Ekspert selgitab, kuidas kaitsta isikuandmeid

3 aastat tagasi Autor: AM

Kohanemise aeg Euroopa Liidu isikuandmete kaitse üldmäärusega (GDPR) on olnud juba piisavalt pikk ning enam ei piisa vabandusest, et ei ole jõutud teemaga tegeleda. Advokaadibüroo Hedman Partners isikuandmete kaitse ekspert toob välja sagedasemad rikkumised ja nende ennetamise võimalused.

Pahatahtlik tegevus internetis ning teadmatusest või hooletusest tekkivad intsidendid inimeste andmetega on Hedman Partnersi isikuandmete kaitse eksperdi Andres Ojaveri sõnul jätkuvalt kasvavas trendis: „Isikuandmete kasutamine kannab endas alati riske – paljud tänapäevased tooted ja teenused nii avalikus kui erasektoris on sageli seotud isikuandmete töötlemisega, mistõttu tuleb tegeleda ka kaasnevate kohustustega. Samas näitab Euroopa menetluspraktika, et järelevalveasutused võtavad sanktsioneerimisel arvesse organisatsiooni pingutusi rikkumisele eelnevalt ja selle lahendamise ajal ehk väga oluline on, kuidas oma kohustusse suhtutakse.“

Üheks sagenevaks rikkumiseks on ebapiisavad tehnilised ja organisatsioonilised meetmed infoturbe tagamisel. „Sellised puudused võivad ilmneda nii pahatahtlike rünnete kaudu infosüsteemidele kui ka organisatsiooni enda poolt põhjustatud andmelekete korral. Samas esineb ka juhtumeid, kus järelevalveasutus või inimene ise avastab kasutamise käigus, et pääseb ligi võõra isiku eraelulisele teabele,“ tõi Ojaver näited rikkumistest.

2020. aasta GDPR trahvide statistika Euroopas näitab, et infoturbe meetmete ebapiisavuse tõttu määrati üle saja rahatrahvi, millest kümmekond ulatus miljoni euroni. Kolm suurimat trahvi ületasid ka kahekümne miljoni euro piiri. „Kordades rohkem on aga juhtumeid, kus järelevalveasutus on teinud ettekirjutuse mõne tegevuse lõpetamiseks või ärimudeli muutmiseks, mis võib olla rahatrahvist suuremagi mõjuga. Lisaks võib juhtuda, et toimunust puudutatud isikud esitavad kahjunõude,“ selgitas Ojaver.

Eestis aset leidnud rikkumised näitavad selgelt, et nende mõju võib olla ulatuslik. Hiljuti tegi Andmekaitse Inspektsioon ettekirjutuse e-apteekidele, sundides sulgema võimaluse osta retseptiravimeid teisele isikule. „Isikukoodi teades oli võimalik vaadata võõrastele inimestele välja kirjutatud retsepte ning kuna isikukoodi teadasaamine ei ole enamasti keeruline, võis see riivata inimese privaatsust. Seetõttu peab hoolikalt jälgima, mida isikukoodi teadmisega infosüsteemides teha lubatakse,“ rõhutas Hedman Partners isikuandmete kaitse valdkonna ekspert.

Sagenenud on ka ründed infosüsteemidele, mille eesmärgiks on näiteks andmete krüpteerimine ja algse olukorra taastamise eest lunaraha nõudmine või süsteemide töö halvamine. On esinenud ka isikuandmete lihtsalt avalikustamise juhtumeid.

Mida teha, et isikuandmed oleksid kaitstud?

Ennetamaks andmekaitsealaseid rikkumisi tuleb teemale läheneda süsteemselt ja terviklikult. Isikuandmete kaitse ekspert Andres Ojaver soovitas seada prioriteete ja saada aru protsesside omavahelistest sõltuvustest.

Kogu maailmas kehtestatakse Ojaveri sõnul Euroopa eeskujul järjest tugevamaid andmekaitsenõudeid ning rahvusvahelises konkurentsis on nende rakendamine juba pigem tava kui erand. „Seetõttu tajuvad organisatsioonid seda üha enam toodete ja teenuste väärtuse osana ning rikkumisi selles vallas mõõdetakse mitte ainult rahatrahvina, vaid ka mainekahjuga,“ tõi Ojaver välja.

Suureks väljakutseks on tema sõnul nö köögipoole koristamine ehk tuleb põhjalikult üle vaadata, mida ja kuidas on seni tehtud - mittevajalik andmestik tuleb kustutada, juurdepääsud vajaduspõhiselt piirata ja rakendada turvameetmed väliste rünnakute vastu.

- **Isikuandmete ülevaade peab olema täpne ja selge**

Igal organisatsioonil peab olema selge pilt sellest, milliseid andmeid milleks kasutatakse.

- **Mõtle läbi, milliseid andmeid ja milleks vaja on**

Isikuandmete kaitse ekspert soovitab mitte alustada andmete kogumist kui pole päris selge, kas neid ikka vaja on. Üleliigsed andmed suurendavad intsidendi korral rikkumise ulatust ja mõju inimeste eraelule. Hea meetod selleks on andmekaitse mõjuhinnangu koostamine.

- **Planeeri andmekaitse põhimõtted oma toodetesse või teenustesse (privacy by design ehk lõimitud andmekaitse)**

Mõjuhinnangust selgunud nõuded saab sageli täita toote või teenuse sellise disainimisega, kus arvestatakse andmekaitse põhimõtetega. Näiteks on teatud veebilahenduste puhul mõistlik kasutada isikute autentimist, andmete kogumisel vältida üleliigsete andmeväljade tekitamist ning kohustuslike ja vabatahtlike väljade selget eristamist.

- **Pane kirja selges ja lihtsas keeles, mida isikuandmetega teed (Privacy Notice ehk Privaatsusteade)**

Lisaks sellele, et andmete töötlemise läbipaistvus on juriidiline nõue, aitab see korrastada organisatsiooni mõtteid. Kui püüad oma kliendile selgitada ausalt, mida tema eraeluliste andmetega teed, võib selle käigus esile kerkida probleemseid kohti, mis vajavad lahendamist.

- **Lase oma tooteid või teenuseid sõltumatul eksperdil lõppkasutaja vaates testida**

Selliselt on võimalik saada raport puudustest, mis kannavad endas andmekaitse riske koos selgete juhistega eksperdilt, kes igapäevaselt andmekaitsega tegeledes oskab ära tunda olulised puudused ning need ka prioriteetide alusel ritta seada.

- **Täida teavitamiskohustus Andmekaitse Inspektsioonile, kui juhtub halvim**

Arvesta ka sellega, et küberintsidendi korral aitab Riigi Infosüsteemi Amet. Hea näide hiljutisest koostööst seostub tuntud automüüjale tehtud küberrünnakuga.

- **Loo infoturbe tervik**

Infoturve on üks olulisemaid andmekaitse komponente. Füüsilised, organisatsioonilised ja infotehnoloogilised turvameetmed on kasulikud kui kõne all on ärisaladuse kaitse, kuid need peavad olema kindlasti rakendatud, kui tegemist on isikute eraeluliste andmete kasutamisega. Vastavalt andmete iseloomust tulenevatele ohtudele tuleb valida infoturbe meetmete tase.

- Lahendused
- Turvalisus