabatahtlik, konkreetne, selgesõnaline ja igal ajal tagasivõetav. Muuhulgas peab nõusolek olema kirjalikku taasesitamist võimaldavas vormis ning vaikimist või tegevusetust nõusolekuks ei loeta. Teisisõnu, kui isikul ei ole tegelikku valikut, ta tunneb end olevat sunnitud nõustuma või on keeldumisel negatiivsed tagajärjed, siis nõusolek ei kehti. Paljudel juhtudel on aga raske tagada, et nõusolek vastaks nendele kriteeriumitele.

Näiteks töösuhetes on nõusolekut töötaja isikuandmete töötlemiseks võimalik kasutada üksikutel juhtudel, sest töötaja allub tööandja juhtimisele ja kontrollile ning töötaja nõusolek ei oleks ei vabatahtlik ega sama lihtsalt tagasi võetav. Samamoodi ei loeta vabatahtlikuks nõusolekuks olukorda, kus n-ö „linnukese kast“ on eeltäidetud.

08

8 Igasugune huvi tähendab õigustatud huvi olemasolu.

Päris nii siiski ei ole. Isikuandmete kaitse üldmäärus näeb ühe isikuandmete töötlemise õigusliku alusena ette õigustatud huvi õigusliku aluse. Sel juhul on isikuandmete töötlemine vajalik andmetöötleja või kolmanda(te) isiku(te) õigustatud huvi korral ning on kaalukam andmesubjekti põhiõigustest ja -vabadustest. Seega ei tähenda mingi huvi olemasolu automaatselt seda, et võimalik oleks tugineda õigustatud huvile kui andmetöötluse õiguslikule alusele.

Enamasti oskavad andmetöötlejad üsna hästi enda huve välja tuua, sest soov andmetöötlusega alustada on millestki alguse saanud. Siiski on hea üle korrata, et õigustatud huvid peavad olema sõnastatud piisavalt selgelt. See tähendab, et ei piisa huvidest, mis on liiga ebamäärased või spekulatiivsed. Muidugi ei ole õigustatud huvi ka mitte miski, mis on ebaeetiline või ebaseaduslik.

Näiteks – kuigi turundus võib üldiselt olla legitiimne eesmärk – ei ole elektroonilise turunduse reeglitega vastuolus rämpsposti saatmine legitiimne. Samamoodi – isegi kui tööandja huviks võib olla näiteks tööaja kontrollimine – ei saa õigustatud huviks olla töötajate pidev ning ülemäärane kontrollimine ja jälgimine jälgimisseadmetega, sest see läheb vastuollu andmekaitset käsitlevate ja muude õigusaktidega. Samamoodi peab enne valvetegevuse alustamist olema käes tegelik olukord, näiteks varasem kahju või varasemad tõsised juhtumid.

9 Andmekaitse Inspektsioon aitab välja nõuda kahjuhüvitisi.

See ei vasta tõele. Teatud juhtudel võib isikutele nende isikuandmete töötlemise tagajärjel ka kahju tekkida ning abi saamiseks pöördutakse Andmekaitse Inspektsiooni poole. Näiteks võib tuua olukorrad, kui meedias on avaldatud ebaõigeid väiteid või kui mingit teavet on levitatud ilma õigusliku aluseta. Andmekaitse Inspektsioonil ei ole sellises olukorras pädevust välja mõista kahjuhüvitisi. Kahju hüvitamise hagiga tuleks pöörduda siis maakohtusse.

Inspektsioon saab kontrollida, kas isikuandmete töötlemiseks (nt avalikustamiseks) on olemas õiguslik alus ning kas andmetöötluses on järgitud kõiki põhimõtteid. Kui õiguslikku alust ei ole, siis saab inspektsioon kohustada isikuandmete töötlejat sellist tegevust lõpetama.

10 Häkkerid valivad sihtmärkideks suuremad ettevõtted ja elutähtsate teenuste pakkujad.

Ei, nii see ei ole. Siiski võib kohati ühiskonnas tajuda suhtumist, justkui oleks andmekaitse ning infoturbe tagamine miski, millega peavad tegelema ainult suured ning rahvusvahelised ettevõtted, sest nende käsutuses on ju suurel hulgal isikuandmeid. Niinimetatud pahalased ei vali aga enam ammu enda sihtmärke ainult nende tuntuse või suuruse alusel. Olulist rolli sihtmärgi valikul mängib ka see, milliseid andmeid töödeldakse ning kui hästi on ennast rünnete vastu kaitstud.

Tõepoolest, küberrünnakud elutähtsate teenuste osutajate vastu on viimase aastaga mitmekordistunud, kuid kindlasti saab sihtmärgi valikul määravaks ka see, kui kerge vaevaga on võimalik ohvrit rünnata. Seega ei ole sisuliselt küsimus enam selles, kes satub mõne rünnaku alla, vaid millal see juhtub ning millal leitakse üles süsteemi nõrgad kohad.

Näiteks võib mõne väiksema meditsiinitarkvara pakkuva ettevõtte ründamine pakkuda ründajatele hoopiski suuremat huvi kui näiteks seda sama teenust kasutava haigla süsteemidesse häkkimine, sest seeläbi on võimalik tekitada suuremat kahju ning paremini ka enda lunarahanõudeid maksma panna.

09 Maksehäirete avaldamine maksehäireregistrites

Võlgniku vastuväite saamisel ei hinda maksehäireregistrid enamikul juhtudel isiku ülemäärast kahjustamist piisaval määral, piirdudes üksnes arvessevõetavate asjaolude loetlemisega ja jättes konkreetset olukorda puudutavad elulised asjaolud sisuliselt hindamata. Veelgi enam paistab silma maksehäireregistrite komme õigustada ülemäärase kahjustamise tegematajätmist sellega, et isik ei ole vastuväite esitamisel välja toonud, kuidas võlaandmete avaldamine tema õigusi ja vabadusi ülemäära kahjustab, või puudub teave, et maksehäire avaldamine on kaebajale mis tahes kahju toonud. Kaalumise kohustus tekib maksehäireregistril endal iga kord juba enne, kui ta kavatseb avaldada või isegi koguda isiku võlaandmeid. Ülemäärase kahjustamise hindamisest jäetakse suuremas osas välja võlausaldajate iseloomustavad asjaolud võlaandmete avaldamise vajaduse kontekstis, nimelt kas võlausaldaja on enne avalikustamist ära kasutanud kõik võimalikud õiguskaitsevahendid võla sissenõudmiseks ja kas võlgnik on enne võlanõude aegumist olnud võlast teadlik jne.

Tihtipeale ei täideta piisava hoolsusega

andmete õigsuse tagamise kohustust. Üldjuhul ei kontrolli maksehäireregistrid maksehäirete avaldamisel võlaandmete õigsust ja lükkavad kogu vastutuse võlausaldajate õlgadele, kes võlaandmeid registritele edastavad. Kõige sagedamini ei kontrollita võlanõude olemasolu, võla summat, tekkimise ja lõppemise aega ning vastavust algdokumentidele. On esinenud olukordi, kus andmete õigsust ei suudetud dokumentaalselt tõendada ei peale isiku vastuväite saamist ega ka inspektsiooni järelevalvemenetluse ajal. Näiteks on inspektsiooni menetluses olnud juhtum, kus maksehäireregister on isiku eelnevatest nõudmistest hoolimata alustanud andmete õigsuse kontrollimist alles pärast järelevalvemenetluse algatamist, muutes menetluse käigus mitmel korral avaldatavaid võlaandmeid selliselt, et ühe nõude summa on võrreldes esialgsega muutunud 6 korda ja teise nõude summa lausa 49 korda suuremaks. Seejuures ei pidanud register vajalikuks ei isikut ega ebaõiged võlaandmed juba saanud kolmandaid isikuid andmete muudatustest teavitada.

Teavitamiskohustuse täitmisesse suhtutakse üldiselt kergekäeliselt. Valdavalt ei kontrollita üle, kas võlausaldaja on enne võlgnevuse registrile edastamist võlgnikku sellest teavitanud, ja seetõttu saab võlgnik tihtilugu emakordselt võlast teada alles siis, kui maksehäire on maksehäireregistris juba üleval. Paraku ei ole selline tegevus kooskõlas nõudega teavitada andmetöötlusest enne töötlema asumist. Samuti ei teavitata võlgnikku vajalikul määral enne tema isikuandmete maksehäireregistris avaldamist avalikustamise tingimustest, piirdudes teabe avaldamisega oma platvormi veebilehel, millest aga ei piisa andmetöötluse läbipaistvuse tagamiseks.

09

Kohustuse rikkumise lõppemisel ehk võla tasumisel lubab seadusandja maksehäiret registris nähtavana hoida veel kuni viis aastat. Tasumata võla avalikustamise aeg on seatud sõltuvusse võla aegumisest. Üldine tehingust tuleneva nõude aegumistähtaeg on kolm aastat pärast nõude sissenõutavaks muutumist ning kui tõendatud on kohustuse tahtlik rikkumine, aeguvad nõuded kümne aasta möödumisel. Seega olukorras, kus võlg jäeti tasumata, kuid nõue aegus kolme aasta jooksul, on võlaandmeid lubatud avalikustada veel lisaks kuni viis aastat (3 + 5 reegel). Tahtlikult rikutud kohustust on õigustatud avaldada kümne aasta jooksul, millele võib lisanduda maksimaalselt 5 aastat (10 + 5 reegel).

Kuivõrd kohtupraktikas on kinnituse leidnud, et andmete edastamine võib olla andmesubjekti õigusi ja vabadusi ülemäära kahjustav ka siis, kui kohustuste rikkumisest ei ole veel möödunud üle viie aasta, valivad maksehäireregistrid automaatselt maksimaalselt lubatud võlaandmete avaldamise pikkuse, jättes hindamata rikkumise tõsiduse ning andmete avaldamisega kaasneva riive võlgniku eraelu puutumatusele. Võlaandmete avaldamine maksimaalses määras viie aasta jooksul on lubatud vaid kõige tõsisemate võlakohustuste rikkumiste korral. Õigustatud ei ole avaldada vabatahtlikult tasutud võlgasid maksimaalse lubatud aja jooksul, sest sellisel juhul asetatakse võla kustutamiseks jõupingutusi teinud võlgnikud ebavõrdsesse olukorda võrreldes nendega, kes võlga üldse ei maksa.

Menetluspraktika näitab, et võlaandmete avaldajad võrdsustavad võlanõude tasumata jätmise kohustuse tahtliku rikkumisega, mis annab neile võimaluse avaldada maksehäireid 15 aasta jooksul. Paraku on selline praktika väär. Kümneaastase avaldamisaja valikul peab andmetöötleja tuginema konkreetsetele faktidele, mis kinnitaksid võlasuhte tahtlikku rikkumist, näiteks kohtuotsusele.

Andmetöötlejad ei suhtu nõutava tõsidusega võlgnike vastuväidetesse. Saades võlgnikult vastuväite teda puudutava võlanõude maksehäireregistris avaldamise suhtes, jätkatakse üldjuhul võlaandmete avalikustamist ja kolmandatele isikutele edastamist hoolimata isikuandmete edasitöötlemise keelust seni, kuni andmetöötleja tõendab, et töötleb andmeid mõjuval õiguspärasel põhjusel, mis kaalub üles andmesubjekti huvid, õigused ja vabadused.

Maksehäireregistrites võlaandmete avaldamist kasutatakse väiksemate aegunud võlgade tasumise sunnimehhanismina. Näiteks avalikustatakse teadlikult hästi vanu alla 100-euroseid ja ilmselt nüüdseks aegunud üksikuid võlanõudeid nagu parkimistrahve, prügiveoarveid vms, mille olemasolust ei pruugi inimene teadlik olla ja mis ilmselt ei näita inimese negatiivset maksekäitumist.

10 Maksehäirete avaldamise juhendi värskendamine

AKI andis 2022. aasta sügisel välja uue maksehäirete avaldamise juhendi, mille sisu ei olnud maksehäireregistrite pidajatele ja osadele krediidiasutuste katusorganisatsioonidele meeltmööda. Mõned ettepanekud kriitikutelt olid asjakohased või vähemasti andmekaitseõiguse vaatest vastuvõetavad ning seetõttu uuendas AKI 2023. aasta suvel juhendis mõningaid seisukohti. Lisaks kasutatavate mõistete lahtikirjutamisele täpsustas AKI muu hulgas järgnevat:

Enne andmete maksehäireregistris avaldamist peab maksehäireregister andmete õigsust kontrollima, kusjuures maksehäireregister võib selle kohustuse panna andmeid maksehäireregistrisse edastavale võlausaldajale, kuid sellisel juhul lepingus võlausaldajaga reguleerima, mis toimingud võlausaldaja enne andmete edastamist maksehäireregistrile andmete õigsuse tagamiseks kindlasti tegema peab. Samuti peab maksehäireregister pidevalt võlausaldajate kontrollimise põhjalikkust monitoorima ja küsima pisteliselt andmete õigsust tõendavaid lisadokumente.

Samuti peab maksehäireregister enne registrist andmete väljastamist kontrollima andmete küsija õigustatud huvi. Lepinguliste klientide puhul tuleb reguleerida lepingus, millistel tingimustel võib andmeid pärida ja asjaolu, et maksehäireregister kontrollib pisteliselt päringute õigustatust lisadokumentide alusel. Üksikpäringute puhul, kus ei ole andmete küsijaga püsilepingut, peab maksehäireregister iga päringu juures nõudma vähemalt lühikirjeldust asjaoludest, mis andmete saamise vajaduse tingivad.

AKI saab siiski hulgaliselt inimeste kaebusi maksehäirete avaldamise kohta. Üksikkaebuste eraldi menetlemine on aga ajamahukas ja ei too muutust maksehäireregistrite üldises praktikas. Seetõttu on AKI ette valmistamas maksehäireregistritele ettekirjutusi praktika üldiseks muutmiseks. Eeskätt näeb AKI probleemi maksehäiretega, mille summa on väiksem kui 100 eurot ja mis on inimese ainuke maksehäire.

AKI praktika näitab, et sellised maksehäired postitatakse maksehäireregistrisse eelkõige erinevate aegunud parkimise leppetrahvide sissenõudmiseks, mitte krediidivõimelisuse kohta info andmiseks ja reeglina ei ole sellistel inimestel tegelikkuses makseraskusi. Teiseks on probleem maksehäirete avaldamise ajaga – registrid soovivad andmeid avaldada maksimaalselt kaua ehk 5 aastat peale kohustuse rikkumise lõppemist või aegumist. Riigikohtupraktika ja IKÜM-i loogika eeldavad aga iga juhtumi puhul kaalumist, kui kaua on põhjendatud maksehäiret avaldada.

11

Positiivne krediidiregister

ja selle arengud

2023. aastal jätkas AKI panustamist positiivse krediidiregistri väljatöötamisse, mille tulemusena peaks Rahandusministeeriumi eestvedamisel valmima isikute finantskohustustest ülevaadet andev register. Eesmärk on luua preventiivse mõjuga register, mis turuosaliste vahel isikute maksekohustuste osas andmeid vahetades aitaks kaasa vastutustundliku laenamise põhimõtte paremale rakendamisele. Nagu on näha ka Andmekaitse Inspektsiooni järjekindlast praktikast, esineb isikutel laenukohustuste täitmisel raskusi, mis toob kaasa suure maksehäirete avaldamise arvu.

Septembris edastati AKI-le arvamuse avaldamiseks Cybernetica AS-i uurimus, mis koondab struktureeritult info loodava registri ja selle rakendamist puudutavate tegurite kohta seni tehtud uuringutest, eri osapoolte hinnangutest ja varasematel aastatel antud tagasisidest positiivse krediidiregistri väljatöötamiskavatsusele. Rahandusministeeriumi tellitud uuringu eesmärgiks on registri tehnoloogilise lahenduse väljapakkumine ja parima arhitektuuri valimine.

Kuna 2023. aastal edastatud uuring oli suuresti varasemalt antud infot koondav ega pakkunud veel registri loomiseks konkreetseid variante, rõhutas AKI enda tagasisides jätkuvalt vajadust mõelda läbi, kuidas tagada inimeste kohta võimalikult väheste andmete kogumine ning registris kajastatavate andmete õigsus. Näiteks vähenevad isiku laenukohustused regulaarselt ja selleks, et tagada registriandmete õigsus, tuleks registrit pidevalt ajakohastada. Ka loodava registri infotehnoloogilise lahenduse osas on isikuandmete kaitse seisukohalt endiselt eelistatud, et krediidiandjatel oleks võimalik andmeid pärida läbi andmevahetuskanali, mitte ühtsest isikute krediidiandmeid koondavast andmekogust, kuivõrd viimase puhul oleks andmelekke korral risk rohkematele inimestele kahju tekkimiseks võrreldamatult suurem.

Andmekaitse Inspektsioon jääb innukalt ootama Rahandusministeeriumi eelnõud positiivse krediidiregistri ellukutsumiseks.

12 Kaamerate

kasutamise küsitavus töökeskkonnas

Videovalve kasutamine on ettevõtetes laialdaselt levinud, paraku ka selle väärpraktika, mistõttu tegeles inspektsioon ka 2023. aastal väga paljude tööandjate andmekaitsealase teadlikkuse tõstmisega.

Paljud tööandjad ei ole teadlikud, milline õiguslik alus kaameratega andmetöötlust võimaldab ning tuginevad ekslikult töötajate nõusolekule, näiteks kogudes selleks töötajatelt allkirjad. Samuti on levinud, et tööandja lihtsalt teavitab andmetöötlusest töölepingus. Töösuhtes ei ole pooled võrdses positsioonis ning seega on vähetõenäoline, et töötaja annab sellistel juhtudel enda jälgimiseks heakskiidu vabatahtlikult, mistõttu ei saa neid viise pidada üldmääruse tingimustele vastavaks tahteavalduseks. Seega on videovalve puhul töötajate isikuandmete töötlemise peamiseks võimalikuks aluseks õigustatud huvi. Sellele alusele saab aga toetuda üksnes siis, kui tööandja on kaalunud eelnevalt mõlema poole huve ning jõudnud järelduseni, et kaamerate kasutamine ei riiva töötajate huve ülemääraselt.

Enne videovalve kasuks otsustamist tuleb läbi mõelda:

- **kas ja milline on selle kasutamise vajadus ning kas kasu kaalub üles jälgimise negatiivsed mõjud,**
- **kas videovalve rakendamiseks on olemas selge üheselt mõistetav eesmärk ning**
- **kas see on efektiivne vahend või on olemas teisi vahendeid, mis isikute õigusi vähem riivaks.**

Terve tööaja vältel kaamerate vaateväljas töötamine kujutab endast väga intensiivset õiguste riivet ning võib töötajate vaimset heaolu mõjutada. Lisaks sellele, et pidev jälgimine piirab isikute väljendusvabadust, võib jälgimine põhjustada stressi ja töövõime langust. Seetõttu tuleb kaamerate kasutamisel töökeskkonnas hoolikalt kaaluda, kas isikutele tekitatav mõju on proportsionaalne taotletavate eesmärkide suhtes.

Kaameraid kasutatakse tihti ülemääraselt ja valedel eesmärkidel – need on paigaldatud ettevõtte igasse ruumi ja nurka või eesmärgiga töökohustusi ja tööajast kinnipidamist kontrollida. Jälgimisseadmeid ei saa töökohal kasutada üldise viitega võimalikele rikkumistele, vaid need peavad olema suunatud konkreetselt määratletud turvaprobleemi lahendamisele. Inspektsiooni töölauale on jõudnud ka juhtumeid, kus video- ja audiosalvestiste abil sooviti lahendada kolleegide vahelisi erimeelsusi ja konflikte klientidega. Ettevõtte sisekorra tagamiseks saab jälgimisseadmeid kasutada vaid juhul, kui nende eesmärgiks on ennetada füüsilisi turvaintsidente, näiteks ohtlike seadmete kasutamisest tingitud võimalikke tööõnnetusi. Seega võib paigaldada videovalve töötajate tõsiste rikkumiste ennetamiseks ja avastamiseks, küll aga ei või salvestiste abil menetleda töötajate teisi väiksemaid rikkumisi.

Eesmärk ei pühitse alati abinõu – kuigi kaamerate kasutamine on peaasjalikult lubatud turvalisuse tagamiseks ja vara kaitseks, ei saa neid siiski igale poole paigaldada, näiteks puhke-, riietus-, duši- ja tualettruumidesse. Paljudel juhtudel on eesmärgi saavutamiseks ka paremaid alternatiive, mis ei kätke isikuandmete töötlemist, näiteks lukud ja

12

turvaelemendid, millega saab vargusi ja vandalismi tõhusamalt ennetada. Kasutatavad meetmed peavad olema adekvaatsed ja proportsionaalsed nende riskide suhtes, mida soovitakse maandada, seega tuleb teostada töötajate jälgimist võimalikest leebemail viisil. Kui leidub isikute õigusi vähem riivav alternatiiv, näiteks vara kaitseks turvatöötaja palkamine või töökonfliktide lahendamiseks personalitöötaja kaasamine, tuleks seda eelistada. Tööprotsesside jälgimiseks ei ole kaamerad ainuke lahendus ning reaalajas töötajat jälgida võimaldava süsteemi kasutamine on selgelt ülemäärane, kui on olemas teisi vahendeid eesmärkide saavutamiseks. Kaamerad ei tohiks kompenseerida personalitöötajate puudust või asendada teisi töötajate juhendamise või juhtimise meetodeid.

Videovalve kasutamise vajaduse väljaselgitamine on oluline ka sobiva tehnika, kaamerate vaateväljа ja funktsioonide ning asukohtade valimisel ja seejuures tuleks lähtuda isikuandmete minimaalse töötlemise põhimõttest. Kui ettevõttel on vaja jälgida fikseeritud ala, näiteks sissekäiku või kassat, pole vajalik paigaldada 360-kraadise vaateväljaga või pööramise ja suumimise funktsioonidega kaamerat. Inspektsioon on seisukohal, et kaameratega heli salvestamine on üldiselt keelatud ning me ei ole veel praktikas kohanud juhtumit, kus selline tööandja sekkumine töötajate privaatsusesse oleks põhjendatud. Nende lisafunktsioonide rakendamine loob ettevõttes ebameeldiva tööõhkkonna, sest kui töötaja iga liigutust jälgitakse või pealt kuulatakse, tekitab see ebamugavust, hirmu ning usaldamatust. Igasuguste lisavõimaluste kasutamise puhul on ettevõttel väga keeruline tõendada andmekaitsenõuete täitmist ning saadav kasu ei kaalu tihti üles nende negatiivset mõju.

Üheks põhiliseks probleemiks on endiselt ka andmetöötluse läbipaistmatus – töötajaid ei ole videovalvest teavitatud, dokumentatsioon on puudulik või puudub üldse. Enne videovalvega alustamist peab ettevõte panema paika reeglid, mis eesmärkidel neid kasutatakse, kes ja mis juhul võib salvestistele ligi pääseda, kui kaua salvestisi säilitatakse ning looma võimaluse kontrollida andmetöötluse õiguspärasust andmetöötlustoimingute registri abil. Töötajal peab olema võimalik aru saada, kas ja kuidas tema tegevusi jälgitakse. Seetõttu on vaja paigaldada videovalvest teavitavad sildid ning ettevõttesiseselt informeerida töötjaid ka andmekaitsetingimuste, töökorralduse või sisekorra reeglitest, mida on töötajatele tutvustatud ning mis on alati lihtsasti kättesaadavad. Töötajal peab olema võimalik saada igal ajal tööandjalt teavet ja selgitusi oma isikuandmete töötlemise kohta ning esitada sellele vastuväiteid.

Kokkuvõttes peab tööandja enne kaamerate kasutamise alustamist olema läbi mõelnud videovalve vajaduse ja eesmärgi, viies läbi õigustatud huvi hindamise, videovalve kasuks otsustades tuleb see dokumenteerida ja töötajaid informeerida, luues kaamerate kasutamise tingimusi ja eesmärke tutvustavad andmekaitsetingimused ja teavitussildid.

13

Kaamera vaateväljas

töötamise mõju vaimsele tervisele

Praegusel ajal on reaalsuseks see, et meie igapäevaelu ümbritsevad kaamerad. Kaamerad on vajalikud, kuna need aitavad meil tagada turvalisust, toetavad meid tõendite kogumisel, võimaldavad meil kiiremini suhelda ja teha tööd kaugtöö vormis. Siiski ei saa vaadata mööda sellest, kuidas mõjub kaameraga töötamine inimese vaimsele tervisele.

Kõige enam täheldatakse, et kaameraga töötamine tekitab stressi, ärevust ning pideva jälgimise tunnet. Videokoosolekutel või kaamera ees töötades tõuseb inimestel enesetunnetuse tase ja hakatakse ümbritsevat keskkonda üha rohkem mõtestama. Kuidas saab enesetunnetus ja mõtestamine üldse kuidagi negatiivne olla? Pidev keskendumine eneseteadlikkusele võib tegelikult osutuda vastumeelseks ning töökeskkonnas ebaproduktiivseks. Usun, et paljud on minuga nõus, kui väidan, et videokoosolekutel jälgitakse kõige rohkem enda kaamerapilti. Jälgitakse enda väljanägemist ja hoiakut ning mõeldakse, kuidas mõjun läbi kaamera teistele. Kaamera ees töötamisel või videokoosolekutel tekibki tunne, et meid hinnatakse pidevalt – see mõjutab töötulemusi ning põhjustab ebavajalikku pinget. Seega tekitab kaamera tunde, et keegi pidevalt vaatab mind.

APA (American Psychological Association) avalikustatud uuring (2021) toob meieni täiesti uue mõiste, mis kujunes välja pärast COVID-19 levikut. Viiruse levik toimetas kõik koosolekud kaamerate ette ning sellest kujuneski lõpuks nähtus Zoom fatigue ehk Zoomi-väsimus. Uuringu oluline leid põhineb asjaolul, et just kaamerat kasutanud katseisikud tundsid kõige suuremat väsimust, eraldi toodi välja uued töötajad ning naised. Põhjuseks arvatakse olevat, et kaamera vahendusel osalemine tekitab „pealtvaatamise“ tunde, mis omakorda tekitab üleliigset stressi. Kõrgenenud eneseteadlikkus koosolekul ning selle üleliigne mõtestamine suunab tähelepanu tööteemadest pigem sissepoole.

Kokkuvõttes võib väita, et kaamerad meie tööelust ei kao, see tähendab, et tasakaalu selle kasutamise eeliste, privaatsuse ning vaimse tervise vahel peavad hoidma nii organisatsioon kui ka tööandja. Seda ei tohiks vaadata kui tüütut lisaülesannet, sest kaamera kasutamise reguleerimine mõjutab töötajate sooritust. Tööandja ning organisatsioon saavad paremaid tulemusi, kui suhtlevad oma töötajatega ning arutlevad, kuidas luua tööd toetav keskkond ka koos kaameratega. (Kasutatud: https://doi.org/10.1037/apl0000948)

Johan Pastarus
Tööinspektsiooni vaimse tervise konsultant

13

14 E-privaatsuse tagamine

elektrooniliste sideteenuste kasutamisel

Seekordses ülevaates on paslik küsida, kas varasematel aastatel tehtud kodutöö on piisav, et liikuda vastu uutele väljakutsetele, mida meie eraelu kaitse eeldaks kõikvõimalike uute tehnoloogiate kasutamisel. Paraku ei saa sellele väga positiivse tooniga vastata.

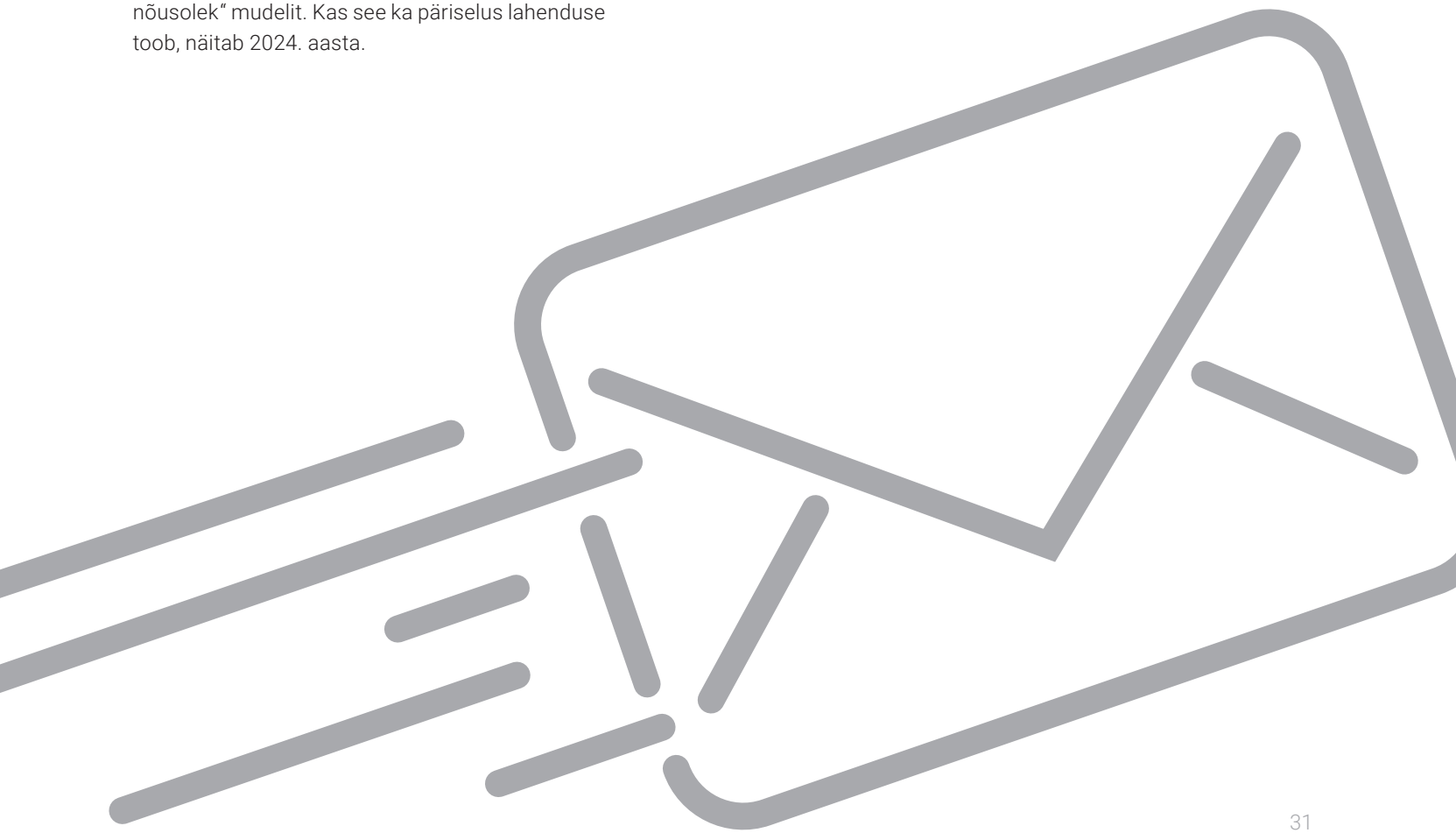
Kes mäletab, siis juba aastal 2002 lepiti Euroopa Liidu üleselt kokku põhimõtetes, mis aitavad meie kõigi isikuandmete töötlemist ja eraelu kaitsta elektroonilise side sektoris. Jutt käib direktiivist 2002/58/EÜ, millele tehti vähesel määral muudatusi 2009. aastal. Nimelt on selles õigusaktis põhimõtteline säte, täpsemalt artikli 5 lõige 3, mille eesmärk on kaitsta lõppkasutaja seadet. Täpsemalt selgitab säte, et teabe salvestamine lõppkasutaja lõppseadmesse ja juurdepääsu saamine seadmesse juba salvestatud teabele saab toimuda ainult lõppkasutaja ehk inimese nõusolekul. Tõsi, ette on nähtud ka kaks erandit – nõusolek ei ole vajalik, kui andmete tehnilise salvestamise ja juurdepääsu ainus eesmärk on edastada sidet elektroonilises sidevõrgus või mis on teenuseosutajale hädavajalik sellise infoühiskonna teenuse osutamiseks, mida lõppkasutaja on sõnaselgelt taotlenud.

Kõik, kes me täna eri veebilehti kasutame, puutume selle põhimõttega iga päev kokku – läbi küpsiste nõusoleku küsimise hüpikakende, mida meile enne veebilehel edasi liikumist kuvatakse. Ekslikult on aga jõus arusaam, et see säte käibki ainult küpsiste kohta. Tegelikkuses väljastavad meie arvutid ja nutiseadmed võrgus toimetades erinevat teavet. See on ühelt poolt vajalik näiteks internetiühenduse toimimiseks ja võrgupäringute õigesse kohta suunamiseks, kasutades IP-aadressi, või näiteks kodusesse WiFi-võrku automaatseks sisselogimiseks, kus võrk tunneb ära seadme MAC-aadressi. Samuti liigub veebipäringutega seadmest kaasa teavet kasutatava operatsioonisüsteemi või seadme tüübi kohta. Pole saladus, et veebiteenuse osutajad peavad meie kohta ka üsna detailset ülevaadet, kes, millal ja millistel veebilehtedel käib. Või kas teate, et kui näiteks meie postkasti potsatab turundusliku sisuga elektronkiri, on levinud praktika, et kirja saatjad saavad teada, millal olete e-kirja avanud ja kas tegite seda näiteks Eestis või välismaal olles. Peenemad meetodid annavad saatjale ka aimu, millist osa turunduskirjast me kõigepealt vaatasime. See kõik on võimalik, kuna e-kirjaga on kaasas koodijupp või jälituslink, mis saatjale saaja tegevustest tagasi raporteerivad. Kuid kas meid sellistest tegevustest üldjuhul teavitatakse? Reeglina mitte. Kui nüüd mõelda eespool selgitatud põhimõttele, et tegemist on meie seadmesse salvestatava teabega (jah, ka jälituskoodi saab pidada teabeks) siis kas ei eeldaks selline tegevus mitte meie selgesõnalist eelnevat nõusolekut? Samuti ei saa sellist tegevust tõenäoliselt ka hädavajalikuks pidada, kuna turunduskirja saab saata ka ilma jälituskoodita.

14

Juba 2017. aasta alguses tuli Euroopa Komisjon välja määrusettepanekuga, mille eesmärk olnuks tagada meie kõigi eraelu austav ja kaitsev tegevus elektrooniliste sideteenuste kasutamisel. Oli ootus, et õigusakt jõustunuks samal ajal isikuandmete kaitse üldmäärusega ehk mais 2018. Kahjuks ei ole ootus õigusakti tasemel Euroopaüleseks praktikate ühtlustamiseks tänaseni realiseerunud. Küll aga on mindud samm tagasi ja algatatud arutelu vabatahtlikkusel põhinevateks printsiipideks (nn Cookie Pledge), mis võiksid lahendada küpsiste ja suunatud reklaamidega seotud tarbijaprobleeme – näiteks seda, kui sageli peaks küpsiste bännerit kasutajale uuesti kuvama, kui nõusolek on kas antud või sellest keeldutud, või mida silmas pidada, kui soovitakse rakendada „maksa või anna nõusolek" mudelit. Kas see ka päriselus lahenduse toob, näitab 2024. aasta.

Küll aga on Euroopa andmekaitseasutused koondanud ühiselt jõud ning Euroopa Andmekaitsenõukogu eestvedamisel pannud kokku värsked suunised, mis selgitavad e-privaatsusdirektiivi artikli 5(3) kohaldumist tänastele ja uutele jälgimistehnikatele, mida kasutatakse näiteks e-posti- või veebiteenustes. Suuniste tööversioon on kõigile huvilistele kättesaadav siin: (https://edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-22023-technical-scope-art-53-eprivacy_en). 2023. aasta lõpuni said kõik huvirühmad dokumendile oma ettepanekuid esitada. 2024. aasta esimeseks pooleks on suuniste lõplik sisu loodetavasti paigas ning andmekaitsenõukogu veebis ka avaldatud.



15

Andmekaitsealane

Schengeni hindamine

2023. aasta novembris koordineeris Andmekaitse Inspektsioon Eestis toimunud Schengeni andmekaitsealast hindamist, mille raames viibisid Eestis Euroopa Liidu liikmesriikide ning Euroopa Komisjoni eksperdid. Eelmine hindamine toimus aastal 2018 ning järgmine toimub vastavalt muudatustele Schengeni hindamise korralduses 7 aasta pärast aastal 2030. Hindamise tulemusena saavad Eesti vastutavad asutused tegevusplaani koos soovitustega võimalike puuduste kõrvaldamiseks.

Schengeni viisaruum võimaldab ligi 420 miljonil inimesel liikuda alas ilma, et nad peaksid läbima sisemisi piirikontrolle, ning efektiivset kaupade ja teenuste vedu. Selleks, et säilitada liikmesriikide ning isikute usaldus süsteemi vastu, on vajalik tagada, et viisaruumi nõudeid kohaldatakse korrektselt, efektiivselt ning kõikides liikmesriikides ühtselt. Kuivõrd ühe Schengeni viisaruumi liikmesriigi puudused või nõueterikkumised võivad mõjuda kogu viisaruumile negatiivselt, loodi selle vältimiseks järelevalvesüsteem, mille eesmärgiks on tuvastada puudusi viisaruumi nõuete täitmisel ning esitada ettepanekuid nende lahendamiseks. (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2021:278:FIN).

Hindamisel käsitletakse strateegilisi elemente nagu ametnike/töötajate piisav koolitatuse tase, inimressursid, riskianalüüs, situatsiooniplaneerimine, ja külastatakse politseid, ministeeriumeid ning teisi asutusi. (16.5.2023 COM(2023) 274 final LISA 1)

15

Andmekaitse valdkonnas on peamine fookus andmesubjektide õigustel, kaebuste lahendamisel ning tundliku informatsiooni käsitlemisel. Põhjalikult käsitletakse andmekaitseasutuse rolli, peamisi ülesandeid, volitusi ja sõltumatust, struktuuri, inimressursse, eelarvet ning avalikkuse teavitamist. Oluliseks aspektiks on samuti koostöö teiste liikmesriikide andmekaitseasutustega. Kuna Schengeni viisaruumis on märkimisväärne roll ka eri riikidevahelistel infosüsteemidel, siis hindamise üheks eesmärgiks on tagada, et infosüsteemid ning neis toimuv infotöötlus vastavad kõikidele vajalikele andmekaitsenõuetele.
(https://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vi7jgta93rwi)

2018. aasta hindamise tulemusena esitas Euroopa Komisjon Eestile soovitused, millele järgnevatel aastatel tähelepanu pöörata ning siseriiklikusse praktikasse üle tuua. Kokku esitati 21 soovitust, millest kuue eest oli vastutav Andmekaitse Inspektsioon. 2023. aasta hindamisel teatas Andmekaitse Inspektsioon, et kõik kuus soovitust on tänaseks täidetud või on käesoleval hetkel ellurakendamisel.
(https://data.consilium.europa.eu/doc/document/ST-12870-2020-INIT/et/pdf)

16 Facebooki platvormi

kasutamine isikuandmete kaitse vaatest

Sotsiaalmeediaplatvormide populaarsus on viimase kümnendi jooksul hüppeliselt kasvanud nii erasfääris kui ka avalikus sektoris. Kahtlemata on üks populaarsemaid kanaleid Meta (Meta Platforms Ireland Limited) platvormide hulka kuuluv Facebook. Kuivõrd Facebooki kasutavad väga erineva demograafilise ja sotsiaalse taustaga inimgrupid, siis aitab Facebooki lehe kasutamine jõuda potentsiaalselt suurema hulga inimesteni kui seda võimaldavad mitmed alternatiivsed kanalid. Lisaks eraisikutele on ka ettevõtete ja avaliku sektori asutuste jaoks Facebooki lehe omamine muutunud tavapäraseks praktikaks. Kahtlemata on selliste lehtede kasutamisel mitmeid positiivseid külgi. Näiteks Politsei- ja Piirivalveamet kasutab Facebooki kadunud inimeste leidmiseks. Avaliku sektori asutused saavad selliste lehtede kaudu inimesi oma tegemistega kursis hoida ning tõsta avalikkuse teadlikkust olulistel teemadel. Samas võivad Facebooki lehe kasutamisega kaasneda ka teatavad riskid lehte külastavate inimeste privaatsusele.

Norra andmekaitseasutus koostas 2021. aastal mõjuhinnangu, et hinnata riske, mis võivad kaasneda andmekaitseasutusele Facebooki lehe loomisega. Mõjuhinnangus rõhutati andmekaitseasutuste rolli juhtfiguurina, mis toob kaasa kõrgendatud ootused isikuandmete töötlemisega kaasnevate riskide hindamiseks ja nendega arvestamiseks. Ühelt poolt oli vajalik hinnata asutuse huvi Facebooki lehe kasutuselevõtmiseks ning teiselt poolt ka lehte jälgivate inimeste huvi privaatsuse vastu.

Norra andmekaitseasutus selgitas oma mõjuhinnangus, et kuivõrd avalik asutus on lehe loomisel kaasvastutav töötleja koos Metaga, siis ei saa asutus ise lõpuni kindlaks määrata seda, kuidas toimub platvormil isikuandmete töötlemine. Isegi kui asutus teeb kõik endast oleneva, et andmekaitse põhimõtteid järgida ning muu hulgas isikuandmete töötlemist minimeerida (nt kommenteerimise võimaluse piiramise kaudu ning privaatsõnumite funktsiooni eemaldamise teel), siis ei peata see andmetöötlust, mida teeb Meta. Mõjuanalüüsis toodi muu hulgas esile asjaolu, et Meta andmekaitsetingimustes loetletud eesmärgid isikuandmete töötlemiseks on küllaltki üldised ja ei pruugi tagada terviklikku ülevaadet sellest, mida Meta isikuandmetega teeb, arvestades andmetöötlemise suuremahulisust ja keerukust. Seejuures ei ole asutusel, kes soovib Facebooki lehte avada, võimalik Metaga eraldi läbi rääkida töötlemisele kohalduvaid lepingutingimusi, kuivõrd kõikidele veebilehe omanikele kohalduvad standardtingimused. Mõjuhinnangu tulemusel otsustas Norra Facebooki lehte mitte kasutusele võtta. (https://www.datatilsynet.no/contentassets/8561465062b04a6b904c8c3573a24687/full-report-en_risk-assessment_should-the-norwegian-data-protection-authority-create-a-page-on-facebook.pdf)

Norraga sarnase mõjuhinnangu on lasknud koostada ka Madalmaade valitsus. Mõjuhinnangu tulemusel tuvastati 7 isikuandmete kaitsega seotud kõrget riski. Riskidena toodi muu hulgas esile probleemid isikuandmetega seotud õiguste teostamisega ning Meta edasise töötlemise üle kontrolli kaotamisega. Samuti on Facebooki lehe kasutamisega seotud riske uurinud Saksa andmekaitseasutus. 2021. aastal andis Saksamaa föderaalse andmekaitseasutuse juht Ulrich Kelber tungiva soovituse

16

kõikidele avaliku sektori asutustele oma fännilehtede sulgemiseks. See soovitus hõlmas ka valitsuse ametlikku veebilehte, millel oli tol hetkel üle miljoni jälgija. (https://www.privacycompany.eu/blogpost-en/dpia-on-government-use-of-facebook-pages-seven-high-data-protection-risks)

Kelber tõi oma pöördumises Norra mõjuhinnanguga sarnaselt esile, et Facebook ei avalda fännilehtede omanikele piisavat ülevaadet selle kohta, kuidas lehe jälgijate isikuandmeid töödeldakse, mis tekitab kõhklusi läbipaistvuse põhimõtte järgimise osas. Rõhutati ka seda, et avalikud asutused ei peaks oma veebilehe jälgijate isikuandmeid avaldama kolmandatele osapooltele (st Metale). Muu hulgas kasutab Meta külastajate isikuandmeid isikustatud reklaami edastamiseks, seejuures kasutatakse ka nende külastajate isikuandmeid, kes ei ole platvormile eraldi kontot loonud. (https://iapp.org/news/a/german-dpa-tells-government-organizations-to-shut-down-facebook-pages/)

Isikustatud reklaamidega seotud probleemaatikat ning seda, kas Meta järgib sellise reklaami edastamisel andmekaitsereegleid, on aastaid uuritud. Euroopa Andmekaitsenõukogu tegi 2022. aasta detsembris otsuse, milles leidis, et Meta ei tohi isikustatud reklaami edastamiseks tugineda lepingulisele alusele. (https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-32022-dispute-submitted_en)

2023. aasta 27. oktoobril tegi Andmekaitsenõukogu uue otsuse, milles leiti, et ka õigustatud huvi alusel isikustatud reklaami edastamine ei ole isikuandmete kaitse üldmäärusega (edaspidi: üldmäärus) kooskõlas. Otsuses rõhutati, et Meta ei ole oma tegevust endiselt varasemate otsustega vastavusse viinud ning kohene keelavate meetmete kasutuselevõtmine on vajalik isikute õiguste ja vabaduste kaitsmiseks (https://edpb.europa.eu/system/files/2023-12/edpb_urgentbindingdecision_202301_no_metaplatformsireland_en_0.pdf). Meta võttis juba enne otsuse tegemist kasutusele uue nõusolekul põhineva süsteemi, mis võimaldab kasutajal valida, kas lubada isikustatud reklaami näitamine või maksta igakuiselt reklaamist keeldumise eest, et hoida sellisel otstarbel ära isikuandmete töötlemine. Tänaseni puudub otsus, mis kinnitaks, et Meta on suutnud oma tegevuse üldmäärusega kooskõlla viia.

Lisaks isikustatud reklaami edastamisele on Metale ette heidetud ka teisi isikuandmete töötlemisega seotud rikkumisi. Kümnest kõige suuremast trahvist pooled on suunatud Meta ja Metale kuuluvate platvormide vastu, seejuures kuulub ka kõige suurem üldmääruse alusel määratud trahv (1,2 miljardit eurot) Metale. Tänaseks on Facebooki veebileht kasutusel vaid mõnel üksikul andmekaitseasutusel. Selline kahanev arengusuund on mõistetav, kuna vähemalt käesoleval hetkel ei ole andmekaitseasutusel Facebooki lehe kasutamisel võimalik täie kindlusega tagada, et kõiki üldmääruse reegleid järgitakse ning et lehe külastajate isikuandmed oleks kaitstud. Seetõttu ei pruugi sellise lehe kasutamisega kaasnevad ohutegurid kaaluda üles veebilehe kasutamise positiivseid külgi.

17 Andmekaitsealased

trahvid Euroopas 2023. aastal

Aasta 2023 osutus andmekaitsetrahvide poolest sündmusterohkeks. Sel aastal saavutati rekord – määrati kõrgeim trahv, mis isikuandmete kaitse üldmääruse all eales määratud on. Iirimaa järelevalveasutus trahvis aprillis Metat 1,2 miljardi euro eest, kuna viimane edastas oma Facebooki teenuse kaudu ilma põhjendatud seadusliku aluseta massiliselt Euroopa Liidu kodanike isikuandmeid Ameerika Ühendriikidesse. Nimelt leidis isikuandmete edastamine aset lepingu tüüptingimuste alusel, kus Euroopa Liidu kodanikel puudusid piisavad kaitsemeetmed ja õiguskaitsevahendid oma andmete töötlemist Ameerikas vaidlustada. See hiigeltrahviotsus lisab rõhku aastakümnepikkusele pingelisele läbirääkimisele Euroopa Liidu ja USA vahel, millega üritatakse võimaldada andmete seaduslikku edastamist üle Atlandi ookeani nimetatud osapoolte vahel.

Eelnevad Euroopa Liidu kaitse piisavuse otsused Ameerika kohta tunnistati kahel korral kehtetuks (aastatel 2015 ja 2020) ettekäändel, et USA seadused ei taganud piisavat kaitset andmesubjektidele, kelle isikuandmete töötlemine leiab aset Ameerikas. Andmekaitsesaaga aga jätkub: 2023. aasta juulis leppisid Euroopa Liit ja USA kokku uue andmekaitseraamistiku (Data Privacy Framework), mille põhjal võivad ettevõtted isikuandmeid kahe mandri vahel edastada, kuid ka see värskeim kokkulepe pole jäänud tähelepanuta – kokkuleppele on mitmed andmekaitseaktivistid juba kriitikat ja kaebuseid esitanud.

Meta sai 2023. aasta jaanuaris ka teise, 390 miljoni suuruse hiigeltrahvi – leiti, et ettevõte ei andnud oma kasutajatele piisavat teavet, millistel põhjustel ja millisel moel nende andmeid Instagrami ja Facebooki teenustes töödeldakse. Lisaks kasutas Meta valet (lepingulist) õiguslikku alust kasutajate andmete töötlemiseks, et neile isikustatud reklaame kuvada. Meta sundis oma kasutajaid andma nõusolekut isikuandmeid üles andma ettekäändel, et see oli vajalik osa Instagrami ja Facebooki teenuse osutamiseks, kuid Iirimaa leidis, et selline käitumine viitas sunnitud nõusolekule ja et isikustatud reklaamide kuvamine lepingu õiguslikul alusel oli vale.

Kolmanda suurima trahvi tiitli (ehk 345 miljon eurot) pälvis noorte seas populaarne sotsiaalmeediavõrgustik TikTok möödunud aasta septembris selle eest, et 2020. aasta juulist kuni detsembrini olid platvormi lapskasutajate isiklikud kontod juba loomisel vaikimisi avalikuks seadistatud. Teave, mis lastele konto tegemisel kuvati, ei sisaldanud läbipaistvat ega selget informatsiooni kasutajate õiguste ja andmete töötlemise laadi kohta, mis tähendas, et alaealise nõusolek ei saanud TikTok-i kasutamisel olla vabatahtlik, nagu andmekaitse regulatsioonid nõuavad. Analüüsides mitmeid tehnilisi elemente, mida TikToki platvorm tollel ajal kasutas, leiti veel, et valikud, mis lapskasutajatele konto privaatsuse seadistamiseks kuvati, julgustasid neid oma kontosid avalikeks jätma, ja postitamise lehel kehtis sama – avalikult postitamine tehti lihtsamaks kui postitamine privaatselt. Laste õiguste

17

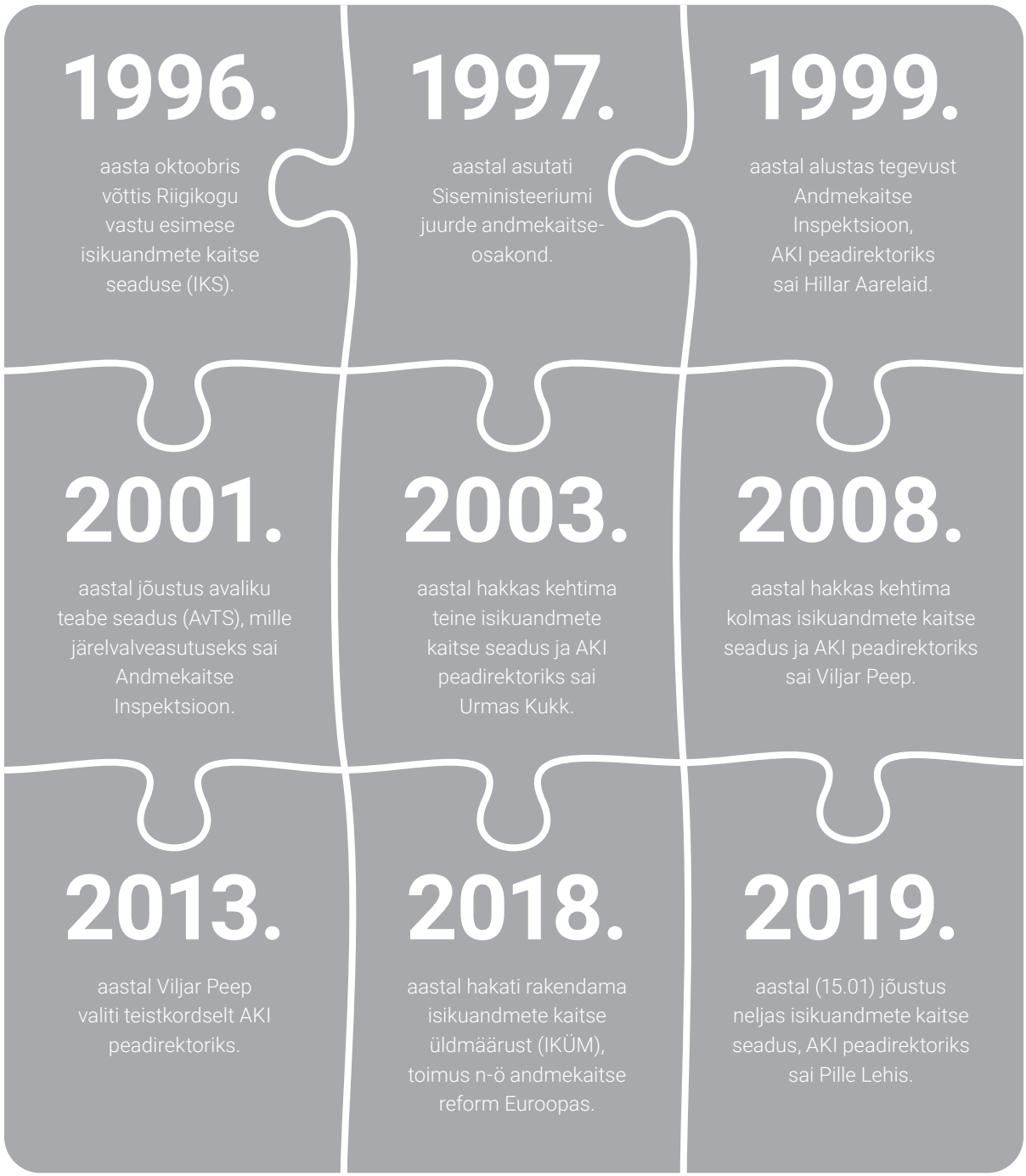
kaitset võetakse andmekaitsemaailmas äärmiselt tõsiselt ja see õigustab ka trahvi suurust. Eraelu puutumatust tugevalt riivavad elemendid TikTok-is tekitasid lapskasutajatele mitmeid riske, sealhulgas kontrolli kaotamise oma andmete üle ning oht sattuda pahatahtlike kasutajate sihtmärgiks.

Väljaspool Iirimaad tegi suurima trahvi Prantsusmaa järelevalveasutus reklaami ja turundusega tegelevale ettevõttele Criteo isikustatud reklaamimise eest. Kaebuse esitas Austrias tegutsev, aga terves Euroopas aktiivne mittetulundusühing None of Your Business (noyb) („pole sinu asi"). Prantsusmaa järelevalveasutus leidis, et rikuti eelkõige läbipaistvuse ja vastutuse põhimõtet, kuna ettevõte ei olnud võimeline tõendama, et nende kasutajatele oli antud piisavat informatsiooni nende isikuandmete töötlemise põhimõtete, eesmärkide ja õiguste kohta. Ettevõte paigaldas kasutajatele jälgimisküpsised ilma nende teadmata. Kasutaja ei teadnud, et tema andmeid üldse töödeldakse ja milliste partner-ettevõteteni need lõpuks jõuavad. Sellest tulenevalt leidis aset raske rikkumine, mille eest trahviti Criteod 40 miljoni euro eest – see on väike number võrreldes eelnevalt mainitud trahvidega tehnoloogiahiiglaste vastu, kuid suur, võttes arvesse, et Criteo kätes olid 370 miljoni Euroopa liidu kasutaja isikuandmed.

Andmekaitsehuviline võib eeldada, et trahvide laviin ei peatu ka 2024. aastal. Nii suuremate kui ka väiksemate tehnoloogiaettevõtete nimed käivad pidevalt läbi Euroopa Andmekaitsenõukogu ja riiklike järelevalveasutuste päevakajalistest teemadest. Alles novembris tutvustatud Facebooki ja Instagrami uus „maksa või anna nõusolek"- ärimudel tõi kohe pärast avalikustamist endaga mitmeid kaebuseid kaasa. Tähelepanu keskpunktis on samuti tehisintellekti kasutamine. Generatiivsele tehisintellektile ja suurtele keelemudelitele eeldatakse tulevatel aastatel tõsiseid trahve. AI-programmide treeningmudelid on siiamaani olnud läbipaistmatud ja pälvinud eetilisuse-teemalist kriitikat. Mudeleid treenitakse andmetega, mis on avalikult internetis üleval ja mis sisaldavad ka isikuandmeid, kuid need andmed ei pruugi olla tõepärased.

Tehisintellekt annab tihti kasutajate küsimustele vastuseks valeandmeid, tekitades andmekaitseasutuste silmis kahtlusi, et suured keelemudelid, nagu on näiteks ChatGPT, ei austa õigsuse põhimõtet. Olukorra tõsidust tõendavad meetmed, mida Itaalia võttis ChatGPT vastu kasutusele märtsis, kui keelas programmi tegevuse oma riigis paaris kuuks, kuni OpenAI lisas veebilehele privaatsuspoliitika ja täiendas vajalikke kaitsemeetmeid 13–17- aastaste kasutajate turvalisuse tagamiseks. Teenus küll taastati, kuid üldine skeptilisus tehisintellekti toimingute vastu meie andmetega, mis on avalikult veebis kättesaadavad, jäi kumama üle maailma. Tasub silmas pidada, et tulevatel aastatel jõustub Euroopa Liidu õigusraamistikus ka tehisintellektimäärus, mille rikkumine võib kaasa tuua veel märkimisväärseid trahve.

18 Andmekaitse Inspektsioon 25 - kronoloogia



18

Inspektsiooni teenistujate arv
aastate võrdluses

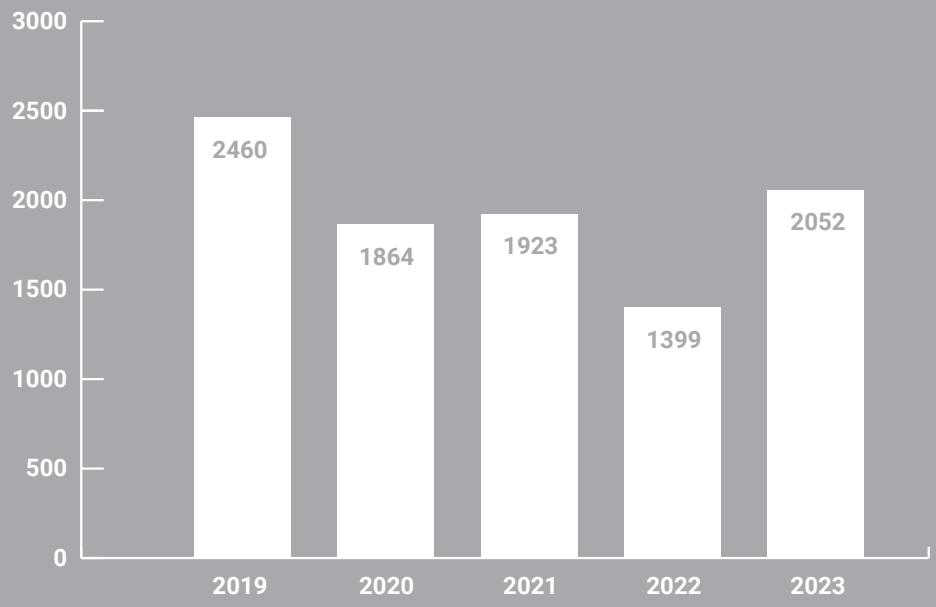
Võrdlusi ajaloost

Kaebused ja vaided	Koolitused	Arvamused õigus-aktide eelnõude kohta
2003 – 147	2003 – 21	2003 – 57
2013 – 550	2013 – 19	2013 – 30
2023 – 1040	2023 – 31	2023 – 82

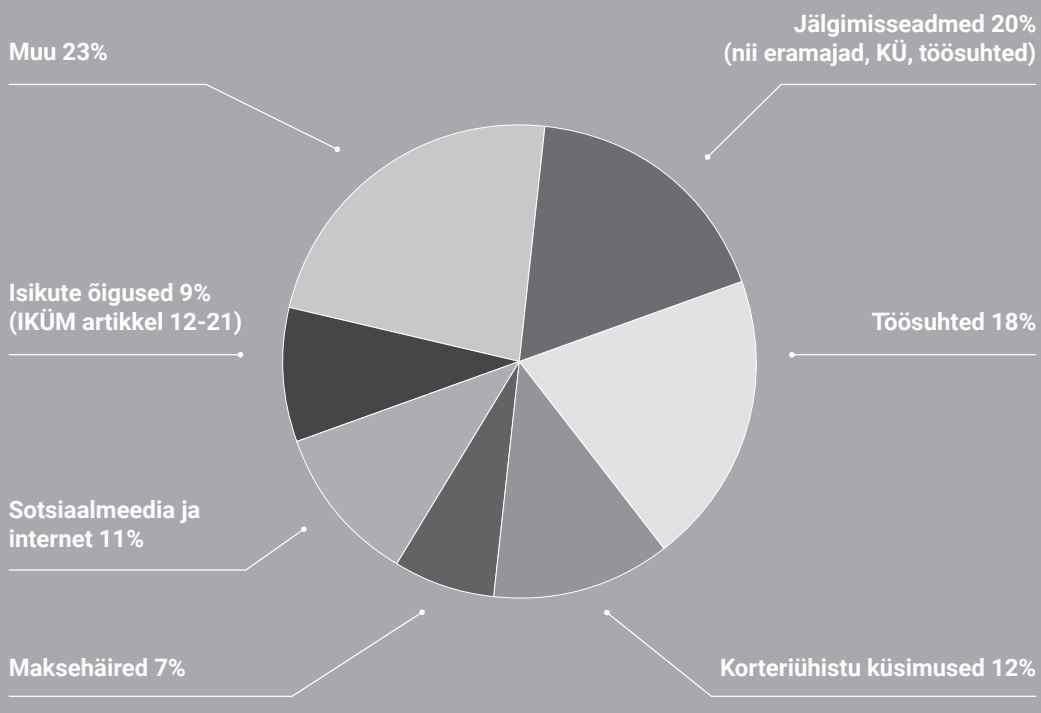
Tegevusnäitajad 2023

2023

Selgitustaotlused, märgukirjad, nõudekirjad, teabenõuded, sh meediapäringute arv

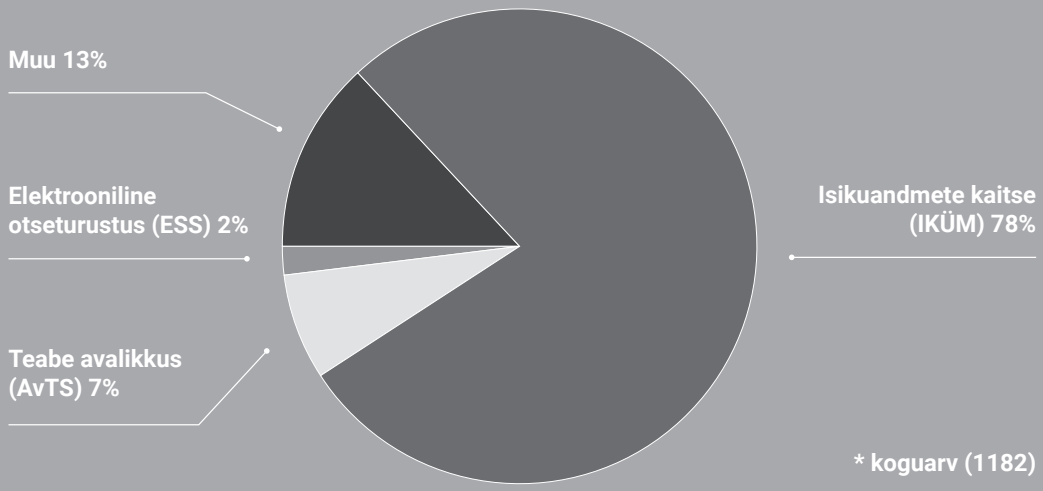


Eraelu kaitse teemalised küsimused



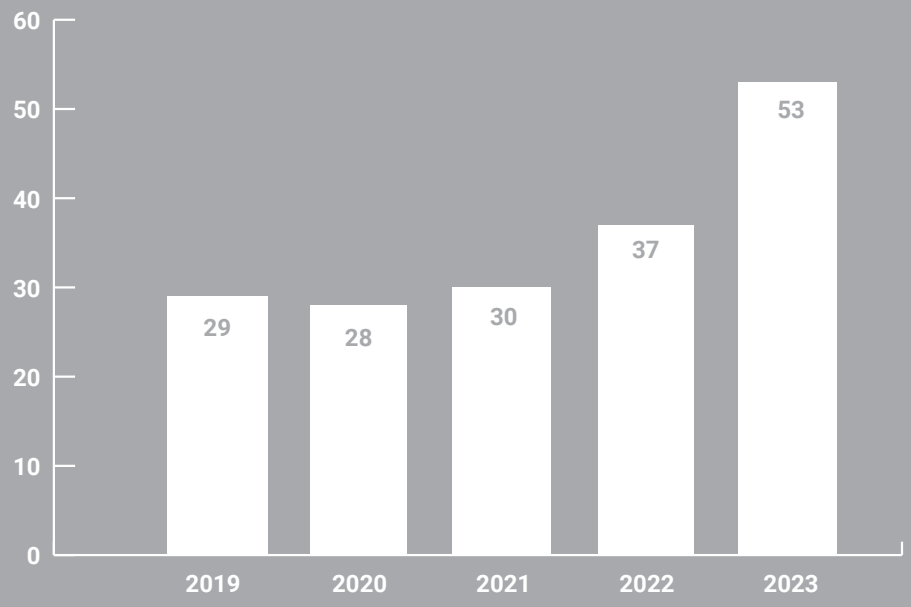
2023

Nõuandetelefonile tulnud kõned

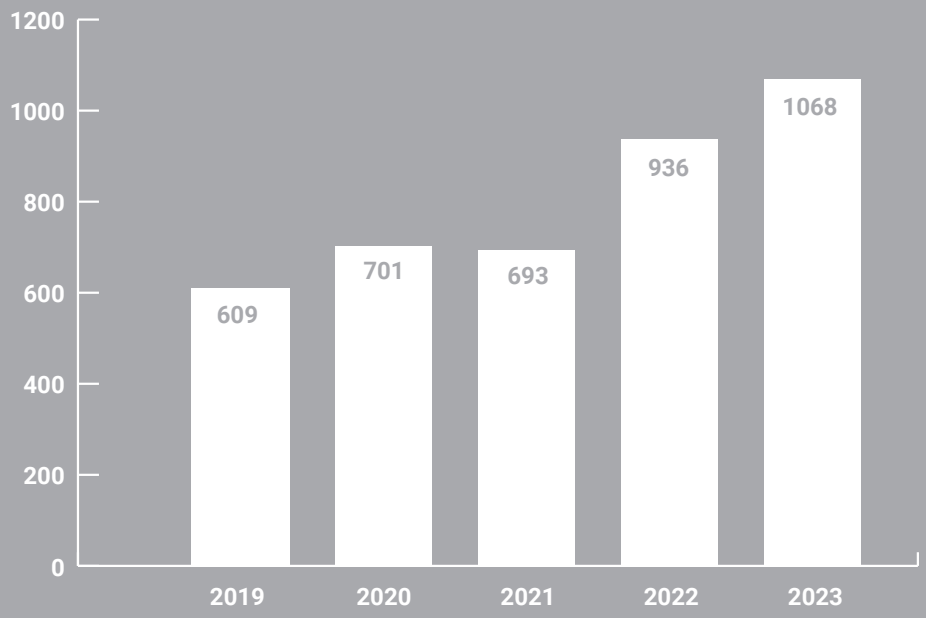


* koguarv (1182)

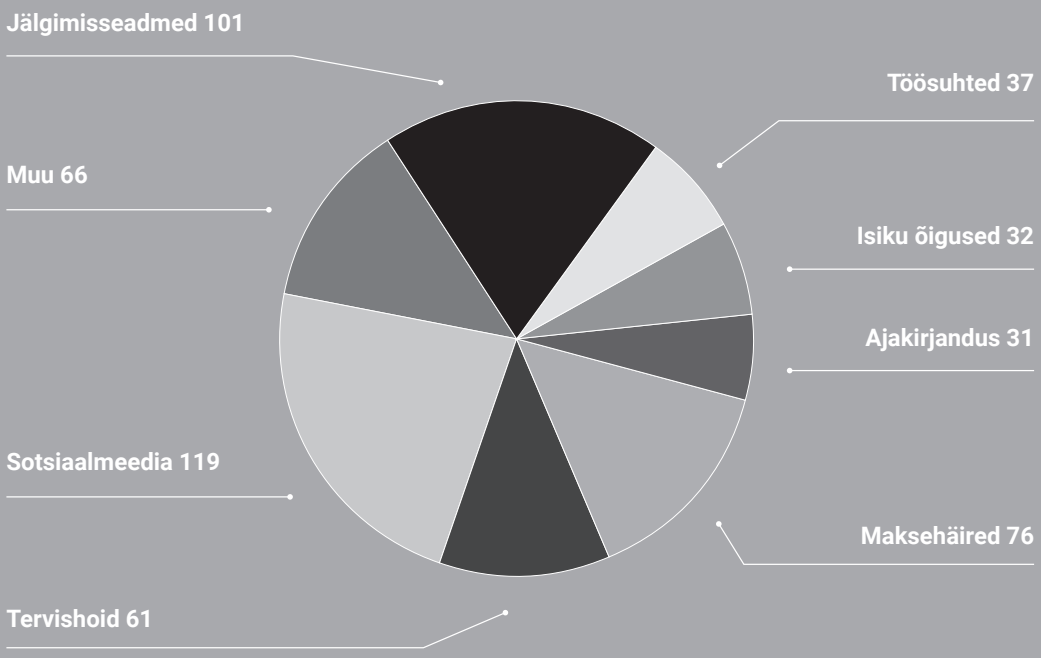
Omaalgatuslikud järelevalvemenetlused



Sissetulnud kaebused ja vaided (sh AKI otsuste osas)



2023. aastal lõpetatud kaebuste menetluste sisuline jaotus

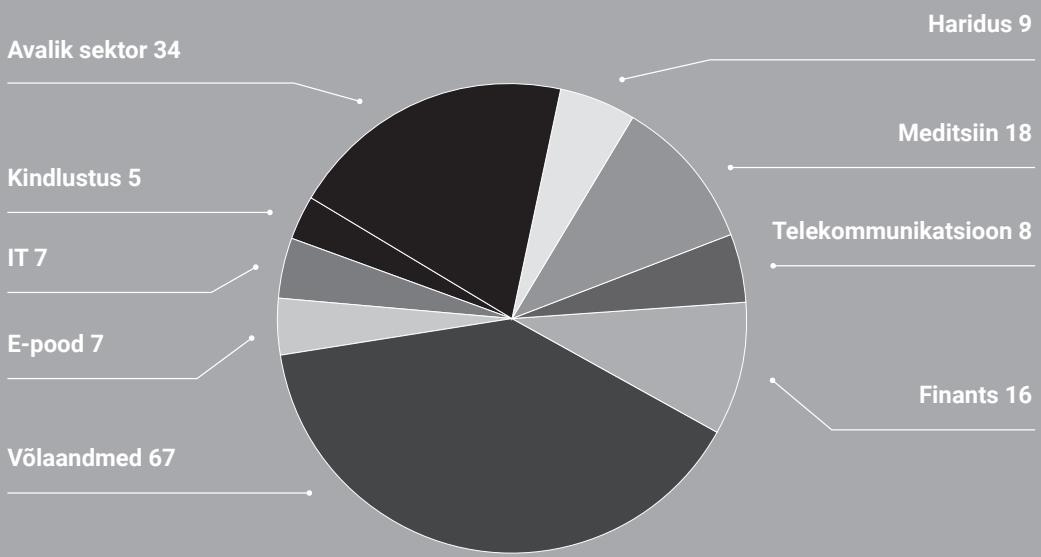


2023

2023. aasta järelevalve tegevus arvudes

Kirjeldus	Arv
tähelepanujuhtimised	93
noomitus ja menetluse lõpetamise teade	63
ettepanekud	213
ettekirjutused-hoiatused	37
väärteomenetlused	8
trahvid ja määratud sunnirahad	12
trahvid ja määratud sunnirahad kokku summas	213 300 €

2023. aasta enim rikkumisteateid saanud valdkondade jaotus



*** puudutatud isikute arv on 322 229**
****rikkumisteadete koguarv 196**

Noppeid numbrites

2023

Produtseeritud andmehäälingu episoodid	8
Läbiviidud koolitused	31
Arvamusavaldused õigusaktide eelnõude osas	82
Poliitikakujundamise uuringute otsused	14
Kohtuvaidlused	26
Osaletud kaasautoritena Euroopa Andmekaitsenõukogu suuniste loomes	4

Suured tänud

aastaraamatu valmimisse oma panuse andmise eest:

Pille Lehis
Viljar Peep
Urmas Kukk
Johan Pastarus
Maarja Kirss
Liisa Ojangu

Merili Koppel
Urmo Parm
Geili Keppi
Kirsika Kuutma
Kadri Levand
Jekaterina Aader
Mari-Liis Uprus

Andra Kask
Stina Veek
Aari Helmelaid
Eleri Pilliroog
Katrin Haug
Marilis Ehvert

Küljendus, illustratsioonid, trükk

Ain Kaldra, Andre Poolma Iconprint OÜ

Fotod

Inga Mattiesen, Postimees, Shutterstock

Andmekaitse Inspektsioon
2023

2023