Valvame, et isikuandmete kasutamisel austatakse eraelu

ning et riigi tegevus oleks läbipaistev

Pärnu Linnavalitsuse suhtes läbiviidud audit isikuandmete kaitseks rakendatud turvameetmete üle

Isikuandmete kaitse seaduse täitmise audit

Tallinn 2011

Teostatud järelevalvest

Eesti kohalikud omavalitsused (edaspidi KOV-id) peavad isikuandmete kaitse seaduse (edaspidi IKS) kohaselt tagama, et inimeste andmed on kuritarvituste eest kaitstud ning infosüsteemid on töökindlad ja turvalised. KOVidel on kohustus kasutada andmekaitse põhimõtete rakendamiseks sobivaid ja efektiivseid meetmeid.

Riikliku järelevalve teostamisel hindab Andmekaitse Inspektsioon, kuidas on korraldatud infoturve[1] ja infoturbe haldussüsteem, mis tagab andmete õigsust ja säilimist ning välistab nende lekkimise. Järelevalve teostamisel arvestatakse isikuandmete kaitse seaduse[2] ja teiste Eesti Vabariigis kehtivate õigusaktide nõudeid.

Seaduse nõuded

IKS § 25 sätestab, et **isikuandmete töötleja on kohustatud kasutusele võtma organisatsioonilised, füüsilised ja infotehnilised turvameetmed isikuandmete kaitseks:**

- andmete tervikluse osas – juhusliku või tahtliku volitamata muutmise eest;
- andmete käideldavuse osas – juhusliku hävimise ja tahtliku hävitamise eest ning õigustatud
- isikule andmete kättesaadavuse takistamise eest;
- andmete konfidentsiaalsuse osas – volitamata töötlemise eest.

Isikuandmete töötleja on isikuandmete töötlemisel kohustatud:

- vältima kõrvaliste isikute ligipääsu isikuandmete töötlemiseks kasutatavatele seadmetele;
- ära hoidma andmete omavolilist lugemist, kopeerimist ja muutmist andmetöötlussüsteemis, samuti andmekandjate omavolilist teisaldamist;
- ära hoidma isikuandmete omavolilist salvestamist, muutmist ja kustutamist ning tagama, et tagantjärele oleks võimalik kindlaks teha, millal, kelle poolt ja milliseid isikuandmeid salvestati, muudeti või kustutati või millal, kelle poolt ja millistele isikuandmetele andmetöötlussüsteemis juurdepääs saadi;
- tagama, et igal andmetöötlussüsteemi kasutajal oleks juurdepääs ainult temale töötlemiseks lubatud isikuandmetele ja temale lubatud andmetöötluseks;

[1] **Infoturve** on riskihalduslik tegevus teabe turvalisuse säilitamiseks vastavalt organisatsiooni tegevuse eesmärkidele, sealhulgas andmekaitse realiseerimise vahend.

[2] Isikuandmete kaitse seadus

- tagama andmete olemasolu isikuandmete edastamise kohta: millal, kellele ja millised isikuandmed edastati, samuti selliste andmete muutusteta säilimise;
- tagama, et isikuandmete edastamisel andmesidevahenditega ja andmekandjate transportimisel ei toimuks isikuandmete omavolilist lugemist, kopeerimist, muutmist või kustutamist;
- kujundama ettevõtte, asutuse või ühenduse töökorralduse niisuguseks, et see võimaldaks täita andmekaitse nõudeid.

Füüsilised infotehnilised turvameetmed (nt lukustatavad uksed, signalisatsioon, trellid jms) ja **infotehnilised turvameetmed** (peamiselt tarkvara ja riistvara) peavad takistama selleks volitamata isikute juurdepääsu andmetele. Volitatud töötaja juurdepääsu korral peab süsteem jätma „logiraamatusse" jälje selle kohta, kes, millal ja milliseid töötlusoperatsioone on teinud. **Organisatsioonilised turvameetmed -** Töö sisekorraeeskirjas ja töölepingutes tuleb täpselt sätestada, milliseid andmeid, mis eesmärgil jne võib isikuandmete töötaja alluvuses töötav isik töödelda.

Puudujäägid Pärnu Linnavalitsuses isikuandmete töötlemisel

Teostatud järelevalve käigus Pärnu Linnavalitsuse infosüsteemide üle tuvastati puudused isikuandmete töötlemisel. Tähelepanuta on jäetud isikuandmete kaitse seaduse § 25-s sätestatud kohustused[3] - isikuandmete organisatsioonilised, füüsilised ja infotehnilised turvameetmed.

Puudujäägid seisnevad eeskätt selles, et tagamata on isikuandmete kaitse organisatsioonilised-, füüsilised- ja infotehnilised turvameetmed. Nimetatud turvameetmed on **kohustuslikud rakendada kõikide riigi ja kohaliku omavalituse andmekogude pidamise puhul.**

Pärnu Linnavalitsuses kasutuselolevad andmebaasid on loodud Microsoft Office Exceli keskkonnas, mis ei taga ülaltoodud nõuete rakendamist. Andmekaitse Inspektsiooni hinnangul kasutatakse süsteemi, mis ei ole andmekogude pidamiseks, andmete turvalisuse seisukohast, sobiv.

Ettekirjutuse sisu

[3] Säte on toodul ülal täistekstiga

Pärnu Linnavalitsus peab võtma kasutusele infosüsteemid, mis tagaksid järgmise:

kõikidest andmete vaatamise, muutmise, kustutamise, edastamise jmt juhtudest peavad säilima logifailid (arvuti või infosüsteemi rakenduse tegevuse päevik), mille järgi on võimalik **tagantjärele hinnata, kes, millal, milliste andmetega, mida ja miks tegi.** Logifailid päevad säilima viisil, mis tagab nende käideldavuse ning, et nende üle oleks võimalik teostada järelevalvet.

Et andmete leke, rikkumine või kättesaamatus ei tabaks ootamatult, on vaja andmeturbega tegeleda terviklikult. Lisaks infotehnoloogiliste süsteemide kaitsmisele tuleb kaitsta ruume, paberdokumente ning koolitada inimesi. Ükski turvameede ei taga sajaprotsendilist turvalisust, kuid süsteemne andmeturbega tegelemine vähendab juhtumite tekkeriski.

Auditi läbiviija:

Boris Põldre
Andmekaitse Inspektsiooni
I järelevalveosakonna andmeturbeekspert