



ANDMEKAITSE INSPEKTSIOON

Lp Pärnu Linnavalitsus

30.10.2024 nr 2.1.-4/24/888-2764-1

Tähelepanu juhtimine

Andmekaitse Inspeksioon (AKI) algatas seire, et saada ülevaade, kas ja kuidas täidetakse avalikus sektoris isikuandmete kaitse üldmääruses (IKÜM) sätestatud kohustust dokumenteerida kõik isikuandmetega seotud rikkumised.

Seire raames küsisime Teilt infot selle kohta, kuidas dokumenteerite isikuandmete töötlemisega seotud rikkumisi ja palju on asutuses olnud rikkumisi. Seiresse valiti 11 avaliku sektori asutust, sh KOV-id.

Seejärel võrreldi esitatud vastuseid AKI-le esitatud rikkumisteade arvu ja Riigi Infosüsteemi Ameti küberintsidentide registri väljavõtetega, et tuvastada, kas intsidentide sisus oli kattuvusi või erinevusi. Kokkuvõttes oli avaliku sektori asutustel probleeme nii isikuandmete rikkumistega seotud intsidentide tuvastamisel kui ka dokumenteerimisel. Lisaks oli mitmel asutusel raskendatud rikkumistega seotud detailse ülevaate väljastamine AKI-le. 11-st asutusest kahel oli esitatud andmete põhjal IKÜM nõuete täitmine korras.

Seire tulemusel juhime Teie tähelepanu alljärgnevale.

Vastavalt IKÜM artikkel 4 lg 1 p 12-le on isikuandmetega seotud rikkumine turvanõuete rikkumine, mis põhjustab edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotamineku, muutmise või loata avalikustamise või neile juurdepääsu. Näiteks võivad sellised rikkumised olla ametnike poolt tehtud volitamata päringud erinevatesse registrisse (nn uudishimupäringud), õigustamatu isikuandmete avaldamine (nt avalikus dokumendiregistris, süsteemis või kodulehel isikuandmete avaldamine) või küberründe tagajärjel hävitatud või lekkinud andmed.

Intsidentiga on ka tegemist siis, kui toimub turvaintsident, mille tõttu ei ole isikuandmed teatud aja jooksul kättesaadavad, kuna andmetele juurdepääsu puudumine võib märkimisväärselt mõjutada füüsiliste isikute õigusi ja vabadusi. Selguse huvides olgu öeldud, et kui isikuandmed ei ole kättesaadavad kavandatud süsteemihoolduse tõttu, ei ole see turvanõuete rikkumine.

Vastavalt IKÜM artikkel 33 lõikele 5 on vastutaval andmetöötlejal isikuandmete seotud rikkumise korral kohustus intsident dokumenteerida. Rikkumiste dokumenteerimine on seotud IKÜM artikli 5 lõikes 2 sätestatud vastutuse põhimõttega. Kuivõrd andmetöötleja peab kõik rikkumised dokumenteerima, on soovituslik pidada sisemist registrit rikkumiste kohta. Registri ülesehitus on

iga andmetöötleva enda otsustada, kuid teatavad elemendid peavad siiski olema olemas, näiteks IKÜM artikli 33 lõikes 5 on sätestatud, et kirjas peavad olema rikkumise põhjused, toimunu kirjeldus, mõjutatud isikuandmed ja võetud parandusmeetmed.

Eelnevast selgitusest tulenevalt juhime tähelepanu, et võtaksite vastu vajalikud meetmed (nt koolitada töötajaid isikuandmete seotud rikkumiste tuvastamisel ja kirjeldamisel või vajadusel täiendada sisedokumente) IKÜM nõuete korrektseks täitmiseks.¹

Tuvastasime, et dokumenteerite isikuandmetega seotud rikkumisi asutuse dokumendiregistri osana, kuid soovitame tungivalt kaaluda alternatiivset võimalust, sest vastasel juhul võib tekkida oht, et asutusel puudub selge ja detailne ülevaade isikuandmetega seotud rikkumistest.

IKÜM artikli 33 lõikes 5 seonduv dokumenteerimise kohustus on seotud artikli 5 lõikes 2 sätestatud vastutuse põhimõttega. Nii teavitamisele mittekuuluvate kui ka teavitamisele kuuluvate rikkumiste registreerimise eesmärk on samuti seotud vastutava töötleva isikuandmete kaitse üldmääruse artiklist 24 tulenevate kohustustega ning järelevalveasutus võib asjaomaseid kandeid näha nõuda. Seetõttu julgustatakse vastutavaid töötlevaid looma asutusesisest rikkumiste registrit hoolimata sellest, kas neil on rikkumisest teatamise kohustus või mitte

Vastutav töötleva võib otsustada dokumenteerida rikkumised isikuandmete töötlemise toimingute registreerimise raames, mida tehakse vastavalt IKÜM artiklile 30. Eraldi registrit ei ole vaja, kui rikkumisega seotud teave on selgelt tuvastatav ja taotluse korral saab teha registrist rikkumisega seotud andmete väljavõtte. Registri ülesehitus on iga andmetöötleva enda otsustada, kuid teatavad elemendid peavad siiski olema olemas, näiteks IKÜM artikli 33 lõikes 5 on sätestatud, et kirjas peavad olema rikkumise põhjused, toimunu kirjeldus, mõjutatud isikuandmed ja võetud parandusmeetmed. Register on asutusele abiks andmekaitsete riskide haldamisel, aidates tuvastada korduvaid mustreid ja suunata tegevusi kolleegide teadlikkuse suurendamiseks.

Dokumendihaldussüsteem (DHS) on avalikus sektoris üks variantidest isikuandmete rikkumistega seotud dokumentide koondamiseks aga peab samal ajal võimaldama täita IKÜM-ist tulenevaid kohustusi sh analüüsida ja täpsemat ülevaadet anda asutuste isikuandmetega seotud rikkumiste kohta. DHS-i kasutamine isikuandmete rikkumistega seotud registri pidamiseks avalikus sektoris võib olla ebasobiv, sest probleeme võib esineda andmete jälgitavuse, haldamise ja säilitamise nõuetega, mis suurendab õiguslike riskide tekkimise võimalust. Seetõttu tuleks kasutada lahendusi, mis on loodud andmekaitse vajadusi arvestades.

Käesolevale tähelepanu juhtimisele inspeksioon vastust ei oota.

Lugupidamisega

Eleri Pilliroog
andmeturbe ekspert
peadirektori volitusel

¹ Täiendavalt soovitame tutvuda ka Euroopa Andmekaitsekoostöögrupi suunistega 9/2022, mis käsitlevad isikuandmetega seotud rikkumisest teatamist isikuandmete kaitse üldmääruse alusel. ([Versioon 2.0, vastu võetud 28. märtsil 2023](#))