ANDMEKAITSE INSPEKTSIOON

Eestimaa haiglad 27.11.2018 nr 2.3.-3/18/3783

Ringkiri lõimitud andmekaitse ning logide kohta

Teatavasti hakkas käesoleva aasta mai kuust kehtima isikuandmete kaitse üldmäärus, mis sätestab muuhulgas andmetöötleja vastutuse põhimõtte. Andmetöötleja peab jälgima nii õigusnorme, õiguspraktikat kui ka infotehnilist arengut ning sellest tulenevaid võimalusi ja ohte.

Eraelu kaitset ei saa tagada ainult andmetöötluse õigusnormistikule vastavuse abil, vaid see peab tulenema organisatsiooni töökorraldusest ning infotehnoloogiast. Mida tundlikumad andmed, seda tõhusam peab olema kaitse. Lõimitud andmekaitse ei ole mitte niivõrd õiguslik mõiste, kuivõrd mõtteviis ja organisatsioonikultuur.

Lõimitud andmekaitse rakendamisel tuleb lähtuda järgmistest põhimõtetest:

1. Ennetamine - ohte tuleb ette näha ja ära hoida enne nende toimumist. Andmekaitse on organisatsiooni tegevusse ning tema infosüsteemidesse sisse ehitatud enne isikuandmete töötlemisega alustamist.
2. Korrapärasus ja süsteemsus - andmekaitse on sisse ehitatud infosüsteemide disaini, arhitektuuri olles osa tuumfunktsionaalsusest. Andmetöötleja hindab korrapäraselt võimalikke ohte ning rakendab vastavalt olukorrale täiendavaid kaitsemeetmeid.
3. Turvalisus algusest lõpuni - alates isikuandmete esmasest kogumisest kuni hävitamiseni on rakendatud asjakohased ja ajakohastatud turvameetmed.
4. Läbipaistvus ja vastutustundlikkus - kõigile organisatsiooni andmetöötlusse kaasatud isikutele ning koostööpartneritele peab olema üheselt arusaadav, mis on andmetöötluse eesmärk. Inimesele on tagatud teave nii tema andmete töötlemise eesmärgi kui ta õiguste kohta selle töötlemise suhtes. Teave on kergelt kättesaadav ning selgelt ja lihtsalt sõnastatud.

Andmetöötlustoimingutest tuvastatavate jälgede – logide – tekitamine ja nende haldamine on üks lõimitud andmekaitse rakendamise kesksemaid aspekte. Kõik organisatsioonid, kes oma tegevuse käigus isikuandmetega kokku puutuvad, on kohustatud tagama, et nende juures töödeldakse isikuandmeid turvaliselt. See tähendab muu hulgas, et infosüsteemides olevaid isikuandmeid kasutatakse ainult sel eesmärgil, mille jaoks nad kogutud on, ning keegi ei pääse andmetele ligi omakasupüüdlikel või pahatahtlikel eesmärkidel ega uudishimust.

Selleks, et ära hoida isikuandmete väärkasutamist ning tagada, et tagantjärele oleks võimalik kindlaks teha, kes, millal ja miks infosüsteemis andmeid vaadanud või kasutanud on, peabki elektroonilise andmetöötluse puhul pidama logikirjeid isikuandmete töötlemise kohta.

Logide pidamise alus tuleneb üldmääruse artiklite 5 ja 32 koosmõjust ning haiglate puhul ka küberturvalisuse seadusest. Isikuandmete töötlemisel peab tagama andmete käideldavuse, tervikluse ning konfidentsiaalsuse. Selleks peab andmetöötleja rakendama asjakohaseid

organisatsioonilisi, infotehnilisi ja füüsilisi turvameetmeid, et kaitsta andmeid loata või ebaseadusliku töötlemise eest.

Küberturvalisuse seaduse alusel kehtestatud määrusest „Võrgu- ja infosüsteemide riskianalüüsi nõuded ning turvameetmete kirjeldus“ tuleneb ka nõue seirata ja ajakohastada turvameetmeid (sh ka logisid), et tagada infosüsteemi riskide haldamine. Mis tähendab, et haiglad peavad regulaarselt seirama ja analüüsima haigla infosüsteemi logisid omamaks operatiivselt ülevaadet nendes kajastuvate sündmuste ja tegevuste kohta.

Lugupidamisega
/allkirjastatud digitaalselt/

Helina-Aleksandra Lettens
vaneminspektor
peadirektori volitusel