



RAKENDUSTE KASUTAMINE HARIDUSASUTUSTE TÖÖS

Nutiajastul kuulub rakenduste kasutamine üha enam koolielu juurde. Rakendused hõlbustavad igapäevatööd, kuid samas võivad töödelda - sh koguda, salvestada, edastada - isikuandmeid. Lisaks kasutajate sisestatud andmetele võivad rakendused koguda andmeid ka automaatselt, näiteks küpsiste või muude jälgimistehnoloogiate kaudu. Seetõttu on oluline teada, kuidas rakendusi turvaliselt kasutada, et koolipere isikuandmed oleksid kaitstud.

Rakendus on tarkvara või veebiteenus, mida kasutatakse õppe-, haldus- või tugiprotsesside läbiviimiseks ning mis võimaldab kasutajatel täita kindlaid ülesandeid, näiteks õppida, suhelda, hallata dokumente, hinnata teadmisi või luua sisu.

Haridusasutustes on tüüpiliselt kasutusel nii veebipõhised rakendused nagu näiteks Moodle, kui ka arvutisse või nutitelefonile paigaldatavad rakendused nagu näiteks Microsoft Teams.

Rakendused ja nende riskitase on erinev. Olenemata kasutusel olevast rakendusest on oluline jälgida, et isikuandmeid töödeldaks ainult vajalikus ulatuses ja kooskõlas muude **andmekaitse- ning infoturbenõuetega**.

Rakenduste kasutamisega kaasnevad mitmed andmekaitseküsimused, millele tähelepanu pöörata.

Kas rakenduses töödeldakse isikuandmeid?

Mitmed rakendused on koolides kasutusel ja heaks kiidetud. Samas rakenduse kasutuselevõtmisel tuleb alati hinnata, kas see on vajalik **õppetöö eesmärgi** saavutamiseks ning milliseid isikuandmeid selles töödeldakse. See kehtib nii tavapäraste digirakenduste kui ka AI-funktsiooniga rakenduste puhul.

Rakenduse kasutajal on oluline mõista, kuidas andmeid töödeldakse:

- kas rakendusse **sisestatakse** õpilaste, töötajate või lapsevanemate isikuandmeid;
- milliseid andmeid rakendus **automaatselt kogub** (nt IP-aadress, seadmeinfo, kasutusstatistika).

See aitab tagada haridusasutusel, et õpilased, töötajad ja vajadusel lapsevanemad saavad aru, milliseid rakendusi kasutatakse, milliseid andmeid neis töödeldakse ja mis eesmärgil seda tehakse.

Milline on õiguslik alus isikuandmete töötlemiseks?

Isikuandmete töötlemine saab toimuda ainult õiguslikul alusel ja kindlal eesmärgil. Haridusasutus töötleb isikuandmeid reeglina avaliku ülesande täitmise raames.

Seetõttu on oluline, et kasutataks rakendusi, mis on haridusasutuse poolt hinnatud ja heaks kiidetud. Rakendustes tuleb töödelda isikuandmeid **minimaalselt** kindla **eesmärgi** huvides.

Andmetöötlusleping rakenduse teenusepakkujaga

Kui rakenduse teenusepakkuja töötleb kooli nimel isikuandmeid, tuleb haridusasutusel üldjuhul sõlmida temaga andmetöötlusleping. Selles lepitakse kokku, kuidas isikuandmeid töödeldakse ning millised on kooli ja teenusepakkuja õigused ja kohustused. Samuti peaks olema hõlmatud, milliseid alltöötlejaid teenusepakkuja kasutab.

Andmetöötlusleping aitab tagada, et isikuandmed oleksid nõuetekohaselt kaitstud, ning annab koolile selge ülevaate sellest, kuidas konkreetne teenusepakkuja andmeid töötleb.

Andmete säilitamine ja liikumine piiriüleselt

Rakendused edastavad ja säilitavad tihtipeale kogutud andmeid väljaspool Euroopa Majanduspiirkonda. Seetõttu on oluline selgitada

- millises riigis andmeid hoitakse;
- kas andmeid edastatakse väljapoole Euroopa Majanduspiirkonda ja mis tingimustel;
- millised kaitsemeetmed sellisel juhul kehtivad.

Eelistada tuleks rakendusi, mis töötlevad andmeid Euroopa Majanduspiirkonnas, ning muul juhul hinnata riske ja piisavaid kaitsemeetmeid.



TEHISARU FUNKTSIOONIGA RAKENDUSED

Tehisaru funktsiooniga rakenduste puhul tuleb läheneda teadlikult ja läbimõeldult. Oluline on silmas pidada rakenduse riskitaset ja milleks seda kasutatakse, et mõista võimalikku mõju inimeste õigustele.

Tehisarul toimiv rakendus suudab andmete põhjal õppida, neid analüüsida ning genereerida vastuseid või teha otsuseid, mitte piirduda üksnes ette programmeeritud käskude täitmisega. Selliste rakenduste puhul tuleb lisaks tavapärastele andmekaitsemeetmetele hinnata ka tehisaru kasutamise kaasnevaid eripärasid.

Haridusasutus peaks tagama, et õppijatele, töötajatele ja vajaduse korral lapsevanematele on selge, millal ja kuidas tehisaru kasutatakse. Teatud juhtudel näeb ka tehisintellekti määrus ette eraldi läbipaistvuskohustused, näiteks kui inimene suhtleb AI-süsteemiga või kui kasutatakse tehislikult loodud sisu. Täpsemalt on võimalik lugeda inspeksiooni [tehisaru rubriigist](#).

Kuigi enamik tehisaru lahendusi on kasulikud, võivad mõned neist tekitada riske inimeste tervisele, turvalisusele ja põhiõigustele, seega tuleb olla tähelepanelik, kuidas turvaliselt kasutamisele läheneda.

Sisestatavad andmed

Hinnata tuleb, kas tehisaru rakendusse on vaja sisestada isikuandmeid. Võimaluse korral kasutada anonüümseid või pseudonüümitud andmeid ning vältida eriliiki isikuandmete (nt terviseandmed) sisestamist.

Anonüümseks muudetud andmed on andmed, mille puhul inimest ei ole enam võimalik tuvastada, pseudonüümitud andmed aga isikuandmed, mida on töödeldud selliselt, et neid ei saa ilma täiendavat teavet kasutamata konkreetse inimesega seostada.

Samuti tuleks välja selgitada, milliseid kasutus- ja tehnilisi andmeid rakendus kogub (nt päringud, logid, seadmeinfo).

Andmete kasutamine tehisaru mudeli arendamiseks

Oluline on veenduda, kas kasutajate sisestatud andmeid kasutatakse tehisaru mudelite treenimiseks või teenuse arendamiseks ning kas seda saab seadistustega piirata või keelata.

Kui tehisaru rakendus kasutab kasutajate sisestatud andmeid mudelite arendamiseks või edasiõpetamiseks, võib see tähendada, et andmeid kasutatakse eesmärgil, mis ei ole seotud õppetööga ja need võivad väljuda haridusasutuse kontrolli alt. Haridusasutusel on vastutus vältida sellist olukorda.

Kui olukord on vältimatu, tuleb õpilast teavitada. Samuti tuleks anda teada, millised on õpilase õigused ja kelle poole saab küsimuste või probleemide korral pöörduda.

Tehisaru väljundite usaldusväärsus

Tehisaru võib anda ebatäpseid või eksitavaid vastuseid ning mõnikord ka õppijatele sobimatut sisu. Seetõttu tuleks tehisaru loodud sisu alati enne kasutamist üle kontrollida. Samuti ei tohiks tehisaru väljund olla ainus alus õppijaid või töötajaid puudutavate otsuste tegemisel.

Sageli võivad tehisaru rakenduste vastused olla kallutatud, sest need põhinevad andmetel, mille peal mudel on treenitud, ja sellel, kuidas mudel töötab. Seetõttu tasub haridusasutustel tehisaru loodud sisu alati kriitiliselt hinnata ning mitte eeldada, et see on automaatselt objektiivne või erapooletu.

Enne tehisaru rakenduse kasutamist tuleks hinnata, millised meetmed on rakenduses ette nähtud ebatäpsuste, eksitavate või kallutatud väljundite selgitamiseks ja tuvastamiseks.

Inimjärelevalve kui prioriteet

Tehisaru roll on eelkõige toetada õpetaja või muu koolitootaja otsuseid, mitte neid täielikult asendada, eriti kui otsused mõjutavad õppijaid.

Seetõttu tuleks eelistada lahendusi, kus tehisaru toimib otsustamise abivahendina ning lõpliku otsuse teeb koolitootaja pärast tehisaru väljundi sisulist hindamist.

Tutvu ka [Hariduse tehnoloogiakompassiga](#). „Hariduse tehnoloogiakompass“ on Eesti koolidele mõeldud tehnoloogiaülevaade, mis annab praktilisi nõuandeid tehnoloogia rakendamiseks kaasaegses õppetöös.



RAKENDUSTE KASUTAMISE KORRALDAMINE HARIDUSASUTUSES

Enne uue rakenduse kasutuselevõttu peaks haridusasutus hindama, milliseid andmeid rakendus kasutab ja kuidas need on kaitstud. Nii saab ennetada olukordi, kus võetakse kasutusele rakendus, mille mõju andmekaitsele ja infoturbele ei ole eelnevalt läbi mõeldud.

Ülevaade rakenduste kasutamisest

Haridusasutus peaks pidama ülevaadet kasutatavatest rakendustest, sh nende kasutamise eesmärgist, töödeldavatest isikuandmetest, teenusepakkujast, andmete säilitamise kohast ning vajaduse korral andmetöötluslepingu olemasolust.

Samuti tuleks tagada, et töötajad teavad, milliseid rakendusi kasutatakse, milliseid isikuandmeid ei tohi rakendustesse sisestada ning kuidas toimub uute rakenduste kasutuselevõtt.

Õppijaid, töötajaid ja vajaduse korral lapsevanemaid tuleb teavitada kasutatavatest rakendustest, nende kasutamise eesmärkidest ning isikuandmete töötlemise põhimõtetest.

Haridusasutus peaks määrama, kes hindab uusi rakendusi enne nende kasutuselevõttu ning kelle poole saavad töötajad pöörduda küsimuste korral, mis puudutavad isikuandmete töötlemist või infoturvet.

Ülevaade kasutatavatest rakendustest ning nende kasutamise põhimõtetest aitab tagada läbipaistvuse ja parema kontrolli isikuandmete töötlemise üle.

Tehisaru rakenduste riskihindamine

Tehisaru sisaldavate rakenduste kasutamisel tuleb järgida andmekaitse põhimõtteid ning tagada, et andmed oleksid piisavalt kaitstud. Selleks tuleb kasutada sobivaid turvameetmeid ja piirata ligipääsu ainult neile, kellel seda tööks vaja on.

Kõrgema riskiga tehisaru kasutamise puhul, näiteks õppijate profileerimisel, automaatsel hindamisel või soovitude tegemisel, tuleb esmalt hinnata võimalikke riske. Vajadusel tuleks teha täiendav riskianalüüs või andmekaitsealane mõjuhindang.

Selline hindamine aitab tagada, et tehisaru rakenduste kasutamine on kooskõlas isikuandmete kaitse, infoturbe ning haridusasutuse vastutustundliku andmekasutuse põhimõtetega.

Kasutustingimused ja privaatsuspoliitika annavad olulist teavet selle kohta, kuidas teenusepakkuja isikuandmeid töötleb ja kaitseb.

Isikuandmetega seotud rikkumistest teatamine

Kui rakenduse teenusepakkuja töötleb haridusasutuse nimel isikuandmeid, peab ta isikuandmete rikkumisest põhjendamatult viivitusega teavitama haridusasutust.

Haridusasutus peaks teadma, kuidas teenusepakkuja sellistest juhtumitest teavitab ning milliseid meetmeid rakendatakse rikkumise mõju vähendamiseks.

Isikuandmete rikkumise korral võib haridusasutusel olla kohustus teavitada Andmekaitse Inspeksiooni ning teatud juhtudel ka inimesi, kelle andmeid rikkumine puudutab.

Meetmed rakenduste turvalisuse tugevdamiseks ja isikuandmete kaitsmiseks

Identiteedihaldus ja autentimine: Kasuta tugevaid paroole ja mitmikautentimist (nt ID-kaart, Mobiil-ID, Smart-ID, ühekordseid paroole genereerivad autentimisrakendused);

Minimaalne ligipääs: Anna kasutajatele ainult vajalikud õigused, et piirata juurdepääsu tundlikule teabele;

Logimine ja monitooring: Jälgi süsteemide tegevusi ja tuvasta anomaaliaid, kasutades näiteks SIEM-lahendusi;

Kaugjuurdepääsude turvalisus: Kaitse VPN- ja RDP-ühendusi ning sulge mittevajalikud ligipääsud;

Pääsuõiguste haldus: Kontrolli regulaarselt, kellel on ligipääs rakendustele, ja eemalda õigused, mida enam ei vajata;

Tarkvarauuendused ja turvapaigad: Uuenda süsteeme ja rakendusi regulaarselt, et vältida turvaauke;

Andmete krüpteerimine: Krüpteeri tundlikud andmed nii edastamisel kui ka salvestamisel.