Andmekaitse krüpto- ja fintechmaailmas

Rahapesu ennetamisel ja takistamisel on andmete töötlemine suurema tähendusega, kui järelevalve seda teadvustab. Kontrollitavat ja läbipaistavat äri aitavad krüptoettevõtetel ajada IT-lahendused.

Krüptost on kahjuks täiesti põhjendamatult saanud justkui sõimusõna. Unustatakse täiesti, et tegu on kasvava majandusharuga, kus Eesti majandus ei peaks jääma kõrvaltvaatajaks ning et krüptoga kaasnevad riskid on tehnoloogiamaailma lahenduste abil edukalt maandatavad.

Andmekaitse nõuete täitmise üle teostab üldjuhul järelevalvet spetsiaalne järelevalveasutus, mille ülesandeks see on seatud. Eestis on selleks Andmekaitse Inspektsioon. Samas leidub aga andmekaitsega seonduvaid nõudeid ka muudes õigusaktides ning andmekaitse nõuete täitmine tõusetub küsimuseks erinevates loamenetlustes – näiteks virtuaalvääringu teenuse pakkumise loa taotlemisel või soovides tegutseda krediidiasutusena. Kuivõrd nende loamenetluste läbiviijaks on aga muud pädevad asutused, – Rahapesu Andmebüroo ja Finantsinspektsioon –, võib tekkida küsimus, kuidas oskavad nemad hinnata isikuandmete töötluse vastavust nõuetele ja lahenduste sobilikkust eesmärgi täitmiseks.

Alustada tuleb sellest, millist eesmärki andmekaitsenõuded üldse täidavad. Tänapäeva maailm on suures osas muutunud digitaalseks, seda eriti krüpto- ja fintechvaldkonnas. Seda olulisemal kohal on andmed, nende töötlemine ja töötlemise eesmärgid. Eeltoodule sarnaselt on lubade menetlemisel sama tähtis tähelepanu pöörata töötlejate tehnilisele ja organisatoorsele võimekusele andmete töötlemisel ehk teisi sõnu kuidas andmeid töödeldakse. Järelevalve peab olema võimeline hindama loataotleja tehnilist ja organisatoorest võimekust andmete töötlemisel ja läbi selle riskide hindamisel.

Andmekaitse kannab mitut eesmärki – ühelt poolt füüsiliste isikute kaitse, teiselt poolt aitab see kaasa rahapesu- ja terrorismi rahastamise tõkestamisele ning lisaks aitab vähendada kahju tekkimise riski. See kõik saab võimalikuks erinevate isikuandmete töötluse kohustuste kaudu – näiteks peavad andmed olema õiged ja täielikud. Samuti peab andmetöötleja teadma, kust andmed tulevad ja kuhu lähevad ning kes ja miks nendega toimetab – seda sarnaselt rahavoogudele, mille puhul peab samuti teada olema, kust raha tuleb, kuhu läheb ning kes ja miks rahaga toimetab. Sellisel juhul tekib ka ülevaade kas kusagil esineb veel muid riske peale andmetöötluse nõuete rikkumise riski.

Seejuures ei ole nõuete täitmine vajalik vaid järelevalve vaatest – selge andmetöötlus aitab leevendada ka andmetöötleja enda riske. Näiteks aitavad eelpool mainitud põhimõtted, mille kohaselt peavad olema andmed õiged ja täielikud, pettusi vältida ja seeläbi võimaliku kahju tekkimise riski vähendada. Kui sul pole andmeid, mis näitaks, kes või kuidas kahju põhjustas, on kahju tekkimise korral raske ka kelleltki kahjuhüvitist nõuda.

Tehnoloogia pole küll mingi võluvits, kuid saab siin paljuski abiks olla. Näiteks saab olenevalt funktsionaalsusest ja võimekusest tehisintellekti rakendada nii isikuandmete kui ka muude andmete töötlemiseks, et andmete töötlejast saaks väärtusliku info valdaja näol esmane ja suurim abikäsi rahapesu ja terrorismi tõkestamisel.

Eeltoodud eesmärgid ei pruugi aga olla nii ilmselged olukorras, kus näiteks Rahapesu Andmebüroo asub loamenetluse käigus küsima, kuidas on reguleeritud isikuandmete töötlus ja andmesubjektide teavitamine. Selgust saaks luua just see sama järelevalvaja, sealhulgas selgitades, milliseid lahendusi ja meetmeid konkreetne loamenetluse läbiviija kohaseks peab. See omakorda nõuab järelevalvelt tugevat pädevust mitte ainult oma valdkonnast lähtuvalt, vaid ka andmekaitsealaseid süvateadmisi. Arusaamist erinevate IT-lahenduste funktsionaalsustest nõuab see nagunii.

LIISI JÜRGEN
VANDEADVOKAAT, PARTNER

(+372) 66 76 440
LIISI.JURGEN@NJORDLAW.EE