HITSA
Hariduse Infotehnoloogia Sihtasutus

ISIKUANDMETE KAITSE ÜLDMÄÄRUSE RAKENDAMINE HARIDUSASUTUSTES

JUHENDMATERJAL

2018

Juhendmaterjal on välja töötatud Haridus- ja Teadusministeeriumi tellimusel ning Hariduse Infotehnoloogia Sihtasutuse juhtimisel. Juhendmaterjali koostamises osalesid FocusIT OÜ partnerid Doris Matteus, Jaan Oruaas ja Anu Tanila ning HITSA juristid Raili Sassian ja Katri Samarütel. Juhendmaterjali „Lisa 1“ koostasid Grant Thornton Baltic OÜ riskijuhtimisteenuste valdkonna juht Siiri Antsmäe ja õigusnõustaja Allan Kubu ning „Lisa 2“ FocusIT OÜ partner Janek Part.
Keeleliselt toimetas teksti Bo Britt Peet.

Kaasrahastatud Euroopa Liidu poolt
Euroopa Ühendamise Rahastu

Targalt internetis

Sisukord

Sissejuhatus

Õigus isikuandmete kaitsele on füüsilise isiku põhiõigus, mis on sätestatud Euroopa Liidu põhiõiguste hartas[1], Euroopa Liidu toimimise lepingus[2] ning samuti Eesti Vabariigi põhiseaduses[3]. Lapse isikuandmete kaitse nõuet rõhutab lisaks ÜRO lapse õiguste konventsioon[4]. Samas ei ole tegemist absoluutse õigusega, oluline on tasakaalustatus teiste põhiõiguste, -vabaduste ning õigusaktides toodud piirangutega.

Näiteks ei ole lapsevanemal õigust otsustada teatud andmete esitamata jätmise üle lapse kooli õppima asumise taotluse esitamisel, kui nende andmete esitamise kohustus tuleneb õigusaktist või õigusakti alusel muust regulatsioonist (*näiteks „Õpilase kooli vastuvõtmise üldised tingimused ja kord ning koolist väljaarvamise kord" § 3 lg 1*).

Isikuandmete kaitse valdkonda Euroopa Liidus ning seega ka Eestis reguleerib alates **25. maist 2018. aastast** Euroopa Parlamendi ja nõukogu määrus 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta[5] (isikuandmete kaitse üldmäärus – ***General Data Protection Regulation,*** *lühend* ***GDPR***). Edaspidi viidatakse tekstis isikuandmete kaitse üldmäärusele kui määrusele.

Tegemist on otsekohalduva määrusega. Otsekohalduv määrus rakendub samal kujul kõigis liikmesriikides, ilma et oleks vaja enne siseriiklikke õigusakte vastu võtta. Siseriiklikus seadusandluses reguleeritakse vaid neid küsimusi, mida määrus ei käsitle või mille osas jätab määrus liikmesriikidele täpsustamise õiguse. *Näiteks annab määrus õiguse kehtestada siseriiklikus seaduses madalama vanusepiiri, kui määruses toodud 16 aastat, mil laps võib anda ise nõusoleku infoühiskonna teenustega seoses oma isikuandmete töötlemiseks. Eestis planeeritakse vanusepiiriks sätestada määruses toodud miinimumtase ehk 13 aastat*.

Eestis on reguleerinud isikuandmete kaitse valdkonda isikuandmete kaitse seadus (IKS). Uus IKS[6], mis arvestab määrusega, on juhendi koostamise hetkel eelnõu staadiumis. Samuti on eelnõu faasis „Isikuandmete kaitse seaduse rakendamise seadus", millega muudetakse mitmeid seadusi, sh haridusvaldkonna seadusi (*nt põhikooli- ja gümnaasiumiseadust, EV haridusseadust, erakooliseadust*).

Euroopa isikuandmete kaitse valdkonna reformimise vajadus on tulenenud eelkõige tehnoloogia kiirest arengust, mis on oluliselt suurendanud isikuandmete kogumise ja jagamise ulatust, võrreldes ajaga, mil töötati välja siiani kehtinud isikuandmete kaitse põhimõtted. Määruse eesmärk on ühelt poolt suurendada füüsiliste isikute kontrolli oma isikuandmete üle ning teiselt poolt tugevdada ja ühtlustada andmekaitse rakendamise põhimõtteid kõikides Euroopa Liidu liikmesriikides.

Oluline on märgata, et seni kehtinud andmekaitse põhimõtted määruse jõustumisel oluliselt ei muutu. Määrus täpsustab mitmeid põhimõtteid ja isikute õigusi, samuti loob juurde õigusi andmesubjektidele ning paneb teatud tingimustel asutustele mõningaid uusi kohustusi (*näiteks andmekaitsespetsialisti määramine ning mõjuhinnangu läbiviimise kohustus*). Seetõttu on asutusel alustuseks olulisim saada ülevaade tänasest seisust ning selle tulemusel asuda kõrvaldama võimalikke puudujääke. Esmalt peab tuvastama, kas asutus vastab määruse nõuetele, ning puudujääkide esinemisel tuleb koostada tegevuskava selleks, kuidas jõuda määrusega vastavuseni.

Käesolev juhendmaterjal on ülevaatlik abivahend haridusasutusele määruse rakendamisel. Juhendi sihtrühmaks on eelkõige alus-, üld- , kutse- ja rakenduskõrgharidust pakkuvad haridusasutused.

---

[1] http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:12012P/TXT&from=ET
[2] http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:12016E/TXT&from=EN
[3] Eesti Vabariigi Põhiseadus (RT 1992, 26, 349) https://www.riigiteataja.ee/akt/115052015002?leiaKehtiv
[4] Lapse õiguste konventsioon (RT II 1996, 16, 56) https://www.riigiteataja.ee/akt/24016
[5] http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32016R0679&from=ET
[6] http://eelnoud.valitsus.ee/main/mount/docList/1909e111-ca98-4d1b-830a-ee49dea64a97#7CI0ZlVx

Mõisted

GDPR – Euroopa Parlamendi ja nõukogu määrus 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta[7] (isikuandmete kaitse üldmäärus - *General Data Protection Regulation*). GDPR-is kasutatavad mõisted on lahti seletatud määruse 4. artiklis, järgenvalt on toodud käesoleva juhendmaterjali kontekstis olulisemate mõistete selgitused.

Isikuandmed – igasugune teave, mille kaudu on otseselt või kaudselt võimalik tuvastada konkreetne füüsiline isik (õpilane, lapsevanem, eestkostja, õpetaja, kooli töötaja jne) eelkõige sellise identifitseerimistunnuse alusel nagu nimi, isikukood, asukohateave, kontaktandmed, võrguidentifikaator (kasutajatunnus, IP-aadress) või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal.

Eriliiki isikuandmed – määruse järgi on eriliiki isikuandmed need, millest ilmneb inimese rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilised andmed, füüsilise isiku kordumatuks tuvastamiseks kasutatavad biomeetrilised andmed, terviseandmed või andmed füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta. *Haridusasutuse kontekstis on töödeldavateks eriliiki isikuandmeteks näiteks lapse terviseseisundit puudutavad andmed, sotsiaalpedagoogi/psühholoogi esitatud teave, sotsiaalteenuste osutamise taotlemist kirjeldavad andmed, andmed, mis ilmnevad seoses hariduslike erivajadustega jms.*

Terviseandmed – füüsilise isiku füüsilise ja vaimse tervisega seotud andmed, sealhulgas isikule tervishoiuteenuste osutamist käsitlevad andmed, mis annavad teavet tema tervisliku seisundi kohta.

Isikuandmete töötlemine – kõik isikuandmete või nende kogumitega tehtavad automatiseeritud või automatiseerimata toimingud, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, samuti edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine.

Andmesubjekt – füüsiline isik, kelle isikuandmeid töödeldakse.

Isikuandmete vastutav töötleja – füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid.

Volitatud töötleja – isik, kes töötleb isikuandmeid vastutava töötleja nimel.

Näiteks on vastutavaks töötlejaks haridusasutus, kes ise või seadusandlusest lähtudes määrab, milliseid andmeid ja kuidas oma tegevuse elluviimiseks kogub ja töötleb. Volitatud töötlejaks võib olla näiteks kooli/lasteaiahaldussüsteemi (e-Kool, Stuudium, Eliis jt), mille abil andmeid kogutakse ja muul viisil töödeldakse, omanik.

Isikuandmete vastuvõtja – füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kellele isikuandmed avaldatakse.

Infoühiskonna teenus – teenus, mida osutatakse majandus- või kutsetegevuse käigus teenuse kasutaja otsesel taotlusel ja mille puhul andmeid töödeldakse, säilitatakse ja edastatakse digitaalkujul andmete töötlemiseks ja säilitamiseks mõeldud elektrooniliste vahendite abil, kusjuures osapooled ei viibi üheaegselt samas kohas. Infoühiskonna teenus peab olema täielikult üle kantud, edastatud ja vastu võetud elektrooniliste sidevahendite abil. Infoühiskonna teenus ei ole faksi ega telefonikõne abil edastatud teenus ega televisiooni- või raadioteenus[8].

Järelevalveasutus – sõltumatu riigiasutus, kelle ülesanne on teha järelevalvet määruse kohaldamise üle ja edendada isikuandmete töötlejate teadlikkust. Eestis on järelevalveasutuseks Andmekaitse Inspektsioon (AKI).

Kasulikud veebilehed

Andmekaitse Inspektsioon: http://www.aki.ee/et/eraelu-kaitse/euroopa-andmekaitse-reform
Euroopa andmekaitseasutuste töörühma veebileht: https://ec.europa.eu/info/law/law-topic/data-protection_en

[7] http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32016R0679&from=ET
[8] Infoühiskonna teenuse seadus (RT I 2004, 29, 191) https://www.riigiteataja.ee/akt/112072014048

1. Haridusasutus isikuandmete töötlejana

Haridusasutus on vastutav töötleja, kes töötleb lasteaialaste/õpilaste/üliõpilase/õppuri, töötajate ning lapsevanemate/lapse eestkostjate andmeid. Sellele nimekirjale võivad lisanduda ka muude isikute, näiteks vilistlaste, toetajate, hoolekogu liikmete jt andmed. Määrus ei rakendu ettevõtete ega teiste juriidiliste isikute andmete töötlemisele, küll aga juriidilise isikuga seotud füüsiliste isikute andmetele, nagu näiteks töötajate nimelised tööalased e-posti aadressid.

Haridusasutuses töödeldavad isikuandmed võib jagada kaheks:
- seaduste täitmiseks töödeldavad isikuandmed ja
- muudel eesmärkidel töödeldavad isikuandmed.

Esimese grupi isikuandmed tulenevad õigusaktidest või nende alusel kehtestatud haridusasutuse sisestest normdokumentidest ning on tavaliselt dokumenteeritud ja registreeritud asutuse dokumendiloetelus/-liigitusskeemis. Neile andmetele on määratud vastutaja, ligipääsu piirangud ja säilitamise tähtaeg. *Sellised on näiteks kooli astumise avalduses, klassitunnistustes, õppenõukogu käskkirjades, protokollides, õpilase immuniseerimispassis, töölepingutes jms sisalduvad andmed.*

Teise grupi isikuandmeid kogutakse vajaduspõhiselt. *Näiteks klassijuhataja mitteametlik otsesuhtlus lapsevanemaga, vanemate sotsiaalmeedia kontod, töökohtade ja ametikohtadega seotud info ja muud andmed, mille kogumine pole otseselt koolile kohustuslik, kuid mis võib olla vajalik koolitöö sujuvaks korraldamiseks, õpilase heaoluks ja turvalisuse tagamiseks. Kirjeldatud viisil võivad haridusasutuste töötajatele saada teatavaks ka lapse tervist puudutavad andmed.*

Praktikas ei pruugi teisel viisil isikuandmete töötlemine olla haridusasutuse pidaja kontrolli all ega kajastuda ametlikus dokumendiloetelus/-liigitusskeemis. Samas vastutab haridusasutuse pidaja kõikide haridusasutuses kogutud isikuandmete töötlemise eest, millest tulenevalt on oluline läbi mõelda, kuidas selliste vajaduspõhiselt kogutud isikuandmete töötlemine reguleeritakse, et oleks täidetud kõik määruse nõuded.

Oluline on analüüsida ja mõista, milline teave isiku kohta loetakse isikuandmeteks. Lihtsam on mõista isikuandmeid, mis on loetletud eelmises alapunktis „isikuandmete" mõiste selgituses, kuid määrus defineerib isikuandmeid laialt kasutades sõnastust „igasugune teave" tuvastatud või tuvastatava füüsilise isiku kohta. *Näiteks on Euroopa Kohus 2017.a lõpus andnud selgituse, et kutseeksami töös esitatud vastused ja kontrollija poolt tööle lisatud märkused on isikuga seotud teave. Kohus selgitab: „Esmalt peegeldab vastuste sisu eksaminandi teadmiste ja oskuste taset konkreetses valdkonnas ning vajaduse korral ka tema arutlusoskusi, analüüsi- ja kriitilise mõtlemise võimet. Kui eksamitöö on käsitsi kirjutatud, sisaldavad vastused lisaks veel ka teavet eksaminandi käekirja kohta."*[9].

Sama Euroopa Kohtu otsuse punktis 34 on kohus selgitanud isikuandmete määratlust järgmiselt: „seadusandja eesmärk oli anda kõnealusele mõistele lai tähendusväli, mis ei ole piiratud tundliku või eraelulise teabega, vaid hõlmab potentsiaalselt igasugust, nii objektiivset kui ka subjektiivset teavet arvamuste või hinnangute vormis, tingimusel, et need „puudutavad" kõnealust isikut.".[10]

[9] Vt lähemalt Euroopa Kohtu kohtuasi C-434/16 (otsus 20.12.2017) *Peter Nowak vs Data Protection Commissioner* (https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:62016CJ0434&from=EN). Otsus on tehtud direktiivi 95/46/EÜ alusel, kuid on asjakohane ka määrusest lähtudes.

[10] samas, p 34

2. Isikuandmete töötlemise põhimõtted ja vastutus

Isikuandmete kaitse nõuete, sh isikuandmete töötlemise põhimõtete järgimise kohustus on kõigil, kes töötlevad või kelle ülesandel töödeldakse isikuandmeid. Nõuded ei rakendu siis, kui isikuandmeid töötleb füüsiline isik üksnes isiklike või koduste tegevuste käigus (*näiteks lapsevanem pildistab lasteaias/koolis lapsi vaid isiklikuks otstarbeks, kuid ei levita neid avalikes allikates, nt Facebookis*).

Määruse artikkel 5 loetleb põhimõtted, millest tuleb isikuandmete töötlemisel lähtuda:

- Isikuandmete töötlemine peab olema **seaduslik, õiglane ja läbipaistev**.
- **Isikuandmete töötlemise eesmärgi piirang** – isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud eesmärkidel ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus (välja arvatud isikuandmete töötlemine avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgil).
- **Isikuandmete minimaalsuse printsiip** – isikuandmed on asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt.
- **Isikuandmete õigsus** – isikuandmed on õiged ja vajaduse korral ajakohastatud.
- **Isikuandmete säilitamise piirang** – isikuandmeid säilitatakse ainult seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse.
- **Usaldusväärsus ja konfidentsiaalsus** – isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest.

Haridusasutus on vastutav töötleja ning seda nii õpilaste, lapsevanemate/eestkostjate kui ka töötajate isikuandmete osas. Teatud juhtudel võib haridusasutus olla ka volitatud töötleja.

Näiteks on haridusasutus volitatud töötleja juhul, kui isikuandmeid töödeldakse koolituse läbiviimiseks, mille on tellinud majaväline osapool.

Vastutav töötleja võib delegeerida mõne osa isikuandmete töötlemisest volitatud töötlejale (*näiteks andmete säilitamine välise partneri serveris, raamatupidamisteenuse sisse ostmine, väljaspool maja asuv arhiiv, õpihaldustarkvara teenuse ostmine, andmete jagamise rakenduste kasutamine jne*). Kuigi ka volitatud töötlejal on isikuandmete töötlemise põhimõtete järgimise kohustus, vastutab isiku ees andmetöötluse põhimõtete järgimise ja isikuandmete kaitse eest vastutav töötleja, kes peab vajadusel suutma tõendada, et isikuandmete töötlemise põhimõtetest on kinni peetud.

Selleks, et olla võimeline põhimõtete järgimist tõendama, peab vastutav töötleja oma tegevust dokumenteerima.

Järgnevas tabelis on toodud näited dokumentatsioonist, mille abil põhimõtete täitmist on võimalik tõendada (loetelu ei ole ammendav):

Põhimõte	Võimalikud tõendid
Isikuandmete töötlemise õiguslik alus	- töötlustoimingute register (määrus ei nõua, et registris kajastuks info õigusliku aluse kohta, kuid ülevaate saamiseks on soovituslik see info lisada) - nõusolek kirjalikku taasesitamist võimaldavas vormis ja/või logid, mis võimaldavad nõusoleku andmist kontrollida - õigusaktid/andmekogude ja infosüsteemide põhimäärused
Isikuandmete töötlemise läbipaistvus	- privaatsuspoliitika haridusasutuse veebilehel - nõusoleku tekst, mis sisaldab nõutud infot, sh andmete töötlemise eesmärkide täpset sõnastust

Isikuandmete töötlemise eesmärgi piirang	- töötlustoimingute register - leping volitatud töötlejaga (andmete kasutamise piirang) - õigusaktid/andmekogude ja infosüsteemide põhimäärused
Isikuandmete minimaalsuse printsiip	- andmekogumise vahendid (avaldused, taotlused, veebivormid jne) - töötlustoimingute register
Isikuandmete õigsus	- tegevused, mis on tehtud selleks, et andmed oleksid õiged ja ajakohased
Isikuandmete säilitamise piirang	- töötlustoimingute register - asutuse dokumendiloetelu/liigitusskeem - andmete hävitamist tõendavad aktid vm dokumendid
Usaldusväärsus ja konfidentsiaalsus	- isikuandmete töötlemist reguleerivad dokumendid (sh õppekorralduse eeskiri, isikuandmete töötlemise kord, arvutisüsteemi kasutamise kord jne) - ligipääsuõiguste andmist reguleerivad dokumendid - töötlustoimingute register - infosüsteemide logid, mis näitavad, millal on infosüsteemis andmetöötlustoiminguid tehtud ja kes neid on teinud - infoturvet reguleerivad dokumendid (arvutivõrgu ja arvutite kasutamise kord jne) - standardile vastavust tõendavad sertifikaadid - volitatud töötlejaga sõlmitud leping (andmekaitse nõuded) - tõendid töötajate seas läbi viidud valdkonna koolituste/teavituse kohta

2.1 Isikuandmete töötlemise õiguslik alus

Isikuandmete töötlemise oluline põhimõte on, et töötlemine peab olema seaduslik, õiglane ja andmesubjektile läbipaistev.

Isikuandmete töötlemise kaardistamisel peaks iga andmerea taha olema võimalik lisada info selle kohta, millisel määruses toodud õiguslikul alusel neid andmeid töödeldakse.

Määrus annab isikuandmete töötlemiseks järgmised õiguslikud alused:

Avalikes huvides oleva ülesande täitmine (määruse artikkel 6 punkt e)

Isikuandmeid tohib töödelda avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks. Eesti Vabariigi põhiseadus näeb ette, et riik ja kohalik omavalitsus peavad ülal vajalikul arvul õppeasutusi ning riigi ülesanne on korraldada kutseõpet. Seega on riigi ja kohaliku omavalitsuse haridusasutuste haridusteenuse pakkumisel tegemist avaliku ülesande täitmisega.

Erakapitalil asutatud haridusasutus ei täida reeglina haridusteenust pakkudes avalikku ülesannet, v.a kui nad pakuvad haridusteenust riigi või kohaliku omavalitsuse eest ja nendega sõlmitud lepingu alusel.

Juriidiline kohustus (määruse artikkel 6 punkt c)

Isikuandmeid tohib töödelda ja peab töötlema, kui see on vajalik andmetöötleja juriidilise kohustuse täitmiseks. Suurem osa haridusasutuste isikuandmete töötlemisest toimub õigusaktides toodud kohustuse täitmiseks.

Näiteks töödeldakse sel alusel õppetöö läbiviimisega seotud isikuandmeid; raamatupidamisarvestuse korraldamisega seotud isikuandmeid; töötajate üle arvestuse pidamisega seotud isikuandmeid; samuti töötajate tervisekontrolli andmeid, kui seadus näeb tööandjale ette kohustuse töötajate tervisekontrolli läbimise tagamiseks jne.

Juriidilise kohustuse alusel toimub ka isikuandmete edastamine kolmandatele isikutele, kui andmete edastamise kohustus tuleneb seadusest (*näiteks kohalikule omavalitsusele, riiklikele registritele, nagu EHIS ja EIS, Maksu- ja Tolliametile, Haigekassale, Sotsiaalkindlustusametile*) või juhul kui kolmas isik esitab oma seadusest tuleneva kohustuse täitmiseks haridusasutuse andmete saamiseks päringu (*näiteks järelevalveasutused, Politsei- ja Piirivalveamet, sotsiaalhoolekandega seotud asutused*).

Leping (määruse artikkel 6 punkt b)

Isikuandmeid tohib töödelda sõlmitud lepingu täitmiseks või lepingu sõlmimisele eelnevate tegevuste käigus vastavalt isiku taotlusele.

Lepingu alusel töödeldakse haridusasutustes näiteks võlaõigusliku lepingu alusel töötavate isikute andmeid (selliste andmete töötlemise aluseks võib olla ka juriidiline kohustus), ka huvi- ja spordiringides osalemiseks võib isikuandmete töötlemise aluseks olla leping. Samuti juhul, kui haridusasutusel on meenete/koolivormide jms müümiseks kasutusel veebipood, siis selliste tellimuste täitmiseks kogutavate isikuandmete töötlemise aluseks on leping.

Eluliste huvide kaitseks (määruse artikkel 6 punkt d)

Isikuandmeid tohib töödelda, kui see on vajalik andmesubjekti või mõne muu füüsilise isiku eluliste huvide kaitsmiseks.

Näiteks saab sellel alusel haridusasutustes isikuandmeid töödelda hädaolukordades ja õnnetuste korral, kui edastatakse isikuandmeid kiirabile.

Õigustatud huvi (määruse artikkel 6 punkt f)

Isikuandmeid tohib töödelda, kui see on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral. Erandiks on siin juhtumid, kus avaliku huvi kaaluvad üles andmesubjekti huvid või põhiõigused ja -vabadused, mille nimel tuleb isikuandmeid kaitsta, eriti juhul, kui andmesubjekt on laps.

Näiteks võib olla asutusel õigustatud huvi infoturbe tagamiseks jälgida oma töötajate arvutikasutust. Samas peab jälgima, et selle tegevusega ei riivataks põhjendamatult töötajate privaatsust.

Nõusoleku alusel (määruse artikkel 6 punkt a)

Juhul kui isikuandmete töötlemiseks ei ole ühtegi teist eeltoodud õiguslikku alust, siis peab nende isikuandmete töötlemiseks olema isiku nõusolek. Järgnevalt vaatame täpsemalt nõusolekule esitatavaid nõudeid.

2.1.1 Isikuandmete töötlemine nõusoleku alusel (näited)

Haridusasutused töötlevad isikuandmeid muuhulgas nõusoleku alusel.

Näited nõusoleku alusel andmete töötlemise kohta haridusasutuses:

- *Lapse terviseandmeid, mille lapsevanem on otsustanud lapse tervise ja heaolu huvides haridusasutusele teatavaks teha. Näiteks võib olla vajalik kooli teavitada lapse allergiast või muust terviseseisundist. Samas nõue esitada koolile lapse tervisekaart tuleneb seadusest*[11].

[11] Õpilase kooli vastuvõtmise üldised tingimused ja kord ning koolist väljaarvamise kord (RT I 2010, 60, 408) § 3 lg 1 p 3 - https://www.riigiteataja.ee/akt/13359746#para3

- *Laste nimekirjade avaldamine haridusasutuste veebilehtedel. Avalik informatsioon lapse lasteaia/kooli kohta võib muuhulgas kujutada riski lapse turvalisusele, mistõttu on oluline eelneva nõusoleku küsimine. Vilistlaste nimekirjade avaldamine haridusasutuste veebilehel on lubatud ilma eelneva nõusolekuta, v.a kui tegemist on erivajadusega lastega. Samas peab haridusasutus tagama, et isiku nõudel tema andmed vilistlaste loendist eemaldatakse.*[12]
- *Haridusasutustes pildistamisel/filmimisel ning fotode/videomaterjali avalikuks tegemisel tuleb eristada, kas tegemist on avalikus kohas pildistamise/filmimisega (nt lõpuaktus), mil ei ole vajalik nõusoleku küsimine ja piisab eelnevast pildistamise/filmimise faktist teavitamisest, või ei ole tegemist avaliku kohaga (nt konkreetne õppetund klassis). Viimasel juhul on vajalik eelnev nõusolek pildistamiseks/filmimiseks ning fotode/videomaterjali avalikuks tegemiseks.*[13]
- *Kui õpilaste uurimustööde koostamisel töödeldakse isikuandmeid, siis saab neid töödelda üksnes isiku nõusoleku alusel. Nõusolekut ei ole vaja, kui andmeid laekuvad ja neid töödeldakse isikustamata kujul (nt anonüümiseeritult).*
- *Lapsevanema e-posti aadressi liitmine klassi lapsevanemate e-posti listiga.*
- *Reklaammaterjali saatmine lapsevanema e-posti aadressile.*
- *Juhtumipõhised ühekordsete ürituste korraldamisel töödeldavad isikuandmed, nt klassiekskursiooni või õppekäiku organiseerides õpilaste andmete edastamine reisifirmale.*
- *Projektides, uuringutes (nt vaikuseminutid) osalemine, mille käigus edastatakse andmed kolmandatele isikutele.*
- *Töötajate lisaandmete töötlemine, näiteks andmed töötaja laste kohta.*
- *Õpilase menüüpiirangute (laktoosivaba, gluteenivaba, mõne toiduaine vaba) info kasutamine toitlustamisel.*

Nõusoleku sellisteks tegevusteks, mis on ette teada (näiteks kooliürituste fotografeerimine ning fotode avaldamine, õpilaste nimekirjade avaldamine veebilehel, lapsevanema meiliaadressi lisamine e-posti listi jne), võib võtta koos kooli astumise avaldusega, kuid tuleb tähele panna, et lapsevanemal peab olema selge võimalus nõusoleku andmisest keelduda ning antud nõusolek tagasi võta (vt punkti „Nõuded nõusolekule“).

Nõusolekut ei pea küsima selliste õppevahendite, õppekeskkondade ja õpperakenduste kasutamiseks, mis on koolis kasutusel üksnes õppetöö läbiviimiseks ning milleta õpilane ei saa õppetöös osaleda *(nt kooli domeeniga meilikonto, Moodle, erinevad õpikeskkonnad jms*). Selliste vahendite, keskkondade, rakenduste jms kasutamine ning nende kasutamisega kaasnevate isikuandmete töötlemise põhimõtted tuleb kajastada haridusasutuse kodukorras ning vajadusel täpsustada privaatsuspoliitikas, IT eeskirjades või muus haridusasutuse siseregulatsioonis tagamaks piisavat selgust isikuandmete töötlemise nõuetele vastavuse osas. Samas peab nõusolekut küsima, kui isikuandmeid töödeldakse õppetöös kasutatavatesse veebikeskkondadesse juurdepääsu tegemiseks, kui selle juurdepääsu kaudu on võimalik kasutada ka õppetööga mitteseotud rakendusi *(nt Youtube kasutajakonto loomine õpilasele)*. Elektroonilise õppeinfosüsteemi kasutamise ja selles isikuandmete töötlemise alus tuleneb haridus- ja teadusministri *25.08.2010* määruse[14] *nr 52 § 2 lg-st 1* ning isikuandmete töötlemiseks määruses toodud mahus ei ole vaja nõusolekut küsida. *(Tekst muudetud 10.09.2018 seisuga).*

[12] Vt täpsemalt AKI juhend „Õpilaste ja vilistlaste nimekirjade avaldamise juhend“ http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/Opilaste_ja_vilistlaste_nimekirjade_avaldamise_juhend_2016.pdf

[13] Vt täpsemalt AKI juhendit „Juhend kaamerate kasutamise kohta“, mis käsitleb muuhulgas isikuandmete kaitse põhimõtteid pildistamisel ja filmimisel
http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Kaamerate%20kasutamise%20juhis.pdf

[14] Kooli õppe- ja kasvatusalastes kohustuslikes dokumentides esitatavad andmed ning dokumentide täitmise ja pidamise kord - https://www.riigiteataja.ee/akt/13352237# - „Koolis peetakse õppe- ja kasvatusalaseid kohustuslikke dokumente paberil või elektroonilises õppeinfosüsteemis.“

Enne määruse jõustumist saadud nõusoleku alusel võib isikuandmeid edasi töödelda, kui varem antud nõusolek vastas määruse tingimustele. Kui varasem nõusolek määruse tingimustele ei vastanud, peab isikuandmete töötlemise jätkamiseks küsima isikult uue nõusoleku.

Näiteks, kui isikuandmete töötlemise aluseks on nõusolek, mis saadi kasutades veebivormil eelmärgistatud märkeruutu, siis selle nõusoleku alusel ei ole isikuandmete töötlemine 25. maist 2018.a-st enam lubatud.

Kui isikuandmete töötlemiseks on olemas mõni muu õiguslik alus (näiteks seadusest tulenev alus või töötlemine on vajalik lepingu täitmiseks), ei tohiks isikult täiendavalt nõusolekut küsida. Sellises olukorras nõusoleku küsimine on eksitav ja võib jätta isikule arusaama, et tal on igal ajal õigus võtta tagasi oma andmete töötlemiseks antud nõusolek.

Nõuded nõusolekule

Nõusolekuks ei saa lugeda ükskõik millist nõustumist. Peamised tingimused, millele nõusolek peab vastama, on loetletud määruse artiklites 7 ja 8.

Nõusoleku andmine peab vastama järgmistele nõuetele:

- vastutav töötleja peab olema võimeline tõendama, et isik on andnud nõusoleku oma isikuandmete töötlemiseks. Vaikimise või tegevusetusega ei saa nimetatud juhul nõusolekut väljendada;
- nõusoleku saamiseks ei tohi kasutada eeltäidetud lahtritega vorme, isik peab ise lahtrid täitma või kastidesse „linnukese“ lisama, st olema aktiivne nõusoleku andmisel;
- nõusoleku vorm peab olema konkreetne, lihtsa ja selge sõnastusega;
- nõusoleku küsimine peab olema selgelt eristatud teistest võimalikest küsimustest, mida samas vormis käsitletakse;
- nõusolek peab olema vabatahtlik, sellest keeldumisele ei tohi järgneda isikule kahjulikke tagajärgi, st olukord, kus nõusoleku andmata jätmisel ei pakuta isikule teenust, kuigi küsitud isikuandmeid teenuse osutamiseks vaja ei ole. Näiteks ei saa nõusolek lapse piltide ja nime avaldamiseks kooli veebilehel olla kooli vastuvõtmise tingimuseks;
- isikul on õigus nõusolek igal ajal tagasi võtta, see võimalus koos viitega tagasivõtmise viisile peab olema märgitud nõusoleku andmise vormile.

Nõusoleku vormis peab olema vähemalt järgmine teave:

- andmed vastutava töötleja kohta, sh kontaktandmed. Isik peab teadma, kellele ta oma andmed annab;
- teave andmete töötlemise eesmärgi kohta. Isik peab teadma, miks tema andmeid küsitakse ja mida nendega on kavas teha. Erineval eesmärgil andmete töötlemisel peab olema võimalus anda eraldi nõusolek iga eesmärgi kohta;
- kui andmeid planeeritakse edastada kolmandatele isikutele, siis informatsioon selle kohta, kes on andmete vastuvõtjad (näiteks volitatud töötlejad, riigiasutused jne).
- teave selle kohta, kas ja milliseid eriliiki isikuandmeid töödeldakse.

AKI on koostanud kontrollnimekirja, mis võimaldab kontrollida nõusoleku küsimise vormide ja protseduuride vastavust määruse nõuetele[15].

Lapse nõusolek

Määrus rõhutab, et erilist tähelepanu tuleb pöörata laste isikuandmete kaitsele. Seda eriti olukorras, kus andmeid kogutakse otse lastelt, samuti juhtudel, kui laste isikuandmeid kasutatakse turunduse eesmärgil, kasutajaprofiili loomiseks või otse lastele pakutavate teenuste puhul. Lapsed ei pruugi olla

[15] AKI nõusoleku kontrollnimekiri: http://www.aki.ee/et/andmekaitse-reform/nousoleku-kontrollnimekiri

piisavalt teadlikud ohtudest ega oma õigustest seoses isikuandmete töötlemisega ja seetõttu on väga oluline, et lapsele edastatakse see teave lihtsas ja selges sõnastuses.

Laps on nii lastekaitseseaduse (§ 3 lg 2)[16] kui tsiviilseadustiku üldosa seaduse (§ 8 lg 2)[17] järgi alla 18-aastane inimene. Kuni lapse 18-aastaseks saamiseni teevad tema eest otsuseid, mis toovad endaga kaasa õiguslikke tagajärgi (sh isikuandmete töötlemiseks nõusoleku andmine), lapse vanemad (eestkostja).

Määrus sätestab siinkohal erisuse nõusoleku andmisele, kui seda on vaja infoühiskonna teenuste pakkumiseks otse lapsele, näiteks kasutajakonto loomisel mõne veebiteenuse kasutamiseks. Määrus näeb ette, et vähemalt 16-aastane isik võib sellises olukorras anda ise nõusoleku oma isikuandmete töötlemiseks. Samas annab määrus liikmesriikidele õiguse kehtestada madalam vanusepiirang, kuid mitte alla 13 aasta. Juhendi koostamise hetkel on IKS-i eelnõus sätestatud vanusepiiriks Eestis 13 eluaastat. Oluline on arvestada, et IKS-i regulatsioonist saab lähtuda alles pärast seaduse jõustumist.

Infoühiskonna teenuste puhul lapse seadusliku esindaja nõusolekut ei eeldata, kui tegemist on lapsele otse pakutavate ennetavate või nõustamisteenustega, mille eesmärgiks on lapse huvide kaitsmine. *Näiteks võib lapse huvides infoühiskonna teenusteks pidada lapsemure.ee vms lastele suunatud nõustamisfoorumeid.*

Oluline on meeles pidada, et alandatud vanusepiir kehtib üksnes nõusoleku andmisel isikuandmete töötlemiseks infoühiskonna teenuste pakkumisel otse lapsele. Kõikidel muudel juhtudel on endiselt vajalik lapse seadusliku esindaja nõusolek lapse isikuandmete töötlemiseks kuni lapse 18-aastaseks saamiseni.

Kui on vaja, et lapse eest annab nõusoleku seaduslik esindaja, peab haridusasutus veenduma, et nõusoleku annab õige isik. *Näiteks sõltuvalt võimaliku riski suurusest tuleb siinjuures otsustada, kas nõusoleku saamiseks piisab e-kirjast või on selleks vajalik lapse seadusliku esindaja kindlam tuvastamine – nõusoleku esitamine digitaalselt allkirjastatuna või õpihaldussüsteemi sisselogituna.*

2.2 Läbipaistvus ja teavitamine

Üks määruse kesksetest põhimõtetest on õiglane ja läbipaistev töötlemine. Sellest tulenevalt on vastutaval töötlejal kohustus esitada kõigile neile, kelle andmeid ta töötleb, teavet isikuandmete töötlemise tingimuste ning isiku õiguste kohta (n-ö privaatsuspoliitika).

Teave, mis tuleb admesubjektile teatavaks teha, on loetletud määruse artiklites 13 ja 14.

Juhul kui isikuandmed kogutakse andmesubjektilt endalt, tuleb talle anda järgmine teave:

- vastutava töötleja nimi ja kontaktandmed;
- andmekaitsespetsialisti kontaktandmed;
- kui isikuandmete töötlemine põhineb õigustatud huvil, siis teave vastutava töötleja või kolmanda isiku õigustatud huvide kohta;
- asjakohasel juhul teave isikuandmete vastuvõtjate või vastuvõtjate kategooriate kohta;
- asjakohasel juhul teave selle kohta, et vastutav töötleja kavatseb edastada isikuandmed kolmandale riigile või rahvusvahelisele organisatsioonile, ning viide kaitsemeetmetele ja nende koopia saamise viisile või kohale, kus need on tehtud kättesaadavaks;
- isikuandmete säilitamise ajavahemik või kui see ei ole võimalik, sellise ajavahemiku määramise kriteeriumid;
- teave õiguse kohta taotleda vastutavalt töötlejalt juurdepääsu isikut puudutavatele isikuandmetele, nende andmete parandamist või kustutamist. Andmesubjektil on õigus nõuda isikuandmete töötlemise piiramist ja saada teavet isikuandmete ülekandmise õiguse kohta. Samuti on õigus esitada

[16] Lastekaitseseadus (RT I, 06.12.2014, 1) https://www.riigiteataja.ee/akt/128112017019?leiaKehtiv
[17] Tsiviilseadustiku üldosa seadus (RT I 2002, 35, 216) https://www.riigiteataja.ee/akt/120042017021?leiaKehtiv

vastuväide isikuandmete töötlemisele, kui andmeid töödeldakse seadusliku aluseta ja/või need on valed;
- kui andmete töötlemise aluseks on nõusolek, siis teave õiguse kohta nõusolek igal ajal tagasi võtta, ilma et see mõjutaks enne tagasivõtmist nõusoleku alusel toimunud töötlemise seaduslikkust;
- teave õiguse kohta esitada kaebus järelevalveasutusele;
- teave selle kohta, kas isikuandmete esitamine on õigusaktist või lepingust tulenev kohustus või lepingu sõlmimiseks vajalik nõue, samuti selle kohta, kas andmesubjekt on kohustatud kõnealuseid isikuandmeid esitama, ning teave selliste andmete esitamata jätmise võimalike tagajärgede kohta;
- teave automatiseeritud otsuste, sealhulgas profiilianalüüsi tegemise kohta ning vähemalt nendel juhtudel sisuline teave kasutatava loogika ja selle kohta, milline on isikuandmete töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks.

Juhul kui andmed ei ole pärit isikult endalt, vaid teistest allikatest (näiteks riiklikud registrid), siis tuleb lisaks informeerida inimest andmete töötlemise alustamisest, isikuandmete päritoluallikast ning asjakohasel juhul anda infot selle kohta, kas need pärinevad avalikult kättesaadavatest allikatest. Seda tuleb teha mõistliku aja jooksul pärast isikuandmete saamist, kuid hiljemalt ühe kuu jooksul.

Näiteks on vaja leida õpilase vanemad mingi kiireloomulise informatsiooni edastamiseks, kuid eelnevalt ei ole need õpetajale kättesaadavad, aga on teada lapsevanema töökoht. Võimalus on leida kontaktandmed äriregistrist, ettevõtte veebilehelt või otsimootoritega. Kui neid andmeid kasutatakse vaid sellel ühel juhtumil lapsevanema informeerimiseks, siis ei ole vajalik lapsevanema teavitamine tema isikuandmete töötlemise kohta. Kui aga on selge kavatsus kanda saadud andmed kooli kontaktide andmebaasi, siis tuleb lapsevanemat sellest teavitada vastavalt määruse artiklile 14. Ilmselt parim hetk selleks on kohe, kui ühendust võetakse. Kui see hetk ei ole sobiv, tuleb lapsevanemat teavitada kuu aja jooksul.

2.3 Isikuandmete töötlemise eesmärgi piirang

Isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud eesmärkidel ning neid ei ole lubatud töödelda hiljem muul otstarbel (välja arvatud avalikes huvides toimuv arhiveerimine, teadus- või ajaloouuringud või statistilised eesmärgid). Juhul, kui andmete töötlemise eesmärk muutub ja andmete töötlemine on jätkuvalt vajalik, on vastutaval ja/või volitatud töötlejal kohustus enne andmete töötlemise alustamist teavitada kõiki andmesubjekte andmetöötluse muutunud eesmärgist.

Näiteks ei tohi lapsevanemate e-posti aadresse, mis on kogutud viitega vajadusele edastada koolieluga seotud infot, kasutada kolmandate isikute reklaami (kursused, laagrid vms) edastamiseks.

2.4 Isikuandmete minimaalsuse printsiip

Isikuandmeid kogudes ja töödeldes tuleb jälgida, et ei kogutaks andmeid, mida andmete töötlemise eesmärgi saavutamiseks tegelikult vaja ei ole. Reeglina ei ole „igaks juhuks“ isikuandmete kogumine õigustatud.

Näiteks küsitakse haridusasutuses sageli lapsevanematelt andmeid nende ameti ja/või töökoha kohta või vanema arvelduskonto numbrit, kuigi neid andmeid ei ole vaja haridusteenuse pakkumiseks. Lapsevanema amet ja töökoht ei ole üldjuhul haridusasutuse ja lapsevanema suhtluseks vajalik ning konto numbrit on vaja vaid erandjuhul (näiteks makstud tasu tagastamiseks). Seetõttu on korrektne küsida arvelduskonto andmeid vaid sellelt lapsevanemalt, kellele on vaja teostada tagasimakse, mitte igaks juhuks kõikidelt lapsevanematelt.

2.5 Isikuandmete õigsus

Isikuandmete töötleja peab tagama, et kogutud andmed on õiged ja vajadusel ajakohastatud ning kasutusel on mõistlikud meetmed, et töötlemise eesmärgi seisukohast ebaõiged isikuandmed kustutatakse või parandatakse viivitamata.

Seda saab tagada näiteks sellega, et andmete esitajale pannakse kohustus andmete muutumisel sellest esimesel võimalusel andmete töötlejat teavitada. Andmete ajakohasust aitavad tagada andmete ajakohastamise võimalikult lihtsaks ja mugavaks tegemine, näiteks selleks veebikeskkonna loomine või andmete uuendamiseks meeldetuletuskirjade saatmine.

Sealjuures tuleb jälgida, et andmetöötluseks kasutatavad lahendused võimaldaksid ebaõigete andmete kustutamist või parandamist. Infosüsteemide puhul on oluline, et andmete muutmine ja kustutamine oleks süsteemi logidest tuvastatav.

2.6 Isikuandmete säilitamise piirang

Isikuandmeid võib säilitada üksnes nii kaua, kui on isikuandmete töötlemise eesmärgi täitmiseks vajalik.

Näiteks kui konkurss ametikoha täitmiseks on lõppenud ja tulemuste vaidlustamise tähtaeg on möödas, siis ei ole alust säilitada kõigi kandideerijate andmeid.

Isikuandmete säilitamise tähtajad võivad tulla õigusaktidest[18], haridusasutuse siseregulatsioonidest (nt dokumentide loetelu/liigitusskeem) või töökorralduslikest kokkulepetest. Säilitustähtaja möödumisel tuleb andmed kustutada/hävitada.

Isikuandmeid ei tohi säilitada „äkki kunagi läheb vaja“ põhjusel.

2.7 Usaldusväärsus ja konfidentsiaalsus

Isikuandmete töötlemisel tuleb tagada andmete turvalisus, kaitstes neid muuhulgas loata või ebaseadusliku töötlemise ning juhusliku kaotamise, hävitamise või kahjustumise eest.

Näiteks peab koolis kasutusel olev õpihaldussüsteemi kasutajaõiguste süsteem tagama selle, et süsteemis olevatele andmetele on ligipääs vaid selleks põhjendatult õigustatud ja vastavat volitust omavad töötajad ning nende töötajate töölepingus vms dokumendis on reguleeritud nende konfidentsiaalsuskohustus tööülesannete täitmisel teatavaks saanud isikuandmete osas.

Turvalisuse tagamisest on lähemalt juttu peatükis „Meetmed andmete kaitseks“.

2.8 Vaikimisi ja lõimitud isikuandmete kaitse

Isikuandmete kaitsega tuleb tegeleda pidevalt ning riske ennetades, mitte alles probleemi tekkides.

Lõimitud andmekaitse põhimõte tähendab, et haridusasutuse andmekaitse meetmed peavad alati olema ennetavad ja ärahoidvad, mitte tagantjärele reageerivad ja korrigeerivad. Andmekaitse meetmed peaksid organisatsioonis olema läbi mõeldud ja rakendatud selliselt, et kõik isikuandmed oleksid kaitstud kogu andmetöötlusprotsessi elutsükli jooksul – andmebaasi loomisest kuni andmete töötlemise täieliku lõppemise ja andmete jäädava kustutamiseni. Isikuandmete töötlemise kogu protsess peab olema selge ja läbinähtav ning seejuures ka andmesubjektile arusaadav.

Vaikimisi andmekaitse põhimõte tähendab, et haridusasutus töötleb neid ja ainult neid isikuandmeid, mis on vajalikud töötlemise eesmärgi saavutamiseks ning millel on olemas andmetöötluse õiguslik alus.

[18] näiteks Koolieelse lasteasutuse õppe- ja kasvatustegevuse alaste kohustuslike dokumentide loetelu ja nende täitmise kord - https://www.riigiteataja.ee/akt/120022018032?leiaKehtiv; Kooli õppe- ja kasvatusalastes kohustuslikes dokumentides esitatavad andmed ning dokumentide täitmise ja pidamise kord - https://www.riigiteataja.ee/akt/13352237# ; töölepingu seadus §5 lg 5 - https://www.riigiteataja.ee/akt/128122017043?leiaKehtiv#para5

Sisuliselt tähendab see, et püütakse ennetada teada olevaid ohte ning rakendatakse meetmeid, et ka uute tehnoloogiate tulekul oleks isikuanded hästi kaitstud.

Samuti on oluline pidevalt tagada meetmed, et teada olevad riskid oleks kontrollitud tasemel. *Näiteks süle- või tahvelarvuti sisse lülitamisel ei tohiks olla WiFi, sinihammas või asukohateenus vaikimisi aktiveeritud, arvuti veebilehitseja turvaseaded ei tohiks vaikimisi võimaldada inimese veebikasutuse ulatuslikku jälgimist, suhtlusrakendustes või sotsiaalmeedia teenustes peab olema vaikimisi andmete jagamine piiratud. Kasutaja ise otsustab, kellele ja millised andmeid ta kättesaadavaks teeb.*

Vaikimisi ja lõimitud andmekaitse põhimõtted ühtivad siinjuures ka eelpool käsitletud andmete töötlemise minimaalsuse põhimõttega. Ei tohiks küsida ja töödelda andmeid, mis ei ole otseselt vajalikud kavandatava tegevuse läbiviimiseks.

Vaikimisi ja lõimitud isikuandmete kaitse põhimõtte rakendamise põhjalikum kirjeldus on toodud AKI veebilehel.[19]

3. Andmesubjekti õigused

Määruse kolmas peatükk kirjeldab andmesubjekti õiguseid:

- läbipaistvus ja õigus teabele;
- õigus tutvuda kogutud isikuandmetega;
- õigus isikuandmete parandamisele ja kustutamisele (õigus olla unustatud);
- õigus isikuandmete töötlemise piiramisele;
- isikuandmete ülekantavuse õigus;
- õigus esitada vastuväiteid oma isikuandmete töötlemisele.

Loetelust on näha, et määruse eesmärk on anda andmesubjektile senisest suurem ja selgemalt sõnastatud otsustusõigus oma isikuandmete töötlemise üle.

Järgnevalt käsitletakse lähemalt nimetatud õiguseid ja seda, kuidas nad haridusasutuse tegevusi mõjutavad.

3.1 Läbipaistvus ja õigus teabele

Isikuandmete töötlemisega seotud teave ja sõnumid peavad olema kergesti kättesaadavad, arusaadavad ning selgelt ja lihtsalt sõnastatud. Erilist tähelepanu tuleb suunata lastele suunatud tekstide sõnastamisele.

Näiteks peab olema andmesubjektil võimalik saada teada: kes on vastutav töötleja? Mis on andmete töötlemise eesmärk ja töötlemisega seotud ohud? Millised on kasutatavad kaitsemeetmed ja andmesubjekti õigused?

Teabe kätte saamise lihtsus ei tähenda siin igaühe juurdepääsu informatsioonile ja isikuandmetele, vaid isikuandmete töötlejad peavad olema läbi mõelnud, kuidas andmesubjekte on teavitatud ning kuidas nad saavad lihtsalt esitada päringuid oma isikuandmete töötlemise kohta ning kuidas neile vastatakse.

Päringu vastuseks võib olla turvalise juurdepääsu andmine päringu esitajale tema enda isikuandmetele. Heaks eeskujuks on siin võimalus oma isikuandmetega tutvuda eesti.ee portaalis.

Teavitamiskohustus on täpsemalt reguleeritud määruse artiklites 13 (andmed on saadud andmesubjektilt) ja 14 (andmed ei ole saadud andmesubjektilt). Lisaks eeltoodule saab vajaliku teabe kättesaadavaks teha asutuse veebilehel dokumendina, mida nimetatakse privaatsuspoliitikaks, privaatsusreegliteks, isikuandmete töötlemise põhimõteteks, isikuandmete töötlemise korraks vms. Tegemist on dokumendiga, kus kirjeldatakse ammendavalt asutuse isikuandmete töötlemise praktikat. Lugeja peab sellest dokumendist saama piisava info selle kohta, milliseid andmeid, kuidas ja kui kaua

[19] http://www.aki.ee/et/andmekaitse-reform/vaikimisi-ja-loimitud-andmekaitse

asutus töötleb ning kellele edastab. Sealjuures ei tohi unustada ka andmeid, mida kogutakse tehniliste lahenduste vahendusel, näiteks infosüsteemide logid, sissepääsusüsteemide logid, videovalve salvestised, veebilehe küpsised ja külastusandmed jne.

3.2 Õigus tutvuda kogutud isikuandmetega

Isikul on õigus teada, kas tema andmeid töödeldakse ning kui töödeldakse, siis mis on töötlemise eesmärk, millist liiki andmeid töödeldakse, kellele on andmed kättesaadavad, milline on andmete säilitamise aeg ja millised on tema õigused. Isikul on ka õigus saada oma isikuandmetest väljavõte, v.a juhul, kui sellega kahjustataks teiste isikute õigusi või vabadusi.

Näiteks ei pea isik saama oma isikuandmete väljavõtet juhul, kui selle käigus saaks avalikuks kellegi ärisaladus, teiste isikute isikuandmed või rikutakse sellega teise isiku autoriõigusi.

Haridusasutustel oleks otstarbekas teha oma veebilehel (nt privaatsuspoliitika osana) teatavaks, kuidas ja kellele tuleks esitada taotlused isikuandmetega tutvumiseks. Kui taotlus on esitatud elektrooniliselt, esitatakse ka teave üldkasutatavate elektrooniliste vahendite kaudu, kui andmesubjekt ei taotle teisiti.

Reeglina tuleb isikuandmete väljavõte esitada taotlejale tasuta, kuid kui isik taotleb lisakoopiaid, võib vastutav töötleja küsida mõistlikku tasu halduskulude katmiseks. Samuti on õigus küsida mõistlikku tasu, kui isikuandmete töötleja tõendab, et andmesubjekti taotlus on selgelt põhjendamatu.

Haridusasutus peab veenduma, et isikuandmete saamiseks taotluse esitanud isik taotleb iseenda või oma alaealise lapse andmeid, küsides selleks vajadusel täiendavat informatsiooni.

3.3 Õigus isikuandmete parandamisele ja kustutamisele (õigus olla unustatud)

Isikul on õigus nõuda, et tema ebaõiged isikuandmed parandataks ning mittetäielikud täiendataks, üleliigsed kustutataks.

Isikuandmed tuleb põhjendamatu viivituseta kustutada, kui kehtib vähemalt üks järgmisest loetelust:

- isikuandmeid ei ole enam vaja sellel eesmärgil, millega seoses need on kogutud või muul viisil töödeldud, sh kui andmete säilitustähtaeg lõpeb;
- isik võtab töötlemiseks antud nõusoleku tagasi ning puudub muu õiguslik alus isikuandmete töötlemiseks;
- andmesubjekt esitab põhjendatud vastuväite isikuandmete töötlemise suhtes ja töötlemiseks pole ülekaalukaid õiguspäraseid põhjuseid;
- isikuandmeid on töödeldud ebaseaduslikult;
- isikuandmed tuleb kustutada selleks, et täita vastutava töötleja juriidilist kohustust;
- juhul, kui isikuandmeid koguti ja töödeldi seoses alaealisele infoühiskonna teenuste pakkumisega ning andmesubjekt ise või tema seaduslik esindaja (kui nõusoleku on andnud seaduslik esindaja) on esitanud taotluse andmetöötluse lõpetamiseks.

Juhul kui vastutav töötleja on isikuandmed avalikustanud/volitatud töötlejale edastanud ja peab isikuandmed kustutama, on tal kohustus teha kõik mõistlike kättesaadavate vahendite ja kulude piires, et teavitada teisi andmeid töötlevaid isikuid kustutamise kohustusest. See kohustus hõlmab ka asjakohaste isikuandmetele osutavate linkide või andmekoopiate või -korduste kustutamist.

Õigus isikuandmete kustutamisele ei kehti selliste andmete puhul, mida töödeldakse õigusakti alusel või lepingu täitmiseks ning isikuandmete töötlemise eesmärk ei ole ära langenud, sealhulgas ei ole saabunud kogutud andmete säilitamise lõpptähtaeg.

Näiteks ei saa nõuda töölepingu kirjalikus dokumendis toodud isikuandmete kustutamist, kui töösuhte lõpetamisest on möödunud vähem kui kümme aastat (TLS §5 lg 5); õpilasraamatus toodud isikuandmete kustutamist ei saa üldse nõuda, sest neile andmetele on määratud alaline säilitamise tähtaeg[20].

Samas saab nõuda enda andmete kustutamist kooli vilistlaste avalikust nimekirjast ja enda või oma alaealise lapse andmete eemaldamist kooli autahvlilt. Keeruline, kui mitte võimatu on nõuda unustamist juba trükikujul ilmunud vilistaste raamatute ja muude juba ilmunud pabertrükiste puhul.

3.4 Õigus töötlemise piiramisele

Isikul on õigus nõuda isikuandmete töötlemise piiramist, kui

- isik vaidlustab isikuandmete õigsuse (ajaks, mis võimaldab vastutaval töötlejal isikuandmete õigsust kontrollida);
- isikuandmete töötlemine on ebaseaduslik, kuid andmesubjekt ei taotle isikuandmete kustutamist, vaid kasutamise piiramist;
- vastutav töötleja ei vaja isikuandmeid enam töötlemise eesmärgil, kuid need on isikule vajalikud õigusnõuete koostamiseks, esitamiseks või kaitsmiseks;
- isik on esitanud isikuandmete töötlemise suhtes vastuväite. Sellisel juhul tuleb piirata isikuandmete töötlemist, kuni selgitatakse välja, kas andmete töötlemine on õiguspärane.

Töötlemise piiramise olukorras on lubatud üksnes isikuandmete säilitamine, kõiki teisi töötlustoiminguid võib teha ainult isiku nõusolekul või seoses isiku enda või teiste õiguste kaitsmise või olulise avaliku huviga.

Näiteks kui isik vaidlustab infosüsteemis olevate isikuandmete õigsuse, siis tuleb tagada, et andmete õigsuse kontrollimise ajal ei ole need isikuandmed ühekski töötlustoiminguks kättesaadavad, v.a kui sellise võimaluse loomine ei ole tehniliselt võimalik või on ebaproportsionaalselt kulukas.

3.5 Isikuandmete ülekantavuse õigus

Isikul on õigus saada isikuandmete töötlejalt tema kohta käivaid isikuandmeid struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul. Õigus laieneb üksnes isikuandmete automatiseeritud töötlemisele ja isikuandmetele, mille isik on töötlejale ise esitanud ning kui isikuandmete töötlemine toimub andmesubjekti nõusoleku alusel või temaga sõlmitud lepingu täitmiseks/tagamiseks. Avaliku ülesande ja juriidilise kohustuse täitmiseks töödeldavatele isikuandmetele ülekantavuse õigus ei laiene.

Näiteks kui haridusasutus töötleb isiku nõusoleku alusel või lepingu täitmiseks isikuandmeid elektroonilisel kujul (nt inimene soovib täiendusõppes kursustel osalemisega ja tulemustega seotud andmed kanda üle teise haridusasutuse täiendusõppe programmi), siis on isikul õigus saada need andmed masinloetaval kujul laialdaselt kasutatavas avatud vormingus (nt XML-, CSV- vms failina). Failivormingu valimisel on asutusel õigus lähtuda enda võimalustest, kuid peab arvestama ka andmesubjekti võimalusega võimalikult mugavalt andmeid uuesti kasutada.

3.6 Õigus esitada vastuväiteid oma isikuandmete töötlemisele

Õigus esitada vastuväiteid oma isikuandmete töötlemisele rakendub isikuandmete töötlemisel otseturunduse eesmärgil; õigustatud huvi / avalikes huvides oleva ülesande täitmisel ning teadus-, ajaloo- ja statistiliste uuringute puhul. Õigusest esitada vastuväiteid oma isikuandmete töötlemisele tuleb isikut teavitada (v.a teadus-, ajaloo- ja statistiliste uuringute puhul). Otseturunduse eesmärgil

[20] Kooli õppe- ja kasvatusalastes kohustuslikes dokumentides esitatavad andmed ning dokumentide täitmise ja pidamise kord § 6 - https://www.riigiteataja.ee/akt/13352237#para6

isikuandmete töötlemisel vastuväidete esitamist põhjendama ei pea, teistel alustel peab isik viitama teda mõjutavale põhjusele ning isikuandmete töötlejal on kohustus iga sellise taotluse põhjendatust uurida üksikjuhtumina.

Nagu eelpool toodud, siis riigi ja KOVi hallatavad haridusasutused täidavad avalikku ülesannet, kuid reeglina siin ei rakendu isikuandmete töötlemisele vastuväite esitamise õigus kuna lisaks avaliku ülesande täitmisele tuleb samade isikuandmete töötlemise alus ka õigusaktidest ehk töötlemise aluseks on ka juriidiline kohustus.

Isikuandmete töötleja peab panema paika, kuidas käitutakse, kui keegi esitab oma isikuandmete töötlemisele vastuväite, nt kuidas tagatakse, et otseturundusest keeldudes sellel eesmärgil isikuandmeid rohkem ei töödelda.

4. Andmekaitsespetsialist

Määrus sisustab uue mõiste, milleks on andmekaitseametnik või andmekaitsespetsialist (*Data Protection Officer – DPO*; edaspidi on tekstis kasutusel termin „andmekaitsespetsialist“) ning näeb ette teatud juhtudel organisatsioonides kohustuse andmekaitsespetsialisti ülesannete täitja määramiseks.

Määruse sissejuhatuse punkt 97 järgi on andmekaitsespetsialist isik, kes tunneb andmekaitsealaseid õigusakte ja tavasid eksperdi tasemel ning kelle ülesandeks on nõustada ja kontrollida isikuandmete töötleja isikuandmete töötlemise vastavust määruse nõuetele.

AKI on koostanud nimekirja soovituslikest teadmistest ja oskustest, mis võimaldavad andmekaitsespetsialisti rolli tulemuslikult täita[21].

Andmekaitsespetsialisti peavad määrama

- isikuandmeid töötlev avaliku sektori asutus või organ, kusjuures siin peetakse silmas kõiki asutusi ja ka eraõiguslikke isikuid, kes täidavad avalikke ülesandeid;
- isikuandmete töötleja, kelle põhitegevus on andmesubjektide ulatuslik, korrapärane ja süstemaatiline jälgimine;
- isikuandmete töötleja, kelle põhitegevus on eriliiki isikuandmete ulatuslik töötlemine.

Enamus Eesti haridusasutusi täidab avalikke ülesandeid ja on seega avaliku sektori asutused ning peavad määrama andmekaitsespetsialisti.[22] Kahes teises aluses toodud „põhitegevuse“ all tuleb mõista seda, et tegemist on andmetöötleja võtmetegevusega, ilma milleta ei saa ta oma igapäevaseid tegevuseesmärke täita. *Haridusasutus näiteks ei saa oma ülesandeid täita ilma isikuandmeid töötlemata*. Kuid tavapäraselt ei ole haridusasutuse põhitegevusena käsitletav eriliiki isikuandmete töötlemine (erandiks on erivajadusega lastele/noortele suunatud haridusasutused) või isikuandmete töötlemine viisil, mis tingib andmesubjekti süstemaatilise jälgimise.

[21] Andmekaitsespetsialisti kompetentside loetelu on leitav aadressilt http://www.aki.ee/et/andmekaitse-reform/andmekaitsespetsialisti-ulesanded-teadmised-ja-oskused

[22] Vt lisaks Euroopa andmekaitseasutuste töörühm on välja töötanud andmekaitsespetsialisti suunised (inglise keeles) http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/guidelines_dpos.pdf

4.1 Andmekaitsespetsialisti määramise võimalused

Kui asutusel on kohustus määrata andmekaitsespetsialist, tuleb asutuse spetsiifikast lähtudes (sisendiks saab olla andmete kaardistuse tulemus) otsustada, kui suur on selle ametikoha koormus. Seejärel saab otsustada, kas antud ametikoha ülesandeid asub täitma mõni olemasolev töötaja, kellele võimaldatakse vajalikke täienduskoolitusi, või värvatakse uus erialateadmistega töötaja. Suurte organisatsioonide puhul võib osutuda otstarbekaks ka mitme positsiooni (eraldi üksuse) loomine. Alternatiiv on ka andmekaitsespetsialisti teenuse sisseost organisatsioonivälistelt juriidiliselt või füüsiliselt isikult teenuslepingu alusel.

4.1.1 Andmekaitsespetsialisti ametikoha loomine

Andmekaitsespetsialisti rolli võib täita nii eraldi inimene kui allüksus. Andmekaitsespetsialist ei pea oma ülesanded täitma üksi, erinevate ülesannete täitmisse võib kaasata meeskonna.

Andmekaitsespetsialisti rolli võib ühendada mõne teise olemasoleva töötaja rolliga, kuid selle käigus ei tohi tekkida rollikonflikti olukorda, kus andmekaitsespetsialist peab andmekaitsespetsialisti ülesannete kõrval otsustama isikuandmete töötlemise eesmärkide ja vahendite üle ning samas andma nende isikuandmete kaitse põhimõtetele vastavuse osas n-ö kõrvalseisja hinnangu.

Näiteks kui direktor, personalijuht või IT-juht, kes reeglina otsustab oma töövaldkonna isikuandmete töötlemise eesmärkide ja vajalike vahendite üle, oleks samaaegselt andmekaitsespetsialist, ei saa ta enda tehtud otsuseid hinnata kõrvalseisjana. Küll saab andmekaitsespetsialisti ülesandeid täita töötaja, kelle puhul sellist konflikti ei esine ning kellel on olemas vajalikud teadmised andmekaitsespetsialisti ülesannete täitmiseks.

Selleks et andmekaitsespetsialist saaks oma tööd tulemuslikult teha, tuleb jälgida järgmisi põhimõtteid:

- andmekaitsespetsialist annab aru kõrgeimale juhtkonna tasemele, mis tagab selle, et kõrgeim juhtimistase on teadlik valdkonna spetsialisti nõuannetest ja soovitustest. Samas on juhtkonnal kohustus kaasata andmekaitsespetsialisti kõikidesse isikuandmete kaitsega seotud küsimustesse;
- andmekaitsespetsialistile eraldatakse piisavad ressursid oma töö tegemiseks;
- andmekaitsespetsialist saab teha oma tööd sõltumatult.

Andmekaitsespetsialisti sõltumatuse tagamiseks on oluline, et juhtkond ei mõjutaks tema tööd ja töö tulemusi.

Näiteks ei tohi anda konkreetseid juhiseid andmekaitsespetsialisti töö tulemustele; ei või kirjutada ette, milline peaks olema kaebuste lahendamise tulemus; mida ta võib/ei või järelevalveasutusele teatada, samuti milline peaks olema tema seisukoht mõnda valdkonna seadust tõlgendades.

Andmekaitsespetsialistile peab olema tagatud võimalus jääda vastutava või volitatud töötleja otsuste osas eriarvamusel ning teha oma eriarvamus teatavaks haridusasutuse juhtkonnale/haridusasutuse pidajale, kui tema hinnangul ei ole tehtud otsus määrusega kooskõlas ning ta on eelnevalt vastuolule viidanud.

Andmekaitsespetsialisti sõltumatuse oluliseks osaks on garantii, et andmekaitsespetsialisti karistamise või töösuhte lõpetamise alus ei saa olla nõuetele vastav andmekaitsespetsialisti tööülesannete täitmine.

4.1.1.1 Ühine andmekaitsespetsialist

Mitme haridusasutuse (avaliku sektori asutus/organ) jaoks võib määrata ka ühe andmekaitsespetsialisti. Sellisel juhul on oluline eelnevalt analüüsida, kas üks isik suudab vastata samal ajal kõigi haridusasutuste, kelle heaks ta töötab, vajadustele ning vajadust tagada talle igas organisatsioonis täiendav abi teiste töötajate näol.

Näiteks võivad kaks haridusasutust otsustada palgata ühe inimese mõlemasse asutusse või palkab väiksem kohalik omavalitsus ühe inimese tegelema kõigi oma haridusasutuste isikuandmete kaitse küsimustega.

4.1.2 Asutusevälise andmekaitsespetsialisti kaasamine

Koosseisulise töötaja asemel võib andmekaitsespetsialisti ülesandeid täita isikuandmete töötleja organisatsioonivälise (füüsiline või juriidiline) isik, kellega tuleb sõlmida teenuse osutamiseks leping. Selline töökorraldus võimaldab vältida lisatööjõu palkamist ning samal ajal kombineerida andmekaitsespetsialisti töös erinevate inimeste oskusi ja tugevusi (nt süvendatud juriidilisi ja infoturbe teadmisi), kui teenust osutab füüsiline isik, kelle meeskonnas on erinevad pädevused esindatud ning see on teenuse osutamise lepinguga kokku lepitud.

Teenusepakkujat valides ning temaga lepingut sõlmides tuleb jälgida, et

- iga andmekaitsespetsialisti ülesandeid täitev meeskonnaliige vastaks kõigile andmekaitsespetsialistile esitatud nõuetele. Eriti oluline on, et ei esineks huvide konflikti;
- igale meeskonnaliikmele oleks kindlustatud andmekaitsespetsialisti sõltumatuse garantii. *Näiteks ei tohi teenuslepingut ebaõiglaselt lõpetada andmekaitsespetsialistina tehtud õiguspäraste toimingute tõttu.*

Juhul kui andmekaitsespetsialisti ülesandeid täidab välise partneri meeskond, siis on oluline teenuse osutamise lepingus sätestada haridusasutuse jaoks üks konkreetne kontakt, kes vastab avalikkusele ja järelevalveasutusele isikuandmete kaitsega seotud küsimustes.

4.2 Andmekaitsespetsialisti töö sisu

Määruse artiklis 39 on kirjeldatud andmekaitsespetsialisti ülesandeid:

- teavitada ja nõustada vastutavat või volitatud töötlejat ning isikuandmeid töötlevaid töötajaid seoses nende kohustustega, mis tulenevad määrusest ja muudest andmekaitsenormidest;
- jälgida andmekaitse määruse, muude andmekaitsenormide ja vastutava töötleja või volitatud töötleja isikuandmete kaitse põhimõtete järgimist, sealhulgas vastutusvaldkondade jaotamist, isikuandmete töötlemises osaleva personali teadlikkuse suurendamist ja koolitamist ning eelnevaga seonduvat auditeerimist;
- anda nõu seoses andmekaitsealase mõjuhinnanguga ning jälgida selle toimimist;
- teha koostööd järelevalveasutusega;
- tegutseda isikuandmete töötlemise küsimustes järelevalveasutuse jaoks kontaktisikuna.

Andmekaitsespetsialisti tööülesanded, nende ulatus ja vastutus peaks olema andmekaitsespetsialistiga sõlmitavas lepingus selgelt välja kirjutatud ning nii juhtkonnale kui kõigile töötajatele edastatud.

Selleks et andmekaitsespetsialist saaks oma tööd tulemuslikult teha, on oluline, et teda nähtaks organisatsioonis valdkonna partnerina, kellest on organisatsiooni jaoks kasu, mitte üksnes järelvalvaja ja kontrollijana. Teda tuleks kaasata isikuandmete kaitsega puutumust omavatesse aruteludesse ning üldse kõikidesse isikuandmete kaitsega seotud küsimustesse võimalikult vara.

AKI on andnud andmekaitsespetsialisti kaasamiseks järgmised soovitused:

- andmekaitsespetsialist kutsutakse regulaarselt osalema tipp- ja keskastmejuhtide koosolekutele;
- andmekaitsespetsialist kaasatakse otsuste tegemisse, millel on andmekaitsega seotud mõju. Kogu asjakohane teave tuleb andmekaitsespetsialist edastada aegsasti, et ta saaks anda õiget nõu;
- andmekaitsespetsialisti arvamust tuleb alati piisavalt kaaluda;
- andmekaitsespetsialistiga tuleb konsulteerida kohe, kui on toimunud andmetega seotud rikkumine või mõni muu vahejuhtum.

Järgnevalt on vaadeldud andmekaitsespetsialisti tööülesandeid ja vastutust konkreetsete töölõikude näitel.

Isikuandmete kaitse nõuete täitmise jälgimine

Määruse nõuete täitmise jälgimine tähendab eelkõige järgmisi tegevusi:

- teabe kogumine isikuandmete töötlemise toimingute kohta;
- isikuandmete töötlemise toimingute õiguspärasuse analüüs ja kontrollimine;
- vastutava või volitatud töötleja teavitamine ning neile nõu ja soovituste andmine.

See tähendab, et andmekaitsespetsialist ei vastuta määruse nõuete järgimise eest. Andmekaitsenõuete järgimine on andmete vastutava töötleja kui asutuse, mitte andmekaitsespetsialisti kohustus. Andmekaitsespetsialist vastutab selle eest, et ta on andmekaitse põhimõtetega kursis, analüüsib olukorda, teavitab õigel ajal võimalikest probleemidest ning teeb ettepanekuid, kuidas saavutada määruse nõuetega vastavus.

Andmekaitsealase mõjuhinnanguga seotud tööülesanded

Andmekaitsealase mõjuhinnangu tegemine on vastutava töötleja ja mitte andmekaitsespetsialisti kohustus. Andmekaitsealase mõjuhinnanguga seoses on andmekaitsespetsialisti ülesanne eeskätt anda nõu. Andmekaitsespetsialisti nõuannetega mitte nõustumist peab andmekaitsealase mõjuhinnangu dokumendis kirjalikult põhjendama.

Andmekaitsespetsialisti kaasamine on mõistlik järgmiste küsimuste otsustamisel:

- enne mõjuhinnangu tegemist: kas andmekaitsealase mõjuhinnangu tegemine on vajalik; kas teha mõjuhinnang ise või tellida teenusena sisse; milline võiks olla parim meetod konkreetse mõjuhinnangu läbiviimiseks;
- mõjuhinnangu koostamisel: milliseid tehnilisi, organisatsioonilisi või muid kaitsemeetmeid võtta kasutusele, et maandada isikuandmete töötlemisel andmesubjektide õiguste ja huvidega seotud riske;
- mõjuhinnangu koostamise järel: kas andmekaitsealane mõjuhinnang on tehtud kooskõlas määrusega ning kas mõjuhinnangu järeldused vastavad määruse nõuetele.

Andmekaitsespetsialisti ülesanded toimingute registreerimisel

Määrus paneb isikuandmete töötlemise toimingute registreerimise ja registri pidamise kohustuse vastutavale töötlejale või volitatud töötlejale, aga mitte andmekaitsespetsialistile. Töökorralduslikult võib osutuda otstarbekaks, et andmekaitsespetsialist haldab isikuandmeid töötlevatelt isikutelt saadud informatsiooni põhjal isikuandmete töötlemise toimingute registrit. Nimetatud ülesande panemist andmekaitsespetsialistile ei välista ka määrus, mis annab andmekaitsespetsialisti ülesannete miinimumloetelu ega välista täiendavate tööülesannete täitmist.

4.3 Andmekaitsespetsialisti kontaktide avaldamine

Määrus kohustab vastutavat ja volitatud töötlejat tegema andmekaitsespetsialisti kontaktandmed avalikuks ja teatama need AKI-le. AKI-t saab andmekaitsespetsialistist teavitada läbi ettevõtjaportaali[23].

Andmekaitsespetsialisti kontaktandmete koosseis peab olema piisav, et isikud ja järelevalveasutus saavad vajadusel andmekaitsespetsialistiga ühendust. Kõige kiirema infovahetuse tagavad telefoninumbri ja e-posti aadressi avaldamine, kuid mõnel juhul võib osutuda vajalikuks ka postiaadressi teatavaks tegemine. Andmekaitsespetsialisti nime avaldamine avalikkusele ei ole kohustuslik, küll tuleb see teatavaks teha AKI-le. Avalikkusele kontaktandmete avaldamiseks on kõige otstarbekam lisada vastavad kontaktandmed haridusasutuse veebilehele, oma töötajate jaoks võib kontakti eraldi välja tuua ka siseveebis, kui see on kasutusel.

Juhul kui andmekaitsespetsialisti ülesandeid täidab allüksus või välise teenusepakkuja meeskond, on oluline, et avalikkusele ja järelevalveasutusele määratakse kontakt.

[23] https://ettevotjaportaal.rik.ee/

5. Isikuandmete kaardistamine ja töötlemise registreerimine

Töödeldavate isikuandmete kaardistamiseks ning andmetöötluse registri sisustamiseks on vaja esmalt isikuandmed üles leida. Selleks on erinevaid viise, millest levinuimad on

- olemasolevate dokumentide analüüs: analüüsitakse asutuses kasutatavaid dokumente – taotluste ja avalduste vorme, andmetöötlust reguleerivaid kordasid ja juhendeid, lepinguid jm.
- kasutuses olevate infosüsteemide analüüs: kirjeldatakse, milliseid infosüsteeme haridusasutuses kasutatakse, kas ja milliseid isikuandmeid neis töödeldakse jne.
- intervjuud ja töötoad: vesteldakse kas eraldi või rühmadena kõikide isikuandmete töötlemisega tegelevate töötajatega, tutvutakse nende tööprotsessiga ja tuvastatakse nende töös kasutatavad andmed, nende hoidmise koht (andmebaas, failiserver, arvuti kõvaketas, pilveteenused jne), töötlemise vahendid ja töömeetodid. Oluline on saada ülevaade ka neist andmetest, mida töödeldakse väljaspool nn ametlikke kohti (koopia failist raamatupidaja sülearvutis, seni kaardistamata rakendus vms).
- küsimustikud: võimaldavad samuti koguda andmeid andmetöötlejatelt.
- vaatlused: andmete ja tööprotsesside kaardistamisel on vahel kasulik vaadelda, kuidas töötaja oma ülesandeid täidab.

Võimaluse isikuandmete töötlemise dokumenteerimiseks ja ülevaate saamiseks annab määruses sätestatud kohustus registreerida kõik isikuandmetega tehtavad töötlustoimingud. Määrus näeb ette mõningad juhud, mil andmetöötlusregistrit pidama ei pea, kuid ühegi haridusasutuse puhul nendele alustele viidata ei ole võimalik, kuna isikuandmete töötlemine ei ole haridusasutustes juhtumipõhine ning töödeldakse ka eriliiki andmeid.

Siinjuures tuleb tähele panna, et eelneva regulatsiooni kohaselt tuli delikaatsete isikuandmete töötlemine registreerida AKI-s, kuid peale määruse jõustumist registreeritakse eriliiki isikuandmete töötlemine üksnes asutuse enda isikuandmete töötlemise registris. Tuleb arvestada, et asutus peab AKI nõudmisel esitama andmetöötlusregistri.

Määrus ei kehtesta konkreetseid nõudeid registri vormile, kuid annab registri sisu kohustuslike osade kirjelduse:

- vastutava töötleja ning kaasvastutava töötleja, vastutava töötleja esindaja ja andmekaitsespetsialisti nimi ja kontaktandmed;
- töötlemise eesmärgid;
- andmesubjektide kategooriate ja isikuandmete liikide kirjeldus;
- vastuvõtjate kategooriad, kellele isikuandmeid on avalikustatud või avalikustatakse, sealhulgas kolmandates riikides olevad vastuvõtjad ja rahvusvahelised organisatsioonid;
- kui isikuandmeid edastatakse kolmandale riigile või rahvusvahelisele organisatsioonile, siis andmed selle kohta koos asjaomase kolmanda riigi või rahvusvahelise organisatsiooni nimega, ning juhul, kui on tegemist juhtumipõhise ja piiratud edastamisega, siis sobivate kaitsemeetmete kohta koostatud dokumendid;
- võimaluse korral eri andmeliikide kustutamiseks ette nähtud tähtajad;
- võimaluse korral määruse artikkel 32 lõikes 1 nimetatud isikuandmete kaitse tehniliste ja korralduslike turvameetmete üldine kirjeldus.

Soovituslik andmeregistri täitmise juhend ning vorm on toodud juhendi „Lisas 1“

Volitatud töötleja peab kõigi vastutava töötleja nimel tehtavate isikuandmete töötlemise toimingute kategooriate registrit, mis sisaldab järgmist teavet:

- volitatud töötleja või töötlejate ja vastutava töötleja, kelle nimel volitatud töötleja tegutseb, ning asjakohasel juhul vastutava töötleja või volitatud töötleja esindaja ja andmekaitseametniku nimi ja kontaktandmed;
- vastutava töötleja nimel tehtava töötlemise kategooriad;
- kui isikuandmeid edastatakse kolmandale riigile või rahvusvahelisele organisatsioonile, siis andmed selle kohta koos asjaomase kolmanda riigi või rahvusvahelise organisatsiooni nimega, ning juhul, kui tegemist on artikli 49 lõike 1 teises lõigus osutatud edastamisega, siis sobivate kaitsemeetmete kohta koostatud dokumendid;
- võimaluse korral artikli 32 lõikes 1 osutatud tehniliste ja korralduslike turvameetmete üldine kirjeldus.

AKI on välja töötanud ja avaldanud oma veebilehel isikuandmete töötlustoimingute registri näidised vastutavale töötlejale ja volitatud töötlejale[24].

6. Mõjuhinnang

Määruse artikkel 35 kehtestab ühe uue nõudena andmetöötlejale kohustuse viia enne isikuandmete töötlemise alustamist läbi andmekaitsealane mõjuhinnang.

Mõjuhinnang on oma olemuselt riskianalüüs, mille käigus andmetöötleja hindab ja analüüsib, millised riskid isikuandmete töötlemisega kaasnevad ning kuidas neid riske maandada. Mõjuhinnang aitab hinnata, kas andmete kaitseks rakendatavad meetmed on piisavad, et isikuandmete töötlemisega andmesubjektile tekkivat võimalikku privaatsusriivet ära hoida või vähendada aktsepteeritavale tasemele.

Määruse kohaselt tuleb mõjuhinnang läbi viia, kui
- isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke arvesse võttes on tõenäoline, et esineb kõrge risk füüsiliste isikute õiguste ja vabaduste riiveks [25];
- andmetöötleja soovib võtta kasutusele uue tehnoloogia, millega kaasneb isikuandmete töötlemine ning millega tal ei ole varem kokkupuudet olnud.

Reeglina tekib mõjuhinnangu tegemise kohustus andmetöötlustoimingutele, millega andmetöötleja alustab pärast määruse jõustumist 25. mail 2018.aastal. Samas laieneb mõjuhinnangu koostamise kohustus ka enne määruse jõustumist alanud andmetöötlustoimingutele, kui sellised isikuandmete töötlemise toimingud ja põhimõtted on alates määruse jõustumisest oluliselt muutunud.

Näiteks võetakse kasutusele uus tarkvara, hakatakse olulise protsessi abistamiseks kasutama pilveteenuseid, hakatakse andmetöötlemiseks kasutama volitatud töötlejat (kooli sööklas asendatakse kooli palgal olevad kokad teenust pakkuva ettevõttega ning neile edastaks sööjate nimed), võetakse kasutusele uus tehnoloogia (uste avamiseks asendatakse kaardilugejad näpujälje lugejatega, aegunud tabeltöötluse asemel kasutakse andmebaasisüsteemi) vm.

Loomulikult võib mõjuhinnangu läbi viia ka muudel juhtudel, kus andmetöötleja peab vajalikuks hinnata mõne andmetöötluse tegevusega seonduvaid riske ning seda, kas need riskid on piisavalt maandatud[26].

Määruse artikkel 35 punkt 7 sätestab mõjuhinnangu miinimumsisu, mille järgi peab mõjuhinnang sisaldama vähemalt:
- kavandatud isikuandmete töötlemise toimingute ja töötlemise eesmärkide süstemaatilist kirjeldust;

[24] http://www.aki.ee/et/tootlustoimingute-registreerimine/tootlemistoimingute-registri-naidised

[25] Vt lisaks AKI veebilehel toodud loetelu mõningatest kõrge riskiga tegevustest, mille puhul tuleb mõjuhinnang kindlasti läbi viia: http://www.aki.ee/et/andmekaitse-reform/mis-andmekaitsealane-mojuhinnang. Loetelus on kõrge riskiga valdkonnana välja toodud muuhulgas ka ulatuslik kaitsetute füüsiliste isikute andmete töötlemine, nagu näiteks lapsed ja vaimse puudega isikud.

[26] Vt lisaks http://www.aki.ee/et/andmekaitse-reform/andmekaitsealase-mojuhinnangu-tegemise-kontrollnimekiri

- hinnangut isikuandmete töötlemise toimingute vajalikkusele ja proportsionaalsusele eesmärkide suhtes;
- andmesubjektide õigusi ja vabadusi puudutavate ohtude hinnangut;
- ohtude käsitlemiseks kavandatud meetmeid, sealhulgas tagatised, turvameetmed ja mehhanismid isikuandmete kaitse tagamiseks ja määruse järgimise tõendamiseks, võttes arvesse andmesubjektide ja teiste asjaomaste isikute õigusi.

Andmekaitsealane mõjuhinnang tuleb vormistada kirjalikult.

Kui andmetöötleja hinnangul rakendatavad meetmed kõrget riski piisavalt ei maanda, on ta kohustatud enne andmetöötlusega alustamist konsulteerima AKI-ga.

Isikuandmete töötlemise mõjude hindamine ei peaks olema ühekordne toiming. Andmete töötleja huvides on pidevalt jälgida töötlemise vastavust määruse nõuetele.

Mõjuhinnangu teemat käsitleb lähemalt Euroopa andmekaitseasutuste töörühma juhend "Suunised, mis käsitlevad andmekaitsealast mõjuhinnangut ja selle kindlaksmääramist"[27].

7. Meetmed andmete kaitseks

Määruse artikkel 32 ütleb, et andmete vastutav ja volitatud töötleja on kohustatud rakendama andmetele vastava turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslike meetmeid. Turvameetmete eesmärgi on hoida ära töödeldavate isikuandmete aluseta hävitamine ja muutmine, kaotamine ning loata avalikustamine või volitamata isikutele juurdepääsu võimaldamine. Määrus toob võimalike meetmetena näiteks isikuandmete pseudonümiseerimise ja krüpteerimise, tehniliste ja korralduslike meetmete rakendamise, testimise ja hindamise ning vastavate kordade kehtestamise. Üksikud tehnilised meetmed ei taga tegelikult piisavat turvalisust. Selleks et seada asutuses sisse üldine turvalisuse mõtteviis, on vaja turvalisusega tegeleda süsteemselt.

Mõned näited võimalikest andmelekete olukordadest, mida saab üldise teadlikkuse suurendamise ja asutusesiseste käitumisreeglite kehtestamise ja järgimisega ära hoida: varastatakse töötaja sülearvuti, mille lokaalsel kettal hoiab töötaja krüpteerimata kujul isikuandmeid ning arvutile ei ole pandud sisenemiseks parooli; töötaja hoiab oma õpihalduskeskkonna paroole märkmepaberil arvuti juures või ei logi tööd lõpetades kontolt välja; õpilastel on võimalus kooli sisevõrku ühendatud arvutites kasutada kontrollimata väliseid seadmeid; õpetaja töötleb õpilaste isikuandmeid oma isiklikku meilikontot kasutades.

Selliste olukordade vältimiseks on esmajoones oluline kehtestada asjakohased juhendid kooli arvutivõrgu kasutamiseks *(näiteks arvutivõrgu kasutamise kord, andmete turvalise edastamise reeglid, sülearvutite kasutamise kord, kaugtöö (kodutöö) tegemise kord, reeglid selle kohta, milliseid andmeid ja milliselt meilikontolt tohib edastada, andmete turvalise kustutamise ja hävitamise reeglid jm)* ning kõiki kooli arvutivõrgu kasutajaid (õpetajad, õpilased, muud isikud) küberhügieeni teemal regulaarselt koolitada.

Soovitused jätkusuutliku turvakultuuri ja harjumuste juurutamiseks on toodud juhendi „Lisas 2".

8. Rikkumistest teavitamine

Isikuandmetega seotud rikkumised on olukorrad, kus töötleja vastutusel olevate isikuandmete osas leiab aset turvanõuete rikkumine, mille tulemusel satub ohtu andmete konfidentsiaalsus, terviklikkus või andmed võivad saada kättesaadavaks õigustamata isikutele.

[27] http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/wp248_rev.01_et.pdf

Näiteks on rikkumine olukord, kus haridusasutuse töötaja salvestab oma sülearvuti kõvakettale krüpteerimata kujul faile õpilaste nimede, vanuste, koduste aadresside jms isikuandmetega. Tema sülearvuti ei ole varustatud parooliga ning see varastatakse töötaja autost, mille tulemusel võivad saada laste isikuandmed kättesaadavaks selleks õigustamata isikutele.

Kui esineb isikuandmetega seotud rikkumine, on vastutaval töötlejal kohustus esimesel võimalusel, kuid hiljemalt 72 tunni jooksul alates rikkumisest teada saamisest teavitada rikkumisest AKI-t, v.a kui rikkumine ei kujuta endast ohtu isiku, kelle isikuandmetega oli rikkumine seotud, õigustele ja vabadustele. Kui on tõenäoline, et rikkumine kujutab endast suurt ohtu andmesubjektide õigustele ja vabadustele, peab vastutav töötleja andmesubjekte põhjendamatu viivituseta teavitama. Andmesubjektide teavitamise kohustus langeb ära, kui iga isiku eraldi teavitamine toob kaasa ebaproportsionaalse jõupingutuse, sellisel juhul võib teha avaliku teavituse. Samuti ei ole vaja teavitada, kui võetakse kasutusele meetmed, mille tulemusel oht andmesubjekti õigustele ja vabadustele ei ole enam tõenäoline või kui asjakohaste kaitsemeetmete rakendamine, näiteks andmete hoidmine krüpteeritult, hoiab ära ohu andmesubjekti õigustele ja vabadustele.[28]

Isikuandmete töötlemisega puutuvad haridusasutuses kokku erinevad töötajad, mistõttu tuleks kehtestada reeglid, kuidas asutuse sees isikuandmetega seotud rikkumiste osas informatsioon peab liikuma. Asjakohased protseduurid saab kehtestada intsidentide haldusega, mis võib olla iseseisev dokument või ka näiteks osa poliitikast.

Kuna isikuandmetega seotud rikkumisest teavitamise kohustus lasub vastutaval töötlejal, siis on oluline, et volitatud töötleja kaasamisel lepitakse lepingus kokku, kuidas volitatud töötleja teavitab vastutavat töötlejat isikuandmetega seotud rikkumistest.

9. Volitatud töötleja kaasamine isikuandmete töötlemisse

Haridusasutus on vastutava töötlejana vastutav kõigi kogutud isikuandmete turvalisuse ja nõuetekohase töötlemise eest. See vastutus laieneb ka andmetele, mida haridusasutus jagab volitatud isikutega, kui nood teevad vastutava töötleja nimel mingit tööd isikuandmetega.

Volitatud töötlejateks on teiste seas erinevad teenusepakkujad, näiteks
- *õpihaldustarkvara pakkuv ettevõte,*
- *andmete majutust pakkuv ettevõte,*
- *videovalvet korraldav ettevõte,*
- *IT-haldusega tegelev ettevõte,*
- *tundlike andmete hävitamisega tegelev ettevõte,*
- *toitlustusteenust pakkuv ettevõte jne.*

Need teenusepakkujad on määruse mõistes volitatud töötlejad, kes töötlevad isikuandmeid vastutava töötleja suuniste ja tingimuste järgi. Tingimused sätestatakse vastutava ja volitatud töötleja vahelises lepingus. Vastutaval töötlejal on määrusest tulenev kohustus valida selline volitatud töötleja, kes suudab anda tagatise, et rakendab piisavaid meetmeid andmete kaitseks. Volitatud töötleja kaasamise täpsemad reeglid on toodud määruse artiklis 28.

Volitatud töötlejate tegevuse edukaks haldamiseks määruse vaates on kaks üldist nõuet:
- vastutav töötleja peab omama pidevat ülevaadet nende volitatud töötlejate kohta, kellega isikuandmeid jagatakse, samuti selle kohta, milliseid andmeid kellega jagatud on;
- volitatud töötlejate sobivust tuleb hinnata ning temaga tuleb sõlmida leping.

[28] Vt lisaks AKI koostatud ülevaadet rikkumisteadete regulatsiooni kohta http://www.aki.ee/et/andmekaitse-reform/rikkumisteated

Tuleb meeles pidada, et ükski leping ei võta vastutavalt töötlejalt vastutust määruse nõuete täitmise eest. Kui volitatud töötleja rikub määruses toodud nõudeid ja selle tulemusel on isikuandmed näiteks kahjustunud, on AKI ja andmesubjektide eest vastutav eelkõige vastutav töötleja.

Seega on mõistlik volitatud töötlejaid hoolikalt valida, nendega sõlmitavates lepingutes andmekaitset puudutavaid teemasid käsitleda ning esitatud nõuete täitmist ka kontrollida.

9.1 Volitatud töötleja valimine ja lepingu sõlmimine

Vastavalt määruse artiklile 28 võib vastutav töötleja kaasata ainult selliseid volitatud töötlejaid, kes annavad piisava tagatise, et rakendavad vajalikke tehnilisi ja korralduslikke meetmeid, eesmärgiga tagada isikuandmete töötlemise vastavus **määruse nõuetele** ja andmesubjekti õiguste kaitse. Seega tuleb väga hoolikalt suhtuda koostööpartneri valimisse ning lisaks hinnale vaadata ka, milline on partneri andmekaitsealane pädevus.

Esmajoones tähendab see küsimuste esitamist ning partneri teadlikkuse kontrollimist.

Mõnes valdkonnas on võimalik küsida potentsiaalselt partnerilt asjakohase sertifikaadi olemasolu või tõendust, et partner on läbinud valdkonna **auditeid või teste**.

Sellisteks sertifikaatideks on näiteks: ISO27001 (infoturve), ISKE (infoturve), OWASP ASVS (veebirakenduste turvalisus).

Partneri sobivuse hindamiseks võib kasutada ka erinevaid küsimustikke ja kontroll-loendeid, kuid sellisel juhul tuleb saadud informatsiooni õigsuses veenduda.

Suuremate infoühiskonna teenuste pakkujate (***nt*** *Google, Microsoft jt*) puhul ei ole reeglina võimalik oma lepingutingimusi esitada, mistõttu on oluline lugeda läbi nende teenuste kasutustingimused ning süveneda sellesse, kuidas tagatakse andmete turvalisus. Samuti tuleks tähelepanu pöörata sellele, millises riigis teenusepakkujad neile kättesaadavaks tehtud isikuandmeid reaalselt hoiavad. Ka Euroopa Liidu välistes riikides andmete töötlemisel on oluline määruse nõuete järgimine. Kui vastutaval töötlejal on kahtlusi volitatud töötleja määruse nõuete täitmise suutlikkuse osas, siis ei tohiks teda volitada isikuandmeid töötlema.

Lepingu sõlmimisel volitatud töötlejaga peab silmas pidama, et

- volitatud töötleja ei tohi kaasata teist volitatud töötlejat ilma vastutava töötleja eelneva kirjaliku loata. See luba võib olla konkreetne või üldine. Üldise loa korral peab volitatud töötleja teavitama vastutavat töötlejat kõigist kavandatavatest muudatustest, mis puudutavad teiste volitatud töötlejate lisamist või asendamist. Vastutaval töötlejal on seejärel võimalik esitada vastuväiteid. Teise volitatud töötleja kaasamisel peab volitatud töötleja omakorda jälgima, et kaasatav täidab samuti kõiki andmekaitsenõudeid.
- Volitatud töötlejaga tuleb sõlmida kirjalik leping (välja arvatud juhul, kui volitatud töötleja kaasamine toimub õigusakti alusel). Leping peab sisaldama infot töötlemise sisu ja kestuse, töötlemise laadi ja eesmärgi, isikuandmete liigi ja andmesubjektide kategooriate, vastutava töötleja õiguste ja kohustuste kohta.
- Lepingus tuleb sätestada, et volitatud töötleja
    - töötleb isikuandmeid ainult vastutava töötleja dokumenteeritud juhiste alusel;
    - tagab, et isikuandmeid töötlevad isikud on kohustatud järgima konfidentsiaalsusnõuet;
    - rakendab vajalikke turvameetmeid (määruse artikkel 32);
    - järgib teiste volitatud töötlejate kaasamiseks kehtestatud tingimusi;
    - aitab võimaluse piires vastutaval töötlejal vastata taotlustele (vt isiku õigusi);
    - aitab vastutavalt töötlejal täita kohustust rikkumistest teavitada;
    - kustutab pärast teenuse osutamise lõppu kõik isikuandmed ja nende koopiad (v.a juhul, kui seadus nõuab andmete säilitamist);

- tõendab kõigi nende kohustuste täitmist ning võimaldab vastutaval töötlejal teha auditeid ja kontrolle.

10. Kuidas alustada?

Nagu teisedki andmetöötlejad, peab haridusasutuste isikuandmete töötlemise korraldus vastama määruse nõuetele 25. maiks 2018.

Selleks et tagada haridusasutuse tegevuse vastavus määrusele, on soovitav teha järgmised tegevused:

1. Andmekaitsespetsialisti määramine (vt juhendi punkt 4)

Määra ametisse andmekaitsespetsialist või sõlmi leping teenusepakkujaga. Sellega saad endale abiks andmekaitseeksperdi, kes tunneb õigusakte ja nende nõudeid ning oskab nõustada ja kontrollida isikuandmete töötlemise vastavust määruse nõuetele.

Kontrollküsimused:
- Kas andmekaitsespetsialist on määratud?
- Kas on olemas andmekaitsespetsialisti tööks vajalikud ressursid?
- Kas andmekaitsespetsialist saab teha oma tööd sõltumatult?
- Kas andmekaitsespetsialisti kontaktandmed on kättesaadavad nii organisatsiooni sees kui ka organisatsioonivälistele isikutele?

2. Andmete kaardistamine (vt juhendi punkt 5)

Kaardista isikuandmed organisatsioonis ning koosta töötlemistoimingute register. Andmete nõuetekohase töötlemise eelduseks on teadmine, milliseid andmeid, kus ja kuidas organisatsioonis töödeldakse.

Kontrollküsimused:
- Kas tead, milliseid isikuandmeid organisatsioon töötleb?
- Kas kõigi andmete töötlemiseks on olemas õiguslik alus?
- Kas kõigi andmete kohta on teada nende päritolu ning koht, kus neid hoitakse?
- Kas kõigil andmetel on määratud töötlemise tähtaeg?
- Kas kõigi andmete kohta on teada, kes neile ligi pääsevad?
- Kas ja kellele andmeid edastatakse?

3. Gap-analüüs

Hinda, kas viis, kuidas isikuandmeid organisatsioonis töödeldakse, vastab määruse nõuetele. Sobiv viis selleks on viia läbi *gap*-analüüs (puudujääkide analüüs), mille käigus võrreldakse tegelikku olukorda esitatud nõuetega ning selgitatakse välja puudused. Pööra sealjuures tähelepanu nii dokumentatsioonile (protseduurid, korrad, otsused jms) kui tööprotsessidele ehk sellele, kuidas asju tegelikult tehakse. Samuti ära unusta isikuandmete kaitseks rakendatavaid organisatsioonilisi ja tehnilisi meetmeid.

Kontrollküsimused:
- Kas nõuete kogum on piisav, et saada täielik ülevaade nõuete täitmisest?
- Kas oled hinnanud nii formaalset töökorraldust ehk dokumentatsiooni kui ka seda, kuidas asju tegelikult tehakse?
- Millised sammud tuleb teha puuduste kõrvaldamiseks?
- Millised on iga konkreetse puuduse kõrvaldamise tähtajad ja kes on vastutajad?

4. Dokumentide ja tööprotsesside koostamine ja ajakohastamine

Vajalike dokumentide hulga ning sisu määravad ära töödeldavad andmed, organisatsiooni töökorraldus, struktuur ja põhiprotsessid, kasutatav tehnoloogia, andmevahetuse vajadus partnerite ja volitatud

töötlejatega jne. Tõenäoliselt kuuluvad vajalike dokumentide hulka privaatsuspoliitika, isikuandmete kaitse juhised töötajatele, infoturvet reguleerivad dokumendid, lepingud volitatud töötlejatega jne. Tööprotsesside osas on oluline tagada, et oleks tagatud andmete töötlemine vaid korrektsel õiguslikul alusel (sh nõusoleku võtmine), andmesubjekti päringutele ja taotlustele vastamine ning rikkumistest teavitamine.

Kontrollküsimused:
- Kas kõigi andmete töötlemiseks on olemas õiguslik alus?
- Kas on määratud ja koostatud piisav ning tarvilik dokumentatsioon, millega tagada vajalike andmekaitse meetmete loomine, rakendamine ning sisemine igapäevane kontroll kõigil juhtimistasanditel?
- Kas töötajad teavad, kuidas töödelda isikuandmeid?
- Kas töötajad teavad, kuidas rikkumisi ära tunda ning menetleda?
- Kas on olemas protsess andmesubjekti taotluste täitmiseks?

5. Andmesubjekti õiguste tagamine (vt juhendi punkt 3)

Vaata üle andmetöötlusprotsessid, selleks kasutatavad vahendid, töökorrad ja volitatud töötlejatega sõlmitud lepingud, ning tee kindlaks, et oled valmis vastama andmesubjektide päringutele ning taotlustele.

Kontrollküsimused:
- Kas on tagatud piisav teave andmesubjektile?
- Kas suudetakse anda andmesubjektile infot selle kohta, milliseid isikuandmeid tema kohta töödeldakse?
- Kas andmete õigsuse tagamise protseduur on olemas?
- Kas isikuandmete kustutamine on vajadusel võimalik?
- Kas isikuandmete ülekandmine on võimalik (eeldusel, et töödeldakse on andmeid, mille osas sellist nõuet saab esitada)?

6. Andmekaitse ajakohastamine

Mõtle läbi ning rakenda süsteemselt andmete kaitsmiseks vajalikud turbemeetmed.

Kontrollküsimused:
- Kas on määratud andmekaitse kõigi tasemete eest vastutajad – juhtkonnas, IT-juhtimine ja -haldus, IT-turvalisus, isikuandmete andmebaaside omanikud jne?
- Kas andmekaitse kordasid ja rakendatud meetmeid vaadatakse regulaarselt üle ning tehakse täiendusi, muudatusi?
- Kas juhtkonnale tehakse regulaarselt aruandeid ning need on juhtkonnas aruteluks?
- Kas töötajad tunnevad kehtivaid kordasid ning omavad piisavat infot andmekaitsest?

7. Mõjuhinnang (vt juhendi punkt 6)

Vajadusel vii läbi mõjuhinnang. Mõjuhinnang on oma olemuselt riskianalüüs, mille käigus andmetöötleja hindab ja analüüsib, millised riskid isikuandmete töötlemisega kaasnevad ning kuidas neid riske maandada. Mõjuhinnang aitab hinnata, kas andmete kaitseks rakendatavad meetmed on piisavad, et hoida ära või vähendada aktsepteeritavale tasemele isikuandmete töötlemisega tekkivat võimalikku privaatsusriivet.

Kontrollküsimused:
- Kas kõik isikuandmete töötlemise tööprotsessid on kirjeldatud ja neis kasutatavad isikuandmed kaardistatud?
- Kas on isikuandmete töötlemises toiminguid või kasutusel tehnilisi lahendusi, mis võiksid põhjustada isikutele suurt ohtu läbi andmetega toimuvate intsidentide?
- Kas kõik riskianalüüsis tuvastatud riskid on maandatud?
- Kas kõigile määruses nõutud kriteeriumid on mõjuhinnangus kirjeldatud?

8. Rikkumiste teavitamine (vt juhendi punkt 8)

Loo rikkumistest teavitamise kord ning õpeta kõik asjassepuutuvad inimesed rikkumisi ära tundma ning neist teavitama.

Kontrollküsimused:

- Kas on olemas rikkumistest teavitamise kord ja protsess?
- Kas kõik asjasse puutuvad isikud oskavad rikkumisi ära tunda?
- Kas on olemas tehnilised abivahendid rikkumiste äratundmiseks?
- Kas kõik asjasse puutuvad isikud on korrast teadlikud ning teavad, mida teha?

9. Teadlikkus

Isikuandmete kaitse tagamiseks on hädavajalik, et kõik – juhtkond, töötajad, õpilased – teavad, miks ja kuidas isikuandmetega ringi käia. Koolita nii juhtkonda, õpetajaid, muid töötajaid kui õpilasi isikuandmete kaitse põhimõtete ning küberturvalisuse teemal.

Kontrollküsimused:

- Kas kõik erinevad sihtrühmad on koolitatud?
- Kas koolitusi (ja võimaluse korral teste) korratakse regulaarselt?

Lisa 1 Andmeregistri täitmise juhend

1. Üldsätted

1.1. Käesolev andmeregistri täitmise juhend (edaspidi nimetatud kui „**juhend**“) on abistavaks materjaliks haridusasutustele isikuandmete kaardistuse läbiviimisel ning isikuandmete kaitse üldmääruses sätestatud kohustusliku andmeregistri[29] koostamisel. Käesoleva dokumendi eesmärgiks on avada registris toodud valdkondi ja mõisteid ning anda ülevaade isikuandmete töötlemise üldistest põhimõtetest, õigustest ja kohustustest isikuandmete töötlemisel, sealhulgas isikuandmete kaitseks rakendatavatest turvameetmetest.

1.2. Käesolev juhend järgib andmeregistris toodud valdkondi ning avab täiendavalt konkreetse valdkonna sisu. Andmeregister järgib põhikooli- ja gümnaasiumiseaduses toodud isikuandmete töötlemise protseduure ning andmeregistri täitja sisestab valdkonniti isikuandmete töötlemist puudutavad aspektid, protseduurid ning meetmed.

1.3. Samuti sätestab käesolev juhend isikuandmete töötlemise üldised põhimõtted, õigused ja kohustused isikuandmete töötlemisel, sealhulgas isikuandmete kaitseks rakendatavad turvameetmed.

1.4. Käesolevas juhendis kasutatakse lühendeid järgmises tähenduses:

1.4.1. PGS – põhikooli- ja gümnaasiumiseadus[30];

1.4.2. IKÜ – EL isikuandmete kaitse üldmäärus 2016/679;

1.4.3. IKS – isikuandmete kaitse seadus[31];

1.4.4. EHIS – Eesti Hariduse Infosüsteemi andmekogu[32];

1.4.5. AKI – Andmekaitseinspektsioon.

2. Isikuandmete töötlemine

2.1. Käesolevas juhendis ja andmeregistris kasutatakse mõisteid järgmises tähenduses:

[29] Üldmääruse artiklis 30 sätestatud isikuandmete töötlemise toimingute registreerimine

[30] Põhikooli- ja gümnaasiumiseadus (RT I 2010, 41, 240) - https://www.riigiteataja.ee/akt/13332410?leiaKehtiv

[31] Isikuandmete kaitse seadus (RT I 2007, 24, 127) - https://www.riigiteataja.ee/akt/106012016010?leiaKehtiv

[32] Eesti Hariduse Infosüsteemi asutamine ning põhimäärus (RT I 2004, 61, 434) - https://www.riigiteataja.ee/akt/12863550?leiaKehtiv

2.1.1. Isikuandmed – tähendab igasugust teavet tuvastatud või tuvastatava füüsilise isiku („andmesubjekti“) kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal;

2.1.2. Isikuandmete töötlemine – on isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine;

2.1.3. Andmete kogum (andmekogu) – isikuandmete igasugune korrastatud kogum, millest võib andmeid tuvastada kriteeriumide põhjal, olenemata sellest, kas kõnealune andmete kogum on funktsionaalsel või geograafilisel põhimõttel tsentraliseeritud, detsentraliseeritud või hajutatud (näiteks e-kooli teenusepakkuja, kooli raamatukogu lugejakaartide andmebaas, isikuandmeid sisaldav õppeinfosüsteem jms);

2.1.4. Vastutav töötleja – füüsiline või juriidiline isik, avaliku sektori või KOV asutus (näiteks haridusasutus), kes on esmaseks isikuandmete kogujaks. Vastutav töötleja määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid;

2.1.5. Volitatud töötleja – füüsiline või juriidiline isik, avaliku sektori või KOV asutus, kes töötleb isikuandmeid vastutava töötleja ülesandel ja tema juhendi alusel;

2.1.6. Kolmas isik – füüsiline või juriidiline isik, avaliku sektori või KOV asutus, amet või organ (näiteks SA Innove, toitlustusteenuse osutaja jms), kes töötlevad isikuandmeid ühekordse päringu alusel.

2.1.7. Isikuandmetega seotud rikkumine – nõuete rikkumine, mis põhjustab edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu;

2.1.8. Terviseandmed – füüsilise isiku füüsilise ja vaimse tervisega seotud isikuandmed, sealhulgas temale tervishoiuteenuste osutamist käsitlevad andmed, mis annavad teavet tema tervisliku seisundi kohta;

2.1.9. Andmesubjekt – isik, kelle isikuandmeid töödeldakse (näiteks õpilane, lapsevanem, eestkostja, haridustöötaja jms);

2.1.10. Isikuandmete kaitse üldmäärus – Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. Aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta;

2.2. Isikuandmete töötlemisel peab tagama, et järgitakse järgnevaid põhimõtteid:

2.2.1. Seaduslikkuse, õigluse ja läbipaistvuse põhimõte – töötlemine on seaduslik, õiglane ja andmesubjektile läbipaistev;

2.2.2. Eesmärgi piirangu põhimõte – isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus;

2.2.3. Võimalikult väheste andmete kogumise põhimõte – isikuandmed on asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt;

2.2.4. Õigsuse põhimõte – isikuandmed on õiged ja vajaduse korral ajakohastatud ning et võetakse kõik mõistlikud meetmed, et töötlemise eesmärgi seisukohast ebaõiged isikuandmed kustutaks või parandataks viivitamata;

2.2.5. Säilitamise piirangu põhimõte – isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse;

2.2.6. Usaldusväärsuse ja konfidentsiaalsuse põhimõte – isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid.

3. Infotehnoloogilised turvameetmed

3.1. Andmete turvalisust hinnates tuleb kaaluda isikuandmete töötlemisest tulenevaid ohte, nagu edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhuslik või ebaseaduslik hävitamine, kaotsiminek, muutmine ja loata avalikustamine või neile juurdepääs, mille tagajärjel võib eelkõige tekkida füüsiline, materiaalne või mittemateriaalne kahju.

3.2. Andmeregistris kasutatakse infotehnoloogiliste turvameetmetega seonduvaid mõisteid järgmises tähenduses:

3.2.1. Pääsuhaldus – volitatud kasutaja poolt lubatud tegevuste reguleerimine, vahendades iga subjekti katset pöörduda süsteemis asuva ressursi poole. Koolides tuleb juurutada formaalne kasutajate registreerimise ja väljaregistreerimise protsess pääsuõiguste määramiseks. Juurdepääsu teabele ja rakendussüsteemide funktsioonidele tuleks kitsendada vastavalt teabevajadusele. Juurdepääsu õigused peavad olema koolides kaardistatud ning juurdepääsuõiguste andmine ja kasutamise (logid) peab olema kontrollitav ja lähtuma teadmisvajadusest ja ametikohast.

3.2.2. Tulemüür – kas tarkvararakendus või spetsiaalne seade, mille põhiülesandeks on reguleerida liiklust erineva turvatasemega arvutivõrkude vahel, eraldades näiteks väiksema kodu- või kontorivõrgu ülejäänud Internetist. Tulemüüri ülesanne on teatada süsteemi haldajat, kui süsteemile on toimunud tahtmatuid ligipääsu katseid. Tuleb rakendada turvameetmeid, mis tagavad teabe turvalisuse võrkudes ning võrgustatud teenuste kaitse volitamata juurdepääsu eest.

3.2.3. Autentimine – kasutaja isiku tõendamine infosüsteemi sisenemisel. Selleks võib kasutada parooli, kiipkaarti või biomeetrilisi võimalusi.

3.2.4. Viirusetõrje – viiruste avastamiseks ja võimalike parandusmeetmete soovitamiseks või rakendamiseks määratud programm. Viirusetõrje kontrollib arvutis käimasolevaid protsesse ning mälus ja kõvakettal või välisel andmekandjal olevaid ja veebist allatõmmatavaid või elektronkirjadega saabuvaid faile, võrreldes neid varem teadaoleva pahavara koodinäidistega. Kui mõni osa kontrollitavast koodist sarnaneb viirusedefinitsioonis oleva näidisega, püüab viirusetõrje nakatunud osa eemaldada ja kui see aga ei õnnestu, paigutatakse nakatunud fail karantiini või kustutatakse.

3.2.5. Võrgu turvalisuse meetmed – võrgu kaudu süsteemi sisenedes VPN-i kasutamine, ligipääsude piiramine ja korrapärane haldamine, turvaliste paroolide kasutamine. Parooli pikkus peab olema vähemalt 8 tähemärki; Parool peab sisaldama suuri ja väikeseid tähti ning numbreid; paroolis ei ole soovitatav kasutada järgmisi tähti: Õ, õ, Ä, ä, Ö, ö, Ü, ü.

3.2.6. Infoturbepoliitika – eesmärk on infovarade kaitse ning nende käideldavuse, tervikluse ja konfidentsiaalsuse tagamine nõutaval tasemel. Tuleb määratleda komplekt infoturbepoliitikaid, saada neile juhtkonna kinnitus, avaldada need ja teha teatavaks töötajatele ja asjassepuutuvatele välistele pooltele. Infoturbepoliitikas tuleks määratleda: pääsukontrolli, informatsiooni turvaliigituse, füüsilise ja keskkonna turve, varundus, infoedastus, kaitse kahjuvara eest, tehniliste nõrkuste haldus, krüptograafilised turvameetmed, sideturve, privaatsus ja isikuandmete kaitse, suhted tarnijatega.

3.2.7. VPN – kasutades VPNi loob arvuti turvalise, krüpteeritud ühenduse VPNi teenuse pakkujaga, peale mida liigub kõik liiklus läbi nende turvalise serveri. Liiklust pole kolmandatel osapooltel võimalik jälgida olenemata asukohast.

4. Isikuandmete kogumise valdkond ja eesmärk

4.1. Veerg **„Valdkond“** – isikuandmete töötlemise valdkond. Registris tuleb kajastada kõiki valdkondi/protsesse, milles isikuandmeid koolis töödeldakse. Registri vormil toodud valdkondi tuleks koolil vastavalt tegelikule töötlemise valdkondadele täiendada.

4.2. Veerg **„Andmetöötluse eesmär**k“ – milleks isikuandmeid kogutakse (näiteks haridusteenuse osutamiseks või tervishoiuteenuse osutamiseks koolis). Eesmärk peab olema konkreetselt sõnastatud ja õiguspärane (st eesmärk peab tulenema isikuandmete kogumise õiguslikust alusest).

4.3. Isikuandmed tuleb koguda täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning isikuandmeid ei tohi töödelda hiljem viisidel, mis on nende eesmärkidega vastuolus. Kui ühe valdkonna all esineb isikuandmete töötlemist erinevatel eesmärkidel, tuleb töötlemine registris kajastada kõigi eesmärkide lõikes eraldi ridadel (nt õpetaja isikuandmete töötlemisel tema laste andmete töötlemine jõulude ajal kommipaki kinkimiseks ei tulene töölepingu seaduse alusest, vaid töötaja vabatahtlikul nõusolekul. Töölepingu seaduse alusel töödeldakse andmeid, mida on vaja töölepingu sõlmimiseks seaduse kohaselt).

4.4. Õiglase ja läbipaistva isikuandmete töötlemise seisukohast on oluline, et koolis eksisteeriks selge arusaam isikuandmete töötlemise toimingute tegemisest ja selle eesmärkidest, mistõttu on oluline registri koostamisel tagada kooli kõigi valdkondade/protsesside kaasatus, kus isikuandmeid töödeldakse.

5. Andmesubjekti kategooria

5.1. Veerg **„Andmesubjekti kategooria“** – kelle isikuandmeid konkreetse protsessi käigus (näiteks kooli vastuvõtmise protsessis) töödeldakse (näiteks õpilane, lapsevanem, eestkostja).

5.2. Andmeregistrit täites on oluline, et isikuandmete töötlejal oleks selge arusaam andmesubjektidest ja nende kategooriatest, eesmärgiga tagada, et isikuandmete töötlemine toimub õiguspärasel ja määruse põhimõtetest lähtuval viisil.

6. Andmete koosseis/liik

6.1. Veerg **„Andmete koosseis/liik“** – koolil tuleb märkida töödeldavate isikuandmete kõikehõlmav koosseis ehk milliseid konkreetseid isikuandmete liike töödeldakse. Võimalikeks liikideks on näiteks: nimed, sünniajad, isikukoodid, aadressid, telefoni numbrid, meiliaadressid, *online* identifitseerija (e-mail, kasutajanimi, IP aadress, seadme ID), pseudonüümi andmed, palgaandmed, terviseandmed, geneetilised andmed, biomeetrilised andmed (näpujälg, näotuvastus), distsiplinaarmärkused, eksami/testide tulemused, muud sõnalised hindamised nt arenguvestluse protokollid.

6.2. Märkida tuleks kõik kogutavad isikuandmed vastava protsessi juures konkreetsel real kajastatud eesmärgi täitmiseks (näiteks kooli vastuvõtmise korral isikukood, nimi, rahvastikuregistrisse kantud elukoha aadress, isikut tõendav dokument jms).

7. Andmete kogumise allikas/tegevus

7.1. Veerg **„Millisest allikast andmeid kogutakse/tegevuse nimetus“** – andmeregistri täitjal tuleb sisestada isikuandmete kogumise allikas või kirjeldada ülevaatlikult isikuandmete kogumiseks tehtavat tegevust.

7.2. Andmete kogumise allika all peetakse silmas viisi, kuidas andmed tekivad või neid kogutakse (näiteks avaldus paberil, elektroonilistest infosüsteemidest saadavad andmed, psühhiaatrilt koolile edastatud tõend jms).

8. Vastutav või volitatud töötleja

8.1. Veerg **„Kool vastutava või volitatud töötlejana“** – andmeregistri täitjal tuleb sisestada roll, milles haridusasutus isikuandmeid töötleb (kas volitatud või vastutav töötleja).

8.2. Vastutav töötleja on haridusasutus juhul, kui ta on esmaseks isikuandmete kogujaks (st kogub isikuandmeid otse algallikast, andmesubjektilt). Volitatud töötleja on haridusasutus juhul kui ta töötleb isikuandmeid vastutava töötleja ülesandel ja tema juhiste alusel. Vastutava töötleja ülesandeks on ka tagada volitatud töötleja poolt isikuandmete töötlemise vastavus nõuetega. Vastutav töötleja peab isikuandmeid töötlema volitatud töötleja juhistest lähtudes.

8.3. Veerg **„Volitatud töötlemise korral lepingu olemasolu“** – juhul kui haridusasutuse näol on tegemist volitatud töötlejaga, peab olema sõlmitud vastutava töötlejaga kas kirjalik leping või isikuandmete töötlemise tingimused peavad olema sätestatud muus dokumendis (näiteks kasutustingimused),

mis sätestavad haridusasutuse õigused, kohustused ja vastutuse. Veergu tuleb märkida, kas kirjalik leping/töötlemise tingimused on kirjalikult sätestatud või mitte.

9. Andmete töötlemise koht

9.1. Veerg **„Isikuandmete töötlemise koht“** – andmeregistri täitjal tuleb sisestada kõik (elektroonilised ja paberkandjal isikuandmete töötlemise) kohad, kus töödeldakse isikuandmeid (näiteks EIS, EHIS, elektroonilised võrgukettad, mälupulgad, välised kõvakettad, paberkandjad jms).

9.2. Elektrooniliste infosüsteemide korral tuleks registrisse märkida infosüsteemi nimetus ning iga infosüsteem eraldi real, kuna infosüsteemide turvalisuse tasemed, süsteemi kasutuse alused ja töötlejad on erinevad ka olukorras, kus eesmärk võib olla sama.

9.3. Isikuandmete töötlejal on kohustus tagada, et isikuandmeid töödeldakse turvalisel viisil (sh turvalises kohas), mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid.

10. Töötlemise õiguslik alus

10.1. Veerg **„Töötlemise õiguslik alus“** – andmeregistri täitjal tuleb sisestada konkreetse protsessi raames kogutavate isikuandmete töötlemise õiguslik alus (näiteks PGS-st tuleneva juriidilise kohustuse täitmiseks, töötervishoiu ja tööohutuse seadusest tulenev tööandja kohustus).

10.2. Isikuandmete töötlemine on seaduslik ainult juhul, kui täidetud on vähemalt üks järgmistest tingimustest, ning sellisel määral, nagu see tingimus on täidetud:

10.2.1. andmesubjekt on andnud nõusoleku töödelda oma isikuandmeid ühel või mitmel konkreetsel eesmärgil;

10.2.2. isikuandmete töötlemine on vajalik andmesubjekti osalusel sõlmitud lepingu täitmiseks või lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele;

10.2.3. isikuandmete töötlemine on vajalik vastutava töötleja juriidilise kohustuse täitmiseks;

10.2.4. isikuandmete töötlemine on vajalik andmesubjekti või mõne muu füüsilise isiku eluliste huvide kaitsmiseks;

10.2.5. isikuandmete töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks;

10.2.6. isikuandmete töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral, välja arvatud juhul, kui sellise huvi kaaluvad üles andmesubjekti huvid või põhiõigused ja -vabadused, mille nimel tuleb kaitsta isikuandmeid, eriti juhul kui andmesubjekt on laps.

11. Andmete säilitamise periood

11.1. Veerg **„Isikuandmete säilitamise periood“** – konkreetsete isikuandmete säilitamise tähtaeg. Isikuandmeid tohib säilitada ainult minimaalse aja, sõltuvalt isikuandmete töötlemise eesmärgist. Säilitamise tähtajad võivad tuleneda seadusest, määrusest, kooli siseregulatsioonist vm õiguslikust alusest.

11.2. Selle tagamiseks, et isikuandmeid ei säilitataks vajalikust kauem, peaks vastutav töötleja kindlaks määrama tähtajad andmete kustutamiseks või perioodiliseks läbivaatamiseks. Vastutav töötleja ei tohiks isikuandmeid säilitada üksnes selleks, et suuta reageerida võimalikele päringutele.

12. Turvameetmete kirjeldus

12.1. Isikuandmeid tuleb töödelda viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid.

12.2. Andmeregistri täitjal tuleb sisestada meetmed, mis on koolis rakendatud konkreetse protsessi/eesmärgi raames kasutatavate isikuandmete turvalisuse tagamiseks, kuna vastutav töötleja ja volitatud töötleja peavad rakendama turvalisuse tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid.

12.3. Infotehnoloogilised turvameetmed, mida eeskätt koolid peaksid esmaselt rakendama, on kajastatud käesoleva juhendi peatükis 3.

12.4. Tehnilised ja korraldusliku meetmed hõlmavad vastavalt vajadusele järgmisi tegevusi:
12.4.1. isikuandmete pseudonümiseerimine ja krüpteerimine;
12.4.2. on tagatud isikuandmeid töötlevate süsteemide ja teenuste kestev konfidentsiaalsus, terviklus, kättesaadavus ja vastupidavus;
12.4.3. on tagatud võimekus taastada õigeaegselt isikuandmete kättesaadavus ja juurdepääs andmetele füüsilise või tehnilise vahejuhtumi (intsidendi) korral;
12.4.4. tehnilisi ja korralduslikke meetmete tõhusust testitakse ja hinnatakse kooli siseselt korrapäraselt.

13. Ligipääsu haldus

13.1. Veerg „**Kellel on ligipääs“** – andmeregistri täitjal tuleb sisestada ametikohad, teenuse osutajad, partnerid jms, kellel on konkreetse protsessi raames kogutud isikuandmetele ligipääs. Näiteks e-kooli andmetele on ligipääs e-kooli teenuseosutajal, lapsevanemal, õpilasel; paberkandjal õpilasraamatule on aga ligipääs ainult õpetajaskonnal ja kooli juhtkonnal.

Lisa 1.a Andmeregistri vorm

Andmeregistri vorm on toodud eraldi Exceli failina.

Lisa 2 Infoturbe meetmed

Infoturbe juurutamine

Tihti arvatakse, et infoturbe meetmete juurutamine nõuab palju raha, kuid tegelikult ei pruugi see sugugi nii olla, kui asutuses töötab IT-spetsialist. Haridusasutustes on enamasti IT-spetsialist(id) juba olemas töölepingu või teenuslepingu alusel.

Selleks et turbemeetmed saaksid paika ja neid ka järgitaks, on kõige olulisem hoopis juhtkonna tugi uute nõuete ja käitumismudelite heaks kiitmisel ja nende fookuses hoidmisel. IT spetsialist üksi ei saa turvalisust tagada.

Olulisemaid teemasid, mis vajavad infovarade (sh isikuandmed) turvalisuse läbi mõtlemist ja põhimõtete paika panemist, on kokku üheksa. Analüüs on mõistlik läbi viia väikeses juht- või projektigrupis ning panna tulemused kirja ühte dokumenti.

Olulised teemad on järgmised:

1. Juhtkonna otsene tugi
   Töötage välja rollid ja vastutusalad, juhtimisstruktuur ja teabetalitluse eeskirjad, et luua infoturbe juhtimiseks vajalik toetusstruktuur.
2. Infoturbe käigushoid
   Infoturvet on vaja käigus hoida pidevalt. Vajadusel määrake selged vastutusalad, näiteks eelarvestamine, turbemeetmete kontroll ja aruandlus, juhendite loomine ja uuendamine, inimressursid jne.
3. Poliitikate ja standardite haldus
   Kirjeldage ja pange kirja põhimõtted ja juhendid, mille alusel tagatakse infoturvet asutuses (nt arvutivõrgu kasutamise kord, sülearvutite ja teiste kantavate seadmete kasutamise põhimõtted, infoturbepoliitika, arvutivõrgu ja infosüsteemide õiguste kord jne).
4. Andmete klassifitseerimine
   Selgitage välja (eeskätt GDPR lähtudes):
   - mis on need andmed, mis vajavad kaitset ning
   - mis tasemel see kaitse peaks olema (inimese, grupi, asutuse sisene või vaba ligipääs).

   Leidke ja tehke kindlaks, kus need andmed asuvad ja millega neid töödeldakse ehk looge infovarade nimekiri (nt arvutid, serverid, pilv, e-posti programm jne).
5. Riskide hindamine
   Vastavalt varadele viige läbi riskianalüüs. Riskide analüüsimiseks käige läbi varadele vastavad kohased ohustsenaariumid ning võimalikud kaitsemeetmed nende ohtude vältimiseks. NB! Tihti ei pöörata riskianalüüsile infoturbes piisavalt tähelepanu, kuid see aitab asutusel pikas plaanis kulusid märkimisväärselt kokku hoida ning keskenduda just kõige suurematele ohtudele.
6. Infoturbe teadlikkus ja koolitamine
   Mõtelge läbi plaan, mis aitab teil koolitada nii töötajaid kui ka õpilasi infoturbe valdkonnas. Olemas on erinevaid programme[33], mis aitavad selliseid koolitusi (ka tasuta) läbi viia.
7. Infoturbe ja füüsilise turbe seosed
   Vaadake üle füüsilise turvalisuse nõuded, sest näiteks serveriruumi kipsist seinad võivad nurjata kõik rakendatud turbemeetmed.
8. Intsidentide haldus
   Tavapärane on läbi mõelda käitumine tulekahju või mõne füüsilise ohu puhul. Infoturbega seotu võib aga luua sarnased olukordi. Sellepärast on vaja paika panna, kes, kuidas ja mida teeb erinevate intsidentide puhul. Mõtelge läbi, millised on need intsidendid, mis vajavad eelnevalt kokku lepitud käitumisjuhiseid, ning kuidas see kõik dokumenteeritakse.

[33] Kaitseliidu Küberkaitse Üksus viib läbi ja koostab näiteks koolitusi - http://www.kaitseliit.ee/et/kuberkaitse-uksus

9. Toimepidevus ja taaste
   Mõtelge läbi, milliseid andmeid ja kuidas kaitsta suuremate intsidentide korral. Kuidas käib varundamine ja kuidas toimub taastamine, kui näiteks serveriruum on maha põlenud või lunavara on krüpteerinud kõik asutuse arvutid ja serverid (need on näited päris elust).

Soovitav on kõik ülalmainitud üheksa valdkonda isikuandmeid silmad pidades läbi käia ning prioriteedid paika seada.

*Näiteks võime võtta **andmete klassifitseerimise:***

- Tuvastame, millistes süsteemides isikuandmed asuvad (lisaks arvutitele ja serveritele ka näiteks paberarhiivis, paberlepingutes jne), ning märgistame need kui konfidentsiaalsed andmed.
- Konfidentsiaalsetele andmetele on ligipääs vaid teatud kasutajagruppidel. Kõik ligipääsu erisused konfidentsiaalsetele andmetele tuleb dokumenteerida.
- Paberil olevad konfidentsiaalsed andmed tuleb vastavalt ka märgistada ning ligipääs neile peab olema piiratud kasutajagruppidel ja/või osakondadel.
- Süsteemides asuvaid andmeid eraldi ei märgistata, sest süsteemile kohalduvad vastavad turvanõuded.

Märkus: antud klassifikatsiooni saab laiendada terve asutuse ulatuses ning andmeid liigitada näiteks järgnevalt: avalikud, asutuse siseandmed, konfidentsiaalsed andmed ja salajased andmed. Vastavalt liigitusele võib seejärel määrata ka andmetele ligipääsud ja turvameetmed.

Turbemeetmete valik ja juurutamine

Turbemeetmed on jagatud kolme gruppi:

- põhimeetmed – meetmed, mille rakendamine aitab saavutada minimaalselt vajaliku turvataseme.
- baasmeetmed – meetmed, mis tagavad, et ka kasutajate tasemel oleks tagatud infoturbe baastase.
- organisatoorsed meetmed – meetmed, mis tegelevad ettevõttes üldise turvataseme tõstmisega ja viivad turbe kõrgemale tasemele.

Infoturbesüsteemi juurutamiseks alustage põhimeetmetest ning liikuge seejärel baasmeetmete ja edasi organisatoorsete meetmete juurde. Meetmete juurutamise järjekorra juures arvestage riskianalüüsis leituga.

Infoturbe eduka juurutamise eeldus

Infoturbe juurutamisel on väga oluline, et juhtkond (ja mitte vaid IT-osakond) veaks projekti. Sellest ei ole midagi, kui teadmisi ei ole piisavalt. Ei tohi karta esitada küsimusi. Lõpuks vastutab infoturbe eest ikka asutuse juht ning sellepärast tuleb ohjad hoida nn äripoole käes.

Meetmed ja meetmete grupid

I Põhimeetmed

Riistvara inventuur ja kontroll

Põhimõte

Kõiki asutuse või ettevõtte võrgus olevaid seadmeid tuleb aktiivselt hallata (arvet pidada, jälgida ja parandada), et ainult lubatud seadmed saaksid juurdepääsu andmetele. Volitamata seadmetele ei võimaldata juurdepääsu andmetele.

Miks on see meede oluline?

Ründajad, kes võivad paikneda kõikjal maailmas, otsivad pidevalt uusi seadmeid, mida võrku ühendatakse. Teadmata võõra seadme olukorda, võime oma võrku sisse tuua haavatava ja nakatunud seadme. Sageli jõuab haavatav seade enne pahavaraga nakatumist olla internetis vaid minuteid.

Tarkvara inventuur ja kontroll

Põhimõte
Lisaks seadmetele on vaja hallata (arvet pidada, jälgida ja parandada) ka võrgus olevat tarkvara, et kasutada saaks ainult volitatud tarkvara ning volitamata tarkvara leitaks ja eemaldataks arvutitest mõistliku aja jooksul.

Miks on see meede oluline?
Halvasti kontrollitavatest seadmetest on suurema tõenäosusega võimalik leida vana ja haavatavat tarkvara. Vana või ebavajalik tarkvara võib kaasa tuua turvaprobleeme ning süsteemide ja isikuandmed võivad sattuda ohtu.

Haavatavuste pidev juhtimine

Põhimõte
Selleks, et pakkuda ründajatele võimalikult vähem võimalusi, on vaja olukorda pidevalt hinnata ja haavatavused õigeaegselt tuvastada.

Miks on see meede oluline?
Haavatavuste mõistmine ja haldamine on pidev tegevus, millele tuleb kulutada aega ja tähelepanu. Asutused, mis ei tuvasta turvaauke ega tegele avastatud puudustega kiirelt, satuvad tihti rünnaku alla. Vajalik on haavatavuste tuvastamine läbi erinevate meetodite (käsitsi testid, automaatsed testid, tootjate infokanalite jälgimine) ning nende haldamine viisil (nn likvideerimine, ajutine paikamine jne), mis maandab haavatavusest tekkiva ohu.

Kontrollitud administraatoriõiguste kasutamine

Põhimõte
Jälgige ja kontrollige administraatoriõiguste andmise korraldust ja nende õiguste kasutamist ning hallake hoolikalt ligipääse võrkude ja rakenduste haldusliidestesse.

Miks on see meede oluline?
Administraatoriõiguste kuritarvitamine on peamine viis, kuidas ründajad liiguvad asutuse võrgus. Õiguste vargus võib toimuda valet veebilehte külastades või õngitsuskirja dokumenti või linki avades.

Riistvara ja tarkvara turvaline konfigureerimine mobiilseadmete, sülearvutite, tööjaamade ja serverite jaoks

Põhimõte
Vaja on luua ja seadistada mobiilseadmete, sülearvutite, serverite ja tööjaamade turvaline aluskonfiguratsioon, kasutades ranget konfiguratsioonijuhtimist ja muudatuste juhtimist, et vältida ründajate ligipääsu tundlikele teenustele.

Miks on see meede oluline?
Tootjad ja edasimüüjad tarnivad tihti oma operatsioonisüsteeme ja -rakendusi vaikekonfiguratsioonis, mida on tavaliselt hõlbus rünnata ja ära kasutada. Heade turvaseadete väljatöötamine on sellepärast ülimalt vajalik.

Logide haldus, järelevalve ja analüüs

Põhimõte
Koguge, hallake ja analüüsige sündmuste logi, mis aitab rünnakut tuvastada ja mõista ning algolukorda taastada.

Miks on see meede oluline?
Puudused logimisel ja logide analüüsimisel võimaldavad ründajal varjata oma asukohta, pahavara ja tegevusi. Isegi kui saate teada, et süsteemid on nakatunud, on logide puudumisel andmed rünnaku ja ründaja tegevuse kohta puudulikud.

II Baasmeetmed

E-posti ja veebibrauseri kaitse

Põhimõte
Piirake ründajate võimalusi veebibrauserit ja e-posti programme kasutavate inimestega manipuleerida. Kõik ei pea olema lubatud.

Näiteks koolitage inimesi kasutama kaht veebibrauserit, kus ühes on piirangud sisu kuvamisele ja skriptide käitamisele. E-posti kliendis ärge lubage läbi dokumente, mis sisaldavad skripte. Näiteid ja meetodeid on mitmed, leidke omale sobiv variant.

Miks on see meede oluline?
Veebibrauserid ja e-posti kliendid on väga levinud sisenemispunktid ründajale. Rünnakud võivad olla paindlikud ja tehniliselt keerukad.

Pahavara kaitse

Põhimõte
Kontrollige pahatahtliku koodi paigaldamist, levitamist ja käitamist.

Optimeerige süsteem automatiseerimist kasutades, et võimaldada kiiret kaitset, andmete kogumist ja parandusmeetmeid. Näiteks kasutage IOC-l (*indication of compromise*) põhinevat monitooringu-süsteemi , mis suudab automaatselt erinevaid infovooge oma tõrjereeglitesse integreerida. Samuti on praegu turul lahendusi, mis pakuvad tehisintellektil põhinevaid tõrjemeetmeid.

Miks on see meede oluline?
Pahatahtlik tarkvara on Interneti kasutamise lahutamatu ja ohtlik kaasavara, mis on mõeldud teie süsteemide, seadmete ja andmete ründamiseks. Pahavara on kiirelt liikuv ja muutuv ning võib siseneda läbi mitmete punktide, nagu lõppkasutajate seadmed, e-posti manused, veebilehed, pilveteenused ja eemaldatavad mäluseadmed.

Võrguportide, protokollide ja teenuste piiramine ja kontrollimine

Põhimõte
Halda, jälgi ja kontrolli portide, protokollide ja teenuste kasutamist võrguseadmetes, et minimeerida ründajatele kättesaadavaid haavatavusi.

Miks on see meede oluline?
Ründajad otsivad kaugjuurdepääsuga võrguteenuseid, mis on manipuleerimise suhtes haavatavad. Tavaliste näidete hulka kuuluvad halvasti konfigureeritud veebiserverid, e-posti serverid, faili- ja printimisteenused ning domeeniserverid (DNS), mis on vaikimisi installitud mitmesuguste erinevate seadmetüüpide jaoks, sageli ilma konkreetse teenuse vajaduseta.

Valmisolek andmete taastamiseks

Põhimõte
Mõelge läbi, mida ja kuidas teha, et kriitiline teave nõuetekohaselt varundada ja vajadusel taastada.

Miks on see meede oluline?
Kui ründajad masina(d) kompromiteerivad, teevad nad sageli olulisi muudatusi seadistuses ja tarkvaras. Mõnikord teevad ründajad ka kompromiteeritud masinatega salvestatud andmetes väikseid muudatusi. See kõik võib seada ohtu organisatsiooni töö.

Võrguseadmete (tulemüürid, marsruuterid ja *switch´*id) turvaline konfigureerimine

Põhimõte
Võrgu infrastruktuuri seadmete turvaline seadistamine ja aktiivne jälgimine, aruandlus ja korrigeerimine on vajalikud, et ründajad ei saaks haavatavaid teenuseid ja seadeid ära kasutada.

Miks on see meede oluline?
Tootjad ja edasimüüjad tarnivad seadmeid vaikekonfiguratsioonis, mis on hõlpsasti kasutatavad algpaigaldusel, kuid ei ole sugugi turvalised.

Perimeetri kaitse

Põhimõte
Jälgi infovoogu, mis liigub erineva usaldustasemega võrkude vahel.

Miks on see meede oluline?
Ründajad keskenduvad selliste süsteemide kasutamisele, milleni nad saavad jõuda interneti kaudu, sealhulgas ka töökohad ja sülearvutid, mis tõmbavad sisu interneti kaudu. Seetõttu peaks perimeetri kaitse olema mitmekihiline, tuginedes tulemüüridele, vahendajaserveritele, DMZ perimeetri võrkudele ja võrgupõhistele IPS[34] ja IDS[35] seadmetele/tarkvarale. Samuti on oluline, et filtreeritaks nii sissetulev kui ka väljaminev liiklus.

Andmekaitse

Põhimõte
Rakendage protsesse ja tööriistu, mida kasutatakse andmekao (*Data Loss Protection* ehk DLP) vältimiseks, et leevendada välja viidud andmete mõju ning kaitsta tundlikku teavet (privaatsuse ja andmete terviklikkuse tagamine).

Miks on see meede oluline?
Andmed asuvad paljudes kohtades. Kõige parem viis andmeid kaitsta on kombineerida krüpteerimist, terviklikkuse kaitset ja vältida andmekadu. Lekkinud või lekkivaid andmeid on võimalik mitmel moel kurjasti ära kasutada ning põhjustada seeläbi majanduslikku kahju.

Kontrollitav ligipääs põhineb teadmisvajadusel

Põhimõte
Andmete klassifitseerimist aluseks võttes saab luua kindla ligipääsu kriitilistele varadele (nt teave, ressursid, süsteemid) ja luua nende ligipääsude kontrollmehhanismid.

Miks on see meede oluline?
Andmete krüptimine annab kindluse, et isegi kui andmed on kahjustatud, on juurdepääs nendele andmetele oluliselt raskendatud. Kontrollides ligipääse ja andmete liikumist üle võrgu piiride nii elektrooniliselt kui ka füüsiliselt, saame viia miinimumini kokkupuute ründajatega.

Traadita juurdepääsu kontroll

Põhimõte
Tuleb luua traadita kohtvõrkude (WLAN), pöörduspunktide ja traadita kliendisüsteemide turvalisuse tagamiseks / juhtimiseks / vältimiseks / parandamiseks kasutatavad protsessid ja vahendid.

Miks on see meede oluline?
Andmete varguse on tihti algatanud ründajad, kes on saanud traadita võrgu kaudu juurdepääsu organisatsioonidele väljastpoolt füüsilist hoonet, minnes mööda organisatsioonide turbepiirangutest.

Kontode jälgimine ja kontroll

Põhimõte
Süsteemide ja rakenduste kontode elutsükli aktiivne haldamine – kontode loomine, kasutamine, puhkeaeg, kustutamine – et minimeerida ründajate võimalusi.

[34] IPS - Intrusion prevention system
[35] IDS - Intrusion detection system

Miks on see meede oluline?
Ründajad kasutavad sageli mitteaktiivseid kasutajakontosid, et imiteerida seaduslikke kasutajaid, mistõttu turvalisuse eest vastutajatel on keeruline avastada ründaja käitumist, kui mitteaktiivsed ja kehtetud kontod pole desaktiveeritud.

III Organisatoorsed meetmed

Turvateadlikkuse tõstmine ja hindamine

Põhimõte
Kõik asutuse töötajad peavad olema turvateadlikud ja toetama turvet asutuses.

Miks on see meede oluline?
Küberturve pole ainult tehniliste tööriistade kogum. Kasutajate asjakohane käitumine tagab paljude ohtude maandamise. Paljud ründed toimuvad inimeste käitumismudelite manipuleerimise teel (*social engineering*) ja seetõttu on turvateadlik inimene oluline kaitsemeede.

Rakendustarkvara turvalisus

Põhimõte
Turvaprobleemide vältimiseks, avastamiseks ja parandamiseks juhtige ettevõtte tarkvara elutsüklit.

Miks on see meede oluline?
Ründed kasutavad tihti rakendustarkvaradel leitud haavatavusi. Seetõttu on oluline haavatavused likvideerida ja paigaldada uuendused.

Intsidentidele reageerimine ja nende juhtimine

Põhimõte
Juurutage intsidentide haldamise protsess – plaanid, rollid, koolitus, side, juhtimisjärelevalve. Samuti seadke sisse isikuandmete rikkumiste tuvastamise, olulisuse hindamise ja osapoolte (AKI/andmesubjekt) informeerimise reeglid juhul, kui informeerimine on nõutav. See võimaldab rünnakuid kiiresti avastada ja seejärel kahju minimeerida.

Miks on see meede oluline?
Küberintsidendid on kahjuks meie eluviisi osa. Isegi suured, hästi rahastatud ja tehniliselt keerukad ettevõtted püüavad rünnakute sageduse ja keerukusega sammu pidada. Küberründe ohvriks langemise puhul pole küsimus „kas", vaid „millal".

Läbistustestid (*pentest*) ja harjutused

Põhimõte
Simuleerige ründeid, et teada saada oma nõrkuseid ja puuduseid.

Miks on see meede oluline?
Ründajad kasutavad tihti ära puuduseid kaitsemeetmetes ning nn heatahtlikud ründetestid võimaldavad need puudused õigeaegselt avastada ja likvideerida.

Lisa 3 – Õigusaktide näitlik loetelu

Selles lisas on toodud näitlik loetelu haridusvaldkonna õigusaktidest (seadused, Vabariigi Valitsuse ning haridus- ja teadusministri määrused), milles on isikuandmete töötlemisega seotud regulatsioone ning mis on teatud juhtudel haridusasutusele aluseks konkreetsete isikuandmete kogumiseks.
Nimekiri ei ole ammendav ning lisaks loetelus välja toomata riiklikele õigusaktidele tuleb lähtuda haridusasutuste pidajate (nt kohalike omavalitsuste) valdkondlikest õigusaktidest/regulatsioonidest ning haridusasutuste sisestest regulatsioonidest.

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32016R0679&from=ET

Teabe andmist ja -haldust reguleerivad õigusaktid

- Avaliku teabe seadus https://www.riigiteataja.ee/akt/104072017011?leiaKehtiv
- Märgukirjale ja selgitustaotlusele vastamise ning kollektiivse pöördumise esitamise seadus https://www.riigiteataja.ee/akt/820158?leiaKehtiv
- Teenuste korraldamise ja teabehalduse alused https://www.riigiteataja.ee/akt/131052017007
- Arhiivieeskiri https://www.riigiteataja.ee/akt/131052017011?leiaKehtiv

Alusharidus

- Koolieelse lasteasutuse seadus https://www.riigiteataja.ee/akt/122012018006?leiaKehtiv
- Koolieelse lasteasutuse õppe- ja kasvatustegevuse alaste kohustuslike dokumentide loetelu ja nende täitmise kord https://www.riigiteataja.ee/akt/120022018032?leiaKehtiv
- Tervisekaitsenõuded koolieelses lasteasutuses tervise edendamisele ja päevakavale https://www.riigiteataja.ee/akt/13360326
- Koolieelse lasteasutuse pedagoogide kvalifikatsiooninõuded https://www.riigiteataja.ee/akt/103092013036?leiaKehtiv

Üldharidus

- Põhikooli ja -gümnaasiumiseadus https://www.riigiteataja.ee/akt/122012018003?leiaKehtiv
- Õpilase kooli vastuvõtmise üldised tingimused ja kord ning koolist väljaarvamise kord https://www.riigiteataja.ee/akt/13359746?leiaKehtiv
- Kooli õppe- ja kasvatusalastes kohustuslikes dokumentides esitatavad andmed ning dokumentide täitmise ja pidamise kord https://www.riigiteataja.ee/akt/13352237#
- Põhikooli ja gümnaasiumi lõputunnistuse ning riigieksamitunnistuse statuut ja vormid https://www.riigiteataja.ee/akt/114022018006?leiaKehtiv
- Riigi üldhariduskooli hoolekogu moodustamise kord ja töökord https://www.riigiteataja.ee/akt/103092013046?leiaKehtiv
- Tasemetööde ning põhikooli ja gümnaasiumi lõpueksamite ettevalmistamise ja läbiviimise ning eksamitööde koostamise, hindamise ja säilitamise tingimused ja kord ning tasemetööde, ühtsete põhikooli lõpueksamite ja riigieksamite tulemuste analüüsimise tingimused ja kord https://www.riigiteataja.ee/akt/120022018014?leiaKehtiv
- Õpetaja ja tugispetsialisti lähtetoetuse taotlemise, maksmise ja tagasinõudmise kord https://www.riigiteataja.ee/akt/102032018001
- Kooliraamatukogude töökorralduse alused https://www.riigiteataja.ee/akt/103092013024?leiaKehtiv
- Direktori, õppealajuhataja, õpetajate ja tugispetsialistide kvalifikatsiooninõuded https://www.riigiteataja.ee/akt/130082013005

- Õpilaspileti väljaandmise kord ja õpilaspileti vorm https://www.riigiteataja.ee/akt/13349855
- Koolitervishoiuteenust osutava õe tegevused ning nõuded õe tegevuste ajale, mahule, kättesaadavusele ja asukohale https://www.riigiteataja.ee/akt/108122011010
- Koduõppe ja haiglaõppe tingimused ja kord https://www.riigiteataja.ee/akt/106032018001
- Põhikooli lihtsustatud riiklik õppekava https://www.riigiteataja.ee/akt/114022018007
- Koolivälisele nõustamismeeskonnale soovituse andmiseks esitatavate andmete loetelu, taotluse esitamise ning koolivälise nõustamismeeskonna soovituse andmise tingimused ja kord https://www.riigiteataja.ee/akt/114022018014
- Tugispetsialistide teenuse kirjeldus ja teenuse rakendamise kord https://www.riigiteataja.ee/akt/127022018010

Kutseharidus

- Kutseõppeasutuse seadus https://www.riigiteataja.ee/akt/122012018007?leiaKehtiv
- Kutseharidusstandard https://www.riigiteataja.ee/akt/116072016008?leiaKehtiv
- Kutseõppeasutuse arendustegevust ja õppekasvatustööd käsitlevate kohustuslike dokumentide nõuded ja dokumentide pidamise kord https://www.riigiteataja.ee/akt/129082013016
- Õpilase kutseõppeasutusse vastuvõtu kord https://www.riigiteataja.ee/akt/129082013018?leiaKehtiv
- Erivajadusega isikute kutseõppeasutuses õppimise tingimused ja kord https://www.riigiteataja.ee/akt/115052014004
- Kutseõppeasutuse õppekasvatusala töötaja vaba ametikoha täitmiseks korraldatava avaliku konkursi tingimused ja kord https://www.riigiteataja.ee/akt/129122013004
- Nõuded kutseõppeasutuse õpilaspiletile ja selle väljaandmise kord https://www.riigiteataja.ee/akt/129082013019
- Õppetoetuste ja õppelaenu seadus https://www.riigiteataja.ee/akt/128112017034?leiaKehtiv
- Kutseõppeasutuses täiendusõppe korraldamise tingimused ja kord https://www.riigiteataja.ee/akt/120092013010

Rakenduskõrgharidus

- Rakenduskõrgkooli seadus https://www.riigiteataja.ee/akt/120122016003?leiaKehtiv
- Kõrgharidusstandard https://www.riigiteataja.ee/akt/126092017010?leiaKehtiv
- Diplomi ja akadeemilise õiendi statuut ja vormid https://www.riigiteataja.ee/akt/128042015007?leiaKehtiv
- Üliõpilaspileti väljaandmise kord https://www.riigiteataja.ee/akt/13011516
- Õppetoetuste ja õppelaenu seadus https://www.riigiteataja.ee/akt/128112017034?leiaKehtiv

Kõikidel haridustasemetel

- Erakooliseadus https://www.riigiteataja.ee/akt/122012018005