Kilvar Kessler: läbimõeldud ja toimiv andmekaitse toetab äriedu

05. aprill 2024

Kliendiandmed ja teabe oskuslik kasutamine võivad ärile anda tohutu konkurentsieelise. IT areng on seda võimalust hüppeliselt kasvatanud. Samaväärselt on aga tõusnud ka küberriskide oht ärile, kliendile ja keskkonnale, kui andmed lekivad või neid kasutatakse muul soovimatul moel. Finantsjärelevalve kogemuse pinnalt annan järgnevalt peamiselt äridele mõtteid paremaks andmekaitseks. Finantssektor toimib põhiliselt klientide usaldusel ning prognoosib just andmete pinnalt riske, hinnastab ja juhib neid.

Proportsionaalsus on märk mõistlikkusest. Oleme kaasajal harjunud, et iga elutahku reguleerivad tuhanded normid. Isegi kui see nii on, siis tuleb reegleid vaadata läbi proportsionaalsuse põhimõtte. See tähendab lihtsustatult seda, millise tugevuse ja ulatusega riik reegleid mingi juhtumi puhul rakendab. Proportsionaalsuse puhul mängivad olulist rolli äri iseloom ja suurus ning seda ka olukorras, kus kohalduvad reeglid on samased. Ettevõtlusvabaduse, konkurentsi ja avalike vahendite efektiivse kasutamise vaatest on küsitav, kas näiteks panga andmekaitse tegevust sättiva paksu reegliraamatu kohaldamine väiksele pagaritöökojale on mõistlik.

Läbimõtlemine toetab äriedu. Ettevõtjal on äri paremaks ajamiseks mõistlik kaardistada äris kasutatavate andmete iseloom, kogus, ajakohasus ning ka see, mis riskid andmetega seonduvad, näiteks soovimatu lekkimine, kadu, muutumine. Läbi tuleks mõelda, miks just sellised riskid, mis võiks olla riski tõenäosus ja selle põhjustatav võimalik kahju.

Seejärel, kui parem pilt ees on, tuleb otsustada, kas talume riski või mitte. Sõltuvalt asjaoludest võib riskiga nõustumine olla täiesti sobiv lahend, kuid negatiivse kahju sündimisel tuleb arvestada tagajärgedega. Riski saab anda üle, näiteks kindlustada või kanda lepinguga teisele isikule. Riski saab ise juhtida näiteks andmete vastuvõtmise, talletamise ning töötlemise korra ja/või tehniliste vahendite kasutamisega. Kokkuvõttes tuleb mõtestada riskikeskkond, riskid kraadida ja juhtida, kusjuures oluline on tagasisidesüsteem, et üldse õigeaegselt aru saada riskikeskkonnast, riskidest ja nende realiseerumisest. Ja veel üks võtmekoht tuleb lahendada – milline peaks olema ettevõtte ja töötajate käitumismudel tegelikkuses, kui risk siiski peaks realiseeruma.

Raske õppustel, kerge lahingus. Nüüd, kui asjad on proportsionaalsuse pinnalt läbimõeldud, tasub neid aeg-ajalt praktikas testida. Kas või avalikkuse ette jõudnud juhtumite eeskujul kolleegidega läbi käia ja arutleda, kas midagi sarnast võib juhtuda ka meie ettevõttes? Kas olemasolevad andmekäsitluse põhimõtted on tegelikkuses toimivad – kes ja millises olukorras teeb mida? Selliselt selguvad nõrkused, mis suunab tagasi asju läbi mõtlema, et andmelekkeks või muuks selliseks probleemiks valmis olla.

Negatiivsest tagajärjest saab võtta maksimumi. Asjad ei kulge alati soovitud rajal, riskid realiseeruvad ja toovad kahju. Infotehnoloogilise riski realiseerumise iseloomulikuks tunnuseks on sündmuse kiirus. Halvemal juhul on tagajärjeks äri lõppemine. Riski realiseerumisel tuleb rakendada ettevõtte vastavad põhimõtted. Iga riskisündmus on detailides unikaalne ning nõuab käitumismudeli vastavat kohandamist. Põhireegel on esmalt selgeks teha riskisündmuse peamised tunnused ja selle kahjulik mõju või selle potentsiaal, samuti esmased kahju vähendavad, pidurdavad ja heastavad meetmed. Seejärel tasub läbi mõelda, kas, keda ning millises ulatuses ja järjekorras teavitada. Suuremad riskisündmused on näidanud, et varajane, aga samas mõistlikult täpne, teatud määral ettevaatav kommunikatsioon aitab pigem kaasa olukorra lahendamisele ettevõtte kasuks.

Riik annab ootused ja tooni. Andmekaitseseadustes kajastub ühiskondlik kokkulepe, sealhulgas arusaamine esmasest riskijaotusest äride, klientide ja muude asjaomaste vahel. Normid on reeglina piisavalt üldised, sest nii säilitatakse paindlikkus käsitleda erinevaid elulisi juhtumeid. Teisalt on äridele vaja selgust normide ja nende rakendamise kohta, et riske juhtida ning seeläbi olla äris efektiivsem. Seega on riigi üheks ülesandeks, arvestades proportsionaalsust ja õigusriigi põhimõtteid, anda selge signaal ootustest. Loomulikult ei ole ootuste sättimine pelk ühepoolne käsk, vaid erinevate sidusrühmadega arutamise optimum, kus lõppsõna jääb normi rakendajale. Normi rakendajal on mõistlik juba varem selgitustööd teha, kuidas ta tulevastele rikkumistele reageerib ehk milline on vastav poliitika.

Riigi selged ootused kaalutuna proportsionaalsusega ning äride läbimõeldud ja -proovitud

riskijuhtimine ka andmekaitse valdkonnas toetavad kokkuvõttes konkurentsi ja kaitsevad tarbijaid.

Finantsinspektsiooni üheks 2024. aasta järelevalvefookuseks on küberkerksus. Finantsvahendajate tugev küberkerksus toetab oluliste finantsteenuste järjepidevat ja turvalist osutamist ning üldist finantsstabiilsust. Finantsinspektsiooni strateegia kohaselt suuname finantsjärelevalve subjekte kasutama rohkem digilahendusi ning arvestades proportsionaalsuse põhimõtet soovime, et finantsvahendajatel on tõhusalt toimivad riskipõhised digilahendid riskide kontrollimiseks.

- Finantsinspektsiooni järelevalvefookus 2024
- Finantsinspektsiooni strateegia 2022–2025

Kilvar Kessler

Teavita mind, kui sisu muutub