Andmekaitse Inspektsioon viis läbi seire huvi- ja spordikoolide isikuandmete rikkumiste registreerimis nõuete täitmisel

Andmekaitse Inspektsioon (AKI) viis perioodil oktoober kuni november 2026 läbi seire, et saada ülevaade, kas ja kuidas täidetakse huvi- ja spordikoolides isikuandmete kaitse üldmääruses (IKÜM) sätestatud kohustust dokumenteerida kõik isikuandmetega seotud rikkumised. Seire raames küsiti organisatsioonidelt infot selle kohta, kuidas dokumenteeritakse isikuandmete töötlemisega seotud rikkumisi ja kui palju on organisatsioonis rikkumisi olnud. Kaasasime seires nii avaliku kui erasektori organisatsioone, et tagada terviklik ülevaade.

Seiresse valiti 13 huvi- ja spordikooli. Vastused saatsid 11 seiratavat - Tallinna Huvikeskus Kullo, IZUM Huvikool, Tartu I Muusikakool, Tartu Loodusmaja, Audentese Spordikool, Spordiklubi Nord, Tartu Spordiseltsi Kalev Spordikool, SK FC Levadia Jalgpallikool, Saaremaa Spordikool, Viljandi Spordikool, Paide Kunstikool. Vastamismääraks seega 85%. Huvi- ja spordikoolidelt saadud vastuseid võrreldi AKI-le esitatud rikkumisteadete väljavõtetega, et tuvastada, kas intsidentide sisus oli erinevusi.

Kokkuvõttes ei tuvastanud AKI suuri probleeme isikuandmete rikkumistega seotud intsidentide dokumenteerimisel. Kahjuks oli mitmel organisatsioonil puudusi rikkumiste registrite kirjeldamises ja raskusi detailse ülevaate väljastamisel AKI-le. Seire tulemusel selgus, et enamikus kontrollitud organisatsioonides ei olnud isikuandmetega seotud rikkumisi tuvastatud. Rikkumisi esines ainult kahes kontrollitud organisatsioonis, sealjuures oli ühest rikkumisest varasemalt teavitatud ka AKI-t. Ühegi organisatsiooni puhul eraldi menetluse alustamist põhjendatuks ei peetud ja ühtegi tähelepanu juhtimist ei tehtud.

Seire täpsemad tähelepanekud ja selgitused

Vastavalt IKÜM-i artikli 4 lõike 1 punktile 12 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 juurdepääsu neile. Näiteks võivad sellised rikkumised olla töötajate tehtud volitamata päringud (nn uudishimupäringud), õigustamatu isikuandmete avaldamine (nt isikuandmete avaldamine avalikus dokumendiregistris, süsteemis või kodulehel) või küberründe tagajärjel hävitatud või lekkinud andmed.

Rikkumisega on tegemist ka siis, kui toimub turvaintsident, mille tõttu ei ole isikuandmed teatud aja jooksul kättesaadavad, kuna juurdepääsu puudumine

andmetele võib märkimisväärselt mõjutada füüsiliste isikute õigusi ja vabadusi. Selguse huvides olgu öeldud, et kui isikuandmed ei ole kättesaadavad kavandatud süsteemihoolduse tõttu, ei ole see käsitletav turvanõuete ehk isikuandmete kaitse rikkumisena.

Vastavalt IKÜM-i artikli 33 lõikele 5 on vastutaval andmetöötlejal isikuandmetega seotud rikkumise korral kohustus intsident dokumenteerida. Rikkumiste dokumenteerimine on seotud IKÜM-i artikli 5 lõikes 2 sätestatud vastutuse põhimõttega. Kuivõrd andmetöötleja peab kõik rikkumised dokumenteerima, on soovituslik pidada sisemist registrit. Nii teavitamisele mittekuuluvate kui ka teavitamisele kuuluvate rikkumiste registreerimise eesmärk on samuti seotud vastutava töötleja IKÜM-i artiklist 24 tulenevate kohustustega ning järelevalveasutus võib asjaomaseid kandeid näha nõuda. Registri ülesehitus on iga andmetöötleja enda otsustada, kuid teatavad elemendid peavad siiski olemas olema, näiteks on IKÜM-i artikli 33 lõikes 5 sätestatud, et kirjas peavad olema rikkumise põhjus, toimunu kirjeldus, mõjutatud isikuandmed ja rakendatud parandusmeetmed.

Lisaks 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.

Oluline on hoida organisatsiooni kontaktandmed ajakohased nii äriregistris, kodulehel kui ka teistes ametlikes kanalites, et vajaduse korral oleks võimalik organisatsiooniga kiiresti ühendust võtta. Seire näitas, et osadel organisatsioonidel on kontaktandmete ajakohasena hoidmisega probleeme. Soovitame igal organisatsioonil veenduda, et nende kontaktandmed on uuendatud ja kehtivad.

IKÜM-i artiklite 33 ja 34 nõuete parema täitmise tagab, kui andmetöötleja on sisemistes kordades või juhendites reguleerinud intsidentide haldamise protsessi. See tähendab, et 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.

AKI tuvastas, et mitmel juhul pidas organisatsioon rikkumiste ülevaateid üldises dokumendiregistris, kuid soovitame tungivalt kaaluda alternatiivset võimalust, sest vastasel juhul võib tekkida oht, et asutusel puudub selge ja detailne ülevaade isikuandmetega seotud rikkumistest.

Dokumendihaldussüsteem (DHS) on 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 võib olla ebasobiv, sest probleeme võib esineda andmete jälgitavuse, haldamise ja säilitamise nõuetega, mis suurendab õiguslike riskide tekkimise võimalust. Seetõttu on soovitatav kasutada lahendusi, mis on loodud andmekaitse vajadusi arvestades.