Juhend ettevõtjale: viis sammu, kui ettevõtet ähvardab GDPR trahv

1 year tagasi Autor: AM

Isikuandmete kaitse üldmääruse (GDPR) rikkumise eest on ettevõtjaid ja riigiasutusi trahvitud Euroopa Liidus kokku 4,4 miljardi euroga. Trahve määratakse enim sellistes valdkondades nagu kaubandus, meedia ja telekommunikatsioon, finantsteenused, tervishoid aga ka avalikus sektoris, tõi välja advokaadibüroo Hedman isikuandmete kaitse ekspert Andres Ojaver.

Rikkumistest enamlevinud on isikuandmete kaitse eksperdi sõnul andmepüük või -vargus pahalaste poolt, samuti arvutikontode volitamata kasutamine ja teenuste peatamine, aga ka näiteks teadmatusest või tahtlusest põhjustatud inimeste andmete väärkasutamine. “Kui ettevõttel tekib kahtlus, et inimeste andmed on sattunud ohtu, tuleb tegutseda kiirelt ja kindla plaani alusel, sest tagajärjed võivad olla tõsised nii kopsaka trahvi kui ka tegevuse peatamise ja mainekahju näol,” selgitas Andres Ojaver.

Advokaadibüroo Hedman isikuandmete kaitse ekspert pakkus välja ka kiirreageerimise plaani, et võimalikke kahjusid minimeerida.

1. Tuvastamine ja võimalikult kiire peatamine

Rikkumise avastamisel on kõige olulisem edasise kahju kiire vältimine. “Tuleb võimalikult täpselt selgeks teha, millised andmed on puudutatud ja kui suures mahus. Kui koheselt ei ole selge, kas turvaintsidendi puhul on isikuandmed mõjutatud või mitte, tuleb eeldada, et on mõjutatud,” soovitas Ojaver ning tuletas meelde, et kui andmeid on võimalik otseselt või kaudselt seostada konkreetse inimesega, on tegemist isikustatud andmetega ja need on GDPRi terava tähelepanu ja kaitse all.

2. Uurimise meeskonna kokku panemine

Ettevõttes tuleb juba eelnevalt kokku leppida, kes vastutavad rikkumise avastamisel selle uurimise eest. Samuti tasub kaaluda ka väliste nõustajate kaasamist, näiteks õiguseksperdid ja IT-spetsialistid on abiks juhtudel, kui kahju piiramiseks tuleb ettevõtte teenused piirata või peatada.

3. Dokumenteerimine ja registri pidamine

Rikkumise dokumenteerimine on vajalik nii põhjuste selgitamiseks ja kahju ulatuse tuvastamiseks kui ka hilisemaks koostööks Andmekaitse Inspektsiooni või Riigi Infosüsteemi Ametiga. Kõigi isikuandmetega seotud juhtumite üksikasjad peaks salvestama selleks ettenähtud registris ning järelevalveasutusel on õigus nõuda registriga tutvumist.

4. IT-analüüs

IT-analüüsi käigus peaks IT-meeskond andma hinnangu, kuidas isikuandmetega seotud intsident aset leidis, tuues välja põhjused ja haavatavused ning mõjutatud andmed või süsteemid. Võimaluse korral tuleb koguda ka juriidilisi tõendeid võimaliku õigusvaidluse jaoks.

5. Teavitamine

Teatud juhtudel on ettevõtjal kohustus teavitada isikuandmetega seotud turvaintsidendist Andmekaitse Inspektsiooni ning seda tuleb teha 72 tunni jooksul. Kui ettevõte pakub digitaalset teenust, sideteenust või usaldusteenust e-identimise ja e-tehingute näol, on kohustuslik ka Riigi Infosüsteemi Ameti teavitamine. Teatud juhtudel tuleb teavitada ka inimesi, keda rikkumine puudutab.

Võimaliku kahju ennetamiseks soovitas ekspert ettevõtjatel ja riigiasutustel investeerida andmete turvalisusesse juba ennetavalt. “Kõik algab korrastatud ülevaatest, miks ja milliseid isikuandmeid töödeldakse, seda nõutakse igalt ettevõttelt ja riigiasutuselt. Ülevaadete koostamiseks ja hoidmiseks saab näiteks kasutada Eestis loodud tarkvaralahendust GDPR Register, mis on välja töötatud selleks, et aidata vältida vigu andmete töötlemisel,” soovitas Andres Ojaver.

Eesti iduettevõtte poolt loodud GDPR Register on arendatud koostöös IT ekspertidega ning teeb GDPRi nõuete järgimise lihtsaks ja loogiliseks, aidates hallata GDPR regulatsiooniga kaasnevaid toiminguid ja dokumente, tagades ka nende nõuetele vastavuse.

Sel aastal Eestis oma 30. tegutsemisaastat tähistav äri- ja ühinguõigusele spetsialiseerunud advokaadibüroo toetab oma kliente investeeringute kaasamisel, osanike- ja aktsionärisuhete korraldamises, tehnoloogiaõiguses, ühinemistel ja ülevõtmistel, äriühingute piiriülestel liikumistel, IT-õiguses ning andmekaitse ja intellektuaalomandi küsimustes.

- Lahendused

Pilt