ANDMEKAITSE INSPEKTSIOON

Lp Rahandusministeerium

30.10.2024 nr 2.1.-4/24/888-2762-1

Tähelepanu juhtimine

Andmekaitse Inspektsioon (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 rikkumisteadete arvuga 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.

Olete jätnud isikuandmetega seotud intsidendi(d) korrektselt tuvastamata ja dokumenteerimata.

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, kaotsimineku, 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.

Intsidendiga 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.

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]

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

Lisaks nendele üksikasjadele on soovitatav, et vastutav töötleja dokumenteeriks ka rikkumisele reageerimiseks tehtud otsuste põhjendused. Eelkõige tuleks asjaomase otsuse põhjendused dokumenteerida juhul, kui rikkumisest ei teatata. Seejuures tuleks esitada ka põhjused, mille alusel vastutav töötleja leiab, et rikkumisest ei tulene tõenäoliselt ohtu üksikisikute õigustele ja vabadustele. Alternatiivina, kui vastutav töötleja leiab, et isikuandmete kaitse üldmääruse artikli 34 lõike 3 mis tahes tingimus on täidetud, peaks ta olema suuteline esitama selle kinnituseks piisavaid tõendeid.

IKÜM 33 ja 34 nõuete paremaks täitmiseks oleks hea, kui andmetöötleja oleks sisemistes kordades või juhendites reguleerinud intsidentide haldamise protsessi, millega on kehtestatud kord, mida järgida pärast rikkumise avastamist, sealhulgas juhised selle kohta, kuidas intsidendi ulatust piirata, seda ohjata ja andmed taastada ning kuidas ohtu hinnata ja rikkumisest teatada.

Eelnevast selgitusest tulenevalt juhime tähelepanu, et kontrolliksite üle, et kõik intsidendid oleksid korrektselt dokumenteeritud ning võtaksite vastu vajalikud meetmed (nt teeksite vastavad muudatused töösisekorras ja uuendaksite vastavaid dokumente, kus sisalduvad isikuandmetega seotud intsidendid) IKÜM nõuete korrektseks täitmiseks.

Tuvastasime, et olete varem dokumenteerinud isikuandmetega seotud rikkumisi asutuse dokumendiregistri osana.

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 töötleja isikuandmete kaitse üldmääruse artiklist 24 tulenevate kohustustega ning järelevalveasutus võib asjaomaseid kandeid näha nõuda. Seetõttu julgustatakse vastutavaid töötlejaid looma asutusesisest rikkumiste registrit hoolimata sellest, kas neil on rikkumisest teatamise kohustus või mitte

Vastutav töötleja 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 andmetöötleja enda otsustada, kuid teatavad elemendid peavad siiski olemas olema, 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 andmekaitseliste 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

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

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. Tunnustame otsust alates 2023. aastast võtta kasutusele alternatiivne variant isikuandmete rikkumiste dokumenteerimiseks.

Käesolevale tähelepanu juhtimisele inspektsioon vastust ei oota.

Lugupidamisega

Eleri Pilliroog
andmeturbe ekspert
peadirektori volitusel