Álit um vinnslu og öryggi persónuupplýsinga í vefkerfinu Mentor - mál nr. 2015/1203

Álit

Hinn 22. september 2015 samþykkti stjórn Persónuverndar, með vísun til 6. tölul. 3. mgr. 37. gr. laga nr. 77/2000, svohljóðandi álit í máli nr. 2015/1203:

I.

Upphaf máls

Bréfaskipti, vettvangsathuganir og viðtöl

1.

Upphaf máls

Síðustu misseri hefur Persónuvernd borist nokkur fjöldi ábendinga og fyrirspurna vegna vefkerfisins Mentor og þeirrar vinnslu persónuupplýsinga sem þar fer fram á vegum grunnskóla. Þær ábendingar sem Persónuvernd hafa borist benda til þess að viðtækarpersónuupplýsingar um grunnskólanemendur séu skráðar í Mentor og að ósamræmi sé milli kennara og/eða grunnskóla við skráningu persónuupplýsinga í kerfið, einkum að því er varðar færslur í dagbókarflipa þess. Þá vörðuðu ábendingarnar sem stofnuninni bárust í einhverjum tilvikum viðkvæmar persónuupplýsingar, meðal annars varðandi andlegt og líkamlegt heilsufar nemenda.

Á grundvelli framangreindra ábendinga taldi Persónuvernd þörf á, í ljósi eftirlitshlutverks stofnunarinnar skv. 2. tölul. 3. mgr. 37. gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga, að framkvæma úttekt sem beindist að skráningu og meðferð persónuupplýsinga í Mentor hjá grunnskólum, sem og öryggi þeirra upplýsinga, m.a. með tilliti til öryggiskerfa þeirra. Var því ákveðið að kanna hvort vinnslapersónuupplýsinga í Mentor og öryggiskerfi ábyrgðaraðila væri í samræmi við lög nr. 77/2000 og reglur nr. 299/2001 um öryggi persónuupplýsinga, t.d. varðandi heimildir fyrir vinnslu og hvort hún samrýmist sjónarmiðum um sanngirni, meðalhóf og áreiðanleika.

Þar sem margir grunnskólar nota vefkerfið Mentor um allt land var talið fýsilegt að velja fimm grunnskóla af handahófi sem úttektin myndi beinast að. Urðu [A-skóli], [B-skóli], [C-skóli], [D-skóli], [E-skóli] fyrir valinu.

Með bréfi Persónuverndar til framangreindra skóla, dags. 17. febrúar 2015, var boðuð úttekt á þeirri vinnslu persónuupplýsinga sem þar færi fram tengd notkun Mentor vefkerfisins með vísan til 2. tölul. 3. mgr. 37. gr. laga nr. 77/2000. Í því skyni var kallað eftir skriflegum gögnum, þ.e. öryggisstefnu, áhættumati og lýsingu á öryggisráðstöfunum, auk þess sem tilkynnt var um fyrirhugaða vettvangsskoðun Persónuverndar hjá viðkomandi skólum. Var Mentor ehf. upplýst um fyrirhugaðar úttektir með bréfi, dags. 31. mars 2015.

2.

Bréfaskipti og málavextir

Í bréfum Persónuverndar til framangreindra grunnskóla var óskað eftir ýmsum upplýsingum til að varpa ljósi á hvernig vinnslu og öryggi persónuupplýsinga í vefkerfinu Mentor er háttað. Einnig var óskað eftir yfirliti yfir þær persónuupplýsingar sem grunnskólarnir vinna með í Mentor og þær lagaheimildir sem vinnsla þeirra byggir á.

Svör grunnskólanna bárust Persónuvernd á tímabilinu 9. mars – 8. apríl 2015. Í svörum grunnskólanna er vísað til þeirra upplýsinga sem skráðar eru í s.k. nemandaspjaldi í Mentor. Á nemandaspjaldinu eru að finna grunnupplýsingar um nemanda, svo sem nafn, kennitölu, heimilisfang, lögheimili, netfang og síma. Svör grunnskólanna varðandi skráningu annarra upplýsinga eru mismunandi. Í sumum svarbréfum kemur ekki fram hvort önnur skráning fari fram, svo sem um ástundun og dagbókarskráningu. Í öðrum svarbréfum kemur fram að skráðar séu upplýsingar í Mentor um ástundun og annar texti í dagbókarflipa vefkerfisins og loks kemur fram í svarbréfi eins grunnskólans að einnig væru skráðar persónuupplýsingar um aðra en nemendur, n.t.t. um starfsmenn og aðstandendur. Varðandi heimildir fyrir vinnslu vísa grunnskólarnir ýmist til laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga eða eldri laga nr. 121/1989 um skráningu og meðferð persónuupplýsinga. Þá vísa sumir skólar sérstaklega til 3., 4. og 7. tölul. 1. mgr. 8. gr. og 7. gr. laga nr. 77/2000 sem heimild fyrir vinnslu persónuupplýsinga.

Varðveislutími gagna

Þá voru grunnskólarnir spurðir út í varðveislutíma gagna í Mentor og hvernig leitast væri við að tryggja að þær væru réttar og áreiðanlegar. Af svörum grunnskólanna verður ráðið að enginn þeirra hafi reglur um varðveislutíma gagna í Mentor en skólarnir vísa til þess að vistun gagna í Mentor falli undir almennar skilgreiningar um vistun opinberra gagna, meðal annars samkvæmt skjalastjórnunarstefnu Reykjavíkurborgar. Nokkrir grunnskólanna vísa til þess að Mentor skrái hver geri breytingar á upplýsingum og kerfið geri t.d. sjálfkrafa viðvart ef miklar breytingar eru gerðar á dagbókar- og ástundunarfærslum nemanda á stuttum tíma.

Öryggisstefna, áhættumat og lýsing á öryggisráðstöfunum

Jafnframt óskaði Persónuvernd eftir að grunnskólarnir sendu skriflega öryggisstefnu, áhættumat, lýsingu á öryggisráðstöfunum og lýsingu á fyrirkomulagi innra eftirlits. Í svörum grunnskólanna kemur fram að enginn skólanna er með skjöl af framangreindum toga.

Þá óskaði Persónuvernd eftir upplýsingum um fyrirkomulag aðgangsstýringa ásamt viðeigandi verklagsreglum. Í svörum grunnskólanna um þessi atriði er því lýst hvernig aðgangsheimildir til starfsmanna eru veittar, en þær eru oftast í höndum skólastjórnenda. Þá sé aðgangi starfsmanna stýrt með þeim hætti að þeir fá aðgang að nemendum þess bekkjar sem þeir kenna samkvæmt stundaskrá. Þá kemur fram í svarbréfunum að aðgangur foreldra stýrist af tengslum þeirra við barnið í Mentor og geti aðrir aðstandendur fengið aðgang að upplýsingum um barnið samkvæmt ósk foreldra. Þá er í einu svarbréfi nokkuð nákvæm lýsing á þeim aðgangshópum sem skilgreindir eru fyrir starfsmenn.

Í bréfi Persónuverndar var óskað eftir lýsingu á þeim öryggisráðstöfunum sem til staðar eru til að koma í veg fyrir að óviðkomandi fái aðgang að upplýsingum sem skráðar eru í Mentor. Í svörum grunnskólanna kemur fram að aðgangi sé stýrt með þeim hætti að starfsmenn hafa einungis aðgang að upplýsingum um þá nemendur sem þeir hafa samskipti við vegna starfs síns. Þá sé aðgangi stýrt með einkvæmu notendanafni og lykilorði og loki kerfið sjálfkrafa á aðgang ef notandi er óvirkur í 40 mínútur. Þá sýni kerfið notanda hvenær hann var skráður inn síðast og getur hann þannig séð hvort einhver annar hafi skráð sig inn með hans notendanafni.

Vinnslusamningur

Þá óskaði Persónuvernd eftir upplýsingum um vinnslusamning grunnskólanna við Mentor ehf. og staðfestingu á því að ábyrgðaraðili, sem að öllum líkindum væri hver og einn grunnskóli, hefði kannað öryggi hjá vinnsluaðila. Grunnskólarnir vísuðu allir í s.k. „nytjaleyfis- og þjónustusamning um upplýsingakerfið Mentor.is“, sem er samningur sem Mentor ehf. gerir við grunnskólana þegar kerfið er tekið í notkun. Í svörum grunnskólanna kemur fram að enginn þeirra hafi kannað öryggi hjá Mentor ehf.

3.
Upplýsingar sem aflað var í vettvangsathugun

Í kjölfar bréfaskipta við grunnskólana var farið í vettvangsathugun í þá skóla sem úttektin náði til, nánar tiltekið hjá skóla A þann 7. apríl 2015, hjá skóla B þann 17. apríl 2015, hjá skóla C þann 8. maí 2015, hjá skóla D þann 27. maí 2015 og hjá skóla E þann 4. júní 2015.

Í hverri vettvangsathugun voru tekin viðtöl við tiltekna starfsmenn skólanna og leitað svara við tilteknum spurningum Persónuverndar. Í hverjum skóla var rætt annars vegar við skólastjórnendur og ritara, og hins vegar við almenna starfsmenn, þ.e. kennara og hjúkrunarfræðinga. Þar sem enginn grunnskólanna starfrækir formlegt öryggiskerfi var markmið vettvangsathuganna einkum að kanna stöðu öryggismála og afstöðu starfsmanna til þeirra auk þess að kanna atriði sem tengjast skráningu upplýsinga í Mentor.

3.1. Viðtöl við skólastjórnendur og ritara

Í upphafi hverrar vettvangsathugunar var rætt við skólastjórnendur og ritara. Þeir voru spurðir um aðgangsstýringar, leiðbeiningar til starfsmanna um skráningu og öryggismál, eftirlit með starfsmönnum, samskipti við Mentor ehf. sem vinnsluaðila, leiðbeiningar til foreldra og öryggiskerfi skólans.

Varðandi aðgangsstýringar kom fram að aðgangur kennara stýrist oftast af uppsetningu stundatöflu, líkt og kom fram í svarbréfum skólanna til Persónuverndar. Umsjónarkennari hafi almennt aðgang að meiri upplýsingum en aðrir kennarar, þar sem oft séu færslur í dagbókarflipa skráðar til birtingar gagnvart umsjónarkennara og stjórnendum en ekki öðrum kennurum. Þá sjái ritarar og skólastjórnendur um að úthluta nýjum kennurum aðgangsorði. Samsetning kennitölu og lykilorðs myndi einkvæman aðgang en sami einstaklingur geti verið með fleiri en einn aðgang, t.d. ef viðkomandi er líka foreldri og hafi foreldraaðgang á sömu kennitölu. Þá sé notendanafn það sama, þ.e. kennitala, en lykilorðin ólík. Dæmi séu um kennara sem kenna í fleiri en einum skóla og hafi þá fleiri en einn notendareikning, þar sem notendanafn er það sama, en lykilorð ólík. Þegar kennari ljúki störfum sé reikningur hans gerður óvirkur. Í viðtölum við flesta skólastjórnendur kom fram að reglulega væri farið yfir lista notenda og sannreynt að ekki væri opinn aðgangur kennara sem lokið hefðu störfum en ekki kom fram að til væri formleg skjölun um slíka framkvæmd. Þá kom fram að aðgangi væri aldrei deilt milli starfsmanna heldur noti hver kennari sinn eigin notendareikning.

Í samtölum við skólastjórnendur kom fram að leiðbeiningar til starfsmanna um skráningu og öryggismál væru almennt veittar á kennarafundum og að einhverju marki til nýrra kennara þegar þeir hefja störf. Þá kom fram að Mentor ehf. hafi í einhverjum tilvikum haldið námskeið að eigin frumkvæði. Hins vegar kom fram að í grunnskólunum væru hvergi fyrirliggjandi skriflegar leiðbeiningar um skráningu í Mentor og öryggismál. Í sumum skólanna hafi nýir starfsmenn verið látnir undirrita þagnarskylduyfirlýsingu en enginn skólanna gat fullyrt að allir starfsmenn hefðu undirritað slíka yfirlýsingu og hvergi hafði sú framkvæmd verið yfirfarin kerfisbundið. Einnig kom fram að þar sem Mentor sé vefkerfi geti kennarar

tengst því hvaðan sem er á netinu en enginn grunnskólanna hafi haft uppi sérstaka fræðslu vegna slíkrar notkunar eða kannað öryggisatriði tengd slíkum fjaraðgangi.

Þá kom fram að stjórnendur hafi almennt ekki kerfisbundið eftirlit með starfsmönnum, hvernig þeir noti Mentor eða hvað þeir skrái inn í kerfið. Í samtölunum kom fram að einstaka stjórnendur hafi gert athugasemdir við skráningar starfsmanna í Mentor en það hafi verið gert í kjölfar þess að stjórnendur hafi fengið tilkynningu frá kerfinu um að færsla hafi verið skráð, en slíkar tilkynningar berast þegar kennari velur sérstaklega að senda þær til t.d. skólastjóra eða umsjónarkennara. Þá kom fram að flestir skólastjórnendur hafi ekki velt fyrir sér hugsanlegri aðgerðaskráningu í kerfinu og því ekki frætt starfsmenn um hana.

Varðandi samskipti við Mentor ehf. sögðust stjórnendur almennt vera á þeirri skoðun að það væri ákvörðun hvers og eins grunnskóla hvort hann gerði samning við Mentor ehf. Þau samskipti sem grunnskólarnir hafi átt við Mentor ehf. hafi fyrst og fremst beinst að virkni kerfisins en ekki meðferð eða öryggi þeirra upplýsinga sem Mentor ehf. vinnur með fyrir ábyrgðaraðila.

Í samtali við skólastjórnendurna kom fram að mismikil áhersla væri lögð á fræðslu til foreldra um Mentor, en foreldrum sé fyrst og fremst leiðbeint um hvernig eigi að fara inn í Mentor þegar nemendur hefji nám í grunnskólum. Þá upplýsi ekki allir skólarnir foreldra um að í Mentor séu hugsanlega skráðar upplýsingar um börn þeirra sem þeir hafi ekki beinan aðgang að, t.d. þegar upplýsingar um nemendur eru ekki birtar foreldrum.

Þá var það staðfest í samtölum við skólastjórnendur, sem fram hafði komið í skriflegum svörum grunnskólanna, að enginn þeirra væri með öryggiskerfi í samræmi við reglur nr. 299/2001 um öryggi persónuupplýsinga.

3.2. Viðtöl við kennara og aðra starfsmenn

Í vettvangsathugun hvers skóla var einnig fundað með völdum kennurum og öðrum starfsmönnum sem höfðu aðgang að Mentor. Í samráði við skólastjórnendur voru valdir kennarar og starfsmenn sem höfðu bæði mismunandi og mismikla aðkomu að skólastarfinu. Voru þeir spurðir um aðgangsstýringar, leiðbeiningar sem þeir hafi fengið, notkun fjaraðgangs og leiðbeiningar til foreldra.

Í samtali við kennara og starfsmenn grunnskólanna kom fram að þeir hafi allir fengið aðgang að Mentor hjá skólastjórnendum eða ritara. Kennarar og starfsmenn hafi yfirleitt aðgang að upplýsingum um nemendur sem stýrist af stundatöflu en sumir hafi aðgang sem sé stýrt sérstaklega niður á hópa. Einhverjir þeirra séu einnig foreldrar barna í öðrum grunnskólum og hafi sem slíkir einnig foreldraaðgang að Mentor. Þá kom fram að kennarar og starfsmenn hafi fengið úthlutað lykilorði sem þeir hafi svo breytt strax, en það sé þó ekki algilt. Þá sé mjög misjafnt hvernig og hversu oft þeir breyti lykilorðum sínum. Kennarar og starfsmenn hafi aðgang að öllum eldri upplýsingum þeirra nemenda sem þeir kenna eða sinna en engan aðgang að upplýsingum um nemendur sem þeir kenni eða sinni ekki lengur. Kennararnir tóku það fram að þeir deili ekki aðgangi sínum með öðrum kennurum.

Varðandi fræðslu um notkun á Mentor kom fram að engar skriflegar leiðbeiningar um skráningu upplýsinga væri að finna hjá grunnskólunum. Þá kom fram að hluti kennaranna og starfsmannanna hafi fengið munnlegar leiðbeiningar um hvernig standa skyldi að skráningu í Mentor, t.d. frá yfirmönnum, frá öðru samstarfsfólki á starfsmannafundum eða frá starfsfólki Mentor ehf. á tilfallandi kynningarfundum þess hjá skólanum. Þá kom fram að kennararnir reyni að gæta þess að nefna ekki nafn þriðja aðila þegar skráð sé í dagbókarflipa og að hafa skráningar hlutlægar. Grunnskólarnir hafi ekki verið með fræðslu um öryggismál en einhverjum kennurum og starfsmönnum höfðu borist áminningar frá kerfisstjórum um að skipta um lykilorð.

Kennarar og starfsmenn grunnskólanna voru spurðir út í fjaraðgang þeirra að Mentor. Í svörum þeirra kom fram að flestir þeirra nýta sér að geta tengst Mentor að heiman. Skólastjórnendur hafi ekki rætt öryggismál tengd notkun á fjaraðgangi að Mentor. Í flestum tilvikum séu kennararnir og aðrir starfsmenn að notast við eigin tölvu sem þeir einir hafi aðgang að og tengist um þráðlaust net, en einnig séu dæmi um að þeir tengist Mentor á tölvum sem þeir deila með öðrum. Þá kom fram að flestir hafi talið að veiruvarnir væru fullnægjandi á heimatölvum sínum og gættu þess að vista ekki lykilorð í vafra. Þá notuðu einstakir kennarar og starfsmenn heimatölvu sem deilt sé með öðrum og vistuðu lykilorð í Mentor í vafra.

Þeir kennarar og starfsmenn sem rætt var við í vettvangsathuguninni höfðu ekki verið fræddir um hugsanlega aðgerðaskráningu, þó að margir segðust allt eins eiga von á því að ýmsar upplýsingar um notkun þeirra á kerfinu væru skráðar.

Þá kom fram í samtölum við kennarana og aðra starfsmenn að ekki væri mikið um reglubundna fræðslu til foreldra um skráningu í Mentor eða notkun kerfisins. Foreldrum gæti því verið ókunnugt um að upplýsingar væru skráðar um börn þeirra í Mentor, enda kjósi kennarar oft að birta ekki foreldrum færslur sem þeir skrifa.

4.
Bréfaskipti við Mentor ehf.

Með bréfi, dags. 26. júní 2015, óskaði Persónuvernd eftir frekari upplýsingum frá Mentor ehf., sem hýsingar- og rekstraraðila vefkerfisins Mentor. Meðal annars óskaði Persónuvernd eftir upplýsingum tengdum samningagerð við þjónustukaupendur, þ.e. hvern grunnskóla, hvort þeir hefðu veitt félaginu fyrirmæli um meðferð eða ráðstöfun persónuupplýsinga í kerfinu, hvernig varðveislu upplýsinganna væri háttað, hvernig aðgerðarskráningu í kerfinu væri háttað og hvernig öryggis væri gætt varðandi aðgangsstýringu.

Í svarbréfi Mentor ehf., dags. 19. ágúst 2015, segir meðal annars að félagið sjálft hafi útbúið þá samninga sem þjónustukaupendur undirrita (s.k. „nytjaleyfis- og þjónustusamninga“) og að þeir séu staðlaðir. Þá hafi félagið í

einhverjum tilvikum, í kjölfar samningagerðar við skólana, fengið fyrirmæli frá einstökum skólum um ráðstöfun upplýsinga úr kerfinu, en þau tilvik hafa einungis lotið að afhendingu tiltekinna upplýsinga til tilgreindra aðila, á borð við Skólapúlsinn ehf., Hagstofuna eða embætti landlæknis, en ekki varðandi öryggi þeirra. Þjónustukaupendur hafa ekki sannreynt hvort Mentor ehf. geti viðhaft viðhlítandi öryggisráðstafanir. Telur Mentor ehf. að það sé í engum tilvikum ábyrgðaraðili vinnslu persónuupplýsinga í vefkerfinu Mentor.

Varðandi útskrifaða nemendur segir Mentor ehf. að þær upplýsingar séu gerðar óaðgengilegar fyrir notendur, nema fyrir skólastjórnendur, en þeim sé ekki eytt úr grunninum.

Bendir Mentor ehf. á að vefkerfið skrái allar aðgerðir sem framkvæmdar eru þar, svo að unnt sé að rekja slóð notenda, en ekki innihald skráninganna. Hafa þau gögn í einstökum tilvikum verið skoðuð í samráði við þjónustukaupanda, en aldrei afhent.

Einnig segir í svarbréfinu að Mentor ehf. haldi reglulega námskeið sem sérstaklega séu ætluð þjónustukaupendum. Á þeim sé farið yfir notendahópa í kerfinu, úthlutun lykilorða, og hvað sé nauðsynlegt að skrá í Mentor svo það starfi í samræmi við væntingar notenda. Þá nota ekki allir skólar dagbókarflipa kerfisins, en þeir sem gera það fá sérstaka kennslu um notkun dagbókarflipans, þótt endanleg útfærsla á skráningum í slíkri dagbók sé val skólanna sjálfra. Sömuleiðis ákveði skólarnir sjálfir hvort þeir heimili foreldrum og/eða nemendum að sjá færslur í dagbókarflipa Mentor.

Með svarbréfi Mentor ehf. fylgdi einnig afrit af lýsingu á notendahópum kerfisins, þar sem lýst er hvernig aðgangi hvers hóps er háttað, sem og afrit af námskeiðsgögnum félagsins. Í námskeiðsgögnunum virðist meðal annars vikið að því að skrá megi viðkvæmar persónuupplýsingar í dagbókarflipa, en að skólarnir beri ábyrgð á að öll vinnsla gagna sé í samræmi við lög um persónuvernd og meðferð persónuupplýsinga. Þá segir einnig að varast skuli að orðalag, sem og lýsingar, séu byggðar á huglægu mati. Þá þurfi samræmi að vera innan skólans varðandi ýmis atriði tengd skráningu upplýsinga í kerfið.

II.

Niðurstaða Persónuverndar

1.

Almenn atriði tengd vinnslu persónuupplýsinga

1.1.

Afmörkun úrlausnarefnis

Svo sem fyrr greinir taldi Persónuvernd þörf á úttekt á efni og öryggi upplýsinga sem skráðar eru í Mentor hjá grunnskólum í samræmi við lög nr. 77/2000 og reglur nr. 299/2001 um öryggi persónuupplýsinga, í ljósi þeirra ábendinga sem stofnuninni hafa borist. Af skriflegum svörum þeirra grunnskóla sem mál þetta varðar var ráðið að enginn þeirra var með öryggiskerfi eða skrifleg gögn tengd öryggi, áhættumati eða innra eftirliti. Þegar af þeirri ástæðu taldi stofnunin ógerlegt að framkvæma þá öryggisúttekt sem lagt var upp með í fyrstu, enda miða slíkar úttektir almennt við að stofnunin leggi mat á áðurnefnd gögn og öryggiskerfi ábyrgðaraðila.

Engu að síður taldi Persónuvernd að unnt væri að ljúka athuguninni með því að kanna almennt lögmæti og öryggi þeirrar vinnslu sem fram fer á vegum skólanna í Mentor, m.t.t. eftirlitshlutverks stofnunarinnar samkvæmt 2. tölul. 3. mgr. 37. gr. laga nr. 77/2000 og veita í kjölfarið álit samkvæmt 6. tölul. sama ákvæðis og tilmæli á grundvelli þess, sbr. eftirfarandi umfjöllun.

1.2.

Gildissvið laga nr. 77/2000

Gildissvið laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga, sbr. 1. mgr. 3. gr. þeirra laga, og þar með valdsvið Persónuverndar, sbr. 1. og 2. mgr. 37. gr. laganna, nær til sérhverrar rafrænnar vinnslu persónuupplýsinga, sem og handvirkrar vinnslu slíkra upplýsinga sem eru eða eiga að verða hluti af skrá. Persónuupplýsingar eru sérhverjar persónugreindar eða persónugreinanlegar upplýsingar, þ.e. upplýsingar sem beint eða óbeint má rekja til tiltekins einstaklings, látins eða lifandi, sbr. 1. tölul. 2. gr. laganna; og vinnsla er sérhver aðgerð eða röð aðgerða þar sem unnið er með persónuupplýsingar, hvort heldur sem vinnslan er handvirk eða rafræn, sbr. 2. tölul. 2. gr. Í athugasemdum við 2. tölul. 2. gr. í því frumvarpi, sem varð að lögum nr. 77/2000, kemur fram að hver sú aðferð, sem nota má til að gera upplýsingar tiltækar, telst til vinnslu.

Af þessu öllu er ljóst að mál þetta lýtur að vinnslu persónuupplýsinga sem fellur undir valdsvið Persónuverndar.

1.3.

Um ábyrgðaraðila og vinnsluaðila

Sá sem ber ábyrgð á að vinnsla persónuupplýsinga samrýmist lögum nr. 77/2000 er nefndur ábyrgðaraðili. Samkvæmt 4. tölul. 2. gr. laganna er þar átt við þann sem ákveður tilgang vinnslu persónuupplýsinga, þann búnað sem notaður er, aðferð við vinnsluna og aðra ráðstöfun upplýsinganna. Hann er jafnan sá sem hefur frumkvæði að vinnslu og ákveður að hún skuli fara fram. Í athugasemdum í greinargerð með frumvarpi því er varð að lögum nr. 77/2000 segir að átt sé við þann aðila sem hefur ákvörðunarvald um vinnslu persónuupplýsinga og að jafnvel þótt slíkur aðili feli öðrum meðferð upplýsinganna beri hann ábyrgðina, svo fremi hann hafi áfram ákvörðunarvaldið.

Vinnsluaðili er hins vegar sá sem vinnur persónuupplýsingar á vegum ábyrgðaraðila, sbr. 5. tölul. 2. gr. laga nr. 77/2000. Um samband ábyrgðaraðila og vinnsluaðila er nánar kveðið í 13. gr. laga nr. 77/2000, sbr. frekari umfjöllun neðar í kafla 4.3..

Persónuvernd telur að hver og einn grunnskóli sem notast við vefkerfið Mentor og skráir persónuupplýsingar um nemendur sína í vefkerfið sé *ábyrgðaraðili* þeirra persónuupplýsinga sem færðar eru í grunn Mentors, í skilningi 4. tölul. 2. gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga, sbr. einnig afstöðu stofnunarinnar í máli nr. 2011/1231.

Er framangreindur skilningur einnig í samræmi við ákvæði 9. gr. reglugerðar nr. 897/2009, um miðlun og meðferð upplýsinga um nemendur í grunnskólum og rétt foreldra til aðgangs að upplýsingum um börn sín, en þar segir að skólastjóri grunnskóla beri ábyrgð á meðferð og vörslu upplýsinga og að uppfylltar séu þær kröfur sem gerðar eru til ábyrgðaraðila samkvæmt lögum nr. 77/2000 og lögum nr. 66/1985 (nú lögum nr. 77/2014 um opinber skjalasöfn).

Aftur á móti telur Persónuvernd að Mentor ehf., sem hýsingar- og rekstraraðili vefkerfisins Mentor, sé *vinnsluaðili* sem vinni með persónuupplýsingarnar á vegum hvers ábyrgðaraðila, þ.e. hvers skóla sem notar vefkerfið Mentor. Ber því hverjum ábyrgðaraðila að ganga úr skugga um að gerður sé vinnslusamningur við vinnsluaðila, í þessu tilviki Mentor ehf., sbr. 13. gr. sömu laga og umfjöllun neðar í kafla 4.3.

2.
Lögmæti vinnslu
2.1.
Um notkun á vefkerfinu Mentor við skráningu persónuupplýsinga um nemendur

Samkvæmt ákvæði 2. mgr. 18. gr. laga nr. 91/2008 um grunnskóla skulu foreldrar veita grunnskóla upplýsingar um barn sitt sem nauðsynlegar eru fyrir skólastarfið og velferð barnsins. Við meðferð slíkra upplýsinga sem fylgt hafa barni úr leikskóla er krafist fullrar þagnarskyldu og málsmeðferðar í samræmi við ákvæði laga nr. 77/2000. Í ákvæðinu kemur jafnframt fram að gera skuli foreldrum grein fyrir þessum upplýsingum. Skal meðferð upplýsinga vera á hendi skólastjóra eða annarra sérfræðinga á vegum sveitarfélagsins samkvæmt nánari ákvörðun þess.

Á grundvelli framangreinds ákvæðis hefur mennta- og menningarmálaráðherra sett áðurnefnda reglugerð nr. 897/2009, um miðlun og meðferð upplýsinga um nemendur í grunnskólum og rétt foreldra til aðgangs að upplýsingum um börn sín. Árið 2011 var ákvæði bætt við reglugerðina, sbr. reglugerð nr. 657/2011, um skráningu upplýsinga og samskipti við foreldra. Í ákvæðinu segir:

Grunnskólum er heimilt að nota rafrænt upplýsingakerfi til skráningar og miðlunar upplýsinga um nemendur samkvæmt þessari reglugerð. Ennfremur getur skóli notað slíkt kerfi til þess að veita foreldrum aðgang að upplýsingum og til samskipta við þá. Komi fram rökstudd beiðni frá foreldrum um að aðgangur að upplýsingum verði jafnframt veittur með öðrum hætti, s.s. með tölvupósti, símleiðis eða bréfleiðis, skal starfsfólk skóla leitast við að verða við slíkum beiðnum, enda þjóni það hagsmunum og þörfum barnsins. Tillit skal tekið til eðlis og mikilvægis þeirra upplýsinga sem um ræðir hverju sinni og hvort sérþarfir barns eða sérstakar aðstæður kalli á að samskipti séu með tilteknum hætti.

Af framangreindu ákvæði leiðir að grunnskólum er heimilt að skrá persónuupplýsingar um nemendur í rafrænu upplýsingakerfi á borð við Mentor.

Aftur á móti hefur ekki verið fjallað um í lögum eða reglugerðum hvaða persónuupplýsingar megi skrá í slíkt kerfi, hve oft megi skrá slíkar upplýsingar, hvernig skuli skrá þær, hvernig haga skuli fræðslu til handa notendum vefkerfisins eða hvernig gæti eigi öryggis þeirra. Hvað varðar hin síðarnefndu atriði ber ábyrgðaraðili ábyrgð á að öðrum ákvæðum laga nr. 77/2000 sé fullnægt, einkum að því er varðar 7.-9. gr., 11.-13. gr. og 20.-21. gr. laganna, sbr. eftirfarandi umfjöllun.

2.2.
Lögmæti vinnslu persónuupplýsinga í vefkerfinu Mentor

Skilyrði laga nr. 77/2000

Til þess að vinnsla almennra persónuupplýsinga sé heimil verður ábyrgðaraðili að gæta þess að eitthvert af skilyrðum 8. gr. laga nr. 77/2000 sé uppfyllt.

Þegar stjórnvöld eða sveitarfélög vinna með persónuupplýsingar vegna lögbundins hlutverks síns verður einkum talið að 3. tölul. 1. mgr. 8. gr. laganna geti átt við en þar segir að vinnsla sé heimil sé hún nauðsynleg til að fullnægja lagaskyldu, en einnig geti átt við 6. tölul. sama ákvæðis, þar sem segir að vinnsla sé heimil sé hún nauðsynleg við beitingu opinbers valds sem ábyrgðaraðili fer með.

Ef um viðkvæmar persónuupplýsingar er að ræða þarf einnig að uppfylla eitthvert af skilyrðum 1. mgr. 9. gr. laga nr. 77/2000. Þá getur ákvæði 7. tölul. 1. mgr. 9. gr. laga nr. 77/2000 átt við, þess efnis að vinnsla persónuupplýsinga er heimil sé hún nauðsynleg til að gæta lögmætra hagsmuna nema grundvallarréttindi og frelsi hins skráða vegi þyngra.

Samkvæmt skilgreiningu c-liðar 8. tölul. 2. gr. laga nr. 77/2000 eru upplýsingar um heilsuhagi taldar vera viðkvæmar persónuupplýsingar. Af þeim skriflegu svörum sem Persónuvernd hefur fengið frá grunnskólunum, sem og viðtölum stofnunarinnar við starfsmenn skólanna, virðist liggja fyrir að í einhverjum tilvikum séu skráðar viðkvæmar persónuupplýsingar um nemendur í vefkerfið Mentor, t.d. um greiningar þeirra eða aðrar heilsufarsupplýsingar. Þarf vinnsla slíkra upplýsinga því bæði að eiga sér stoð í 8. og 9. gr. laganna.

Þar að auki þarf öll vinnsla persónuupplýsinga að fullnægja öllum grunnkröfum 1. mgr. 7. gr. laga nr. 77/2000, m.a. um að persónuupplýsingar séu unnar með sanngjörnum, málefnalegum og lögmætum hætti (1. tölul.) og að þær séu fengnar í yfirlýstum, skýrum og málefnalegum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi (2. tölul.), og að aðeins sé unnið með upplýsingar að því marki sem nauðsynlegt er miðað við tilgang vinnslunnar (3. tölul.).

Samkvæmt lögunum hvílir sú skylda á ábyrgðaraðila að tryggja öryggi þeirra persónuupplýsinga sem unnið er með, sbr. 11.–13. gr. laganna og reglur Persónuverndar nr. 299/2001 um öryggi persónuupplýsinga, sbr. frekari umfjöllun í kafla 4.

Skilyrði reglugerðar nr. 897/2009

Einnig er minnst á framangreindar kröfur laga nr. 77/2000 í áðurnefndri reglugerð nr. 897/2009. Þar segir meðal annars að óheimilt sé að miðla persónuupplýsingum um nemendur til annarra en þeirra sem þess þurfa vegna starfa sinna nema samkvæmt heimild í lögum eða fyrirmælum þeirrar reglugerðar. Einnig segir að málsmeðferð skuli að öðru leyti vera í samræmi við lög nr. 77/2000.

Þá segir sérstaklega í 7. gr. reglugerðarinnar að við meðferð og öflun persónuupplýsinga skuli þess gætt að þær séu unnar með sanngjörnum, málefnalegum og lögmætum hætti og að öll meðferð þeirra sé í samræmi við vandaða vinnsluhætti persónuupplýsinga skv. lögum nr. 77/2000 og lögum um Þjóðskjalasafn Íslands nr. 66/1985 (nú lögum nr. 77/2014 um opinber skjalasöfn).

Loks segir í reglugerðinni að þegar skólagöngu barns er lokið og ekki eru lengur fyrir hendi málefnalegar ástæður til varðveislu upplýsinga um það skuli sá aðili sem falin er meðferð og varsla upplýsinga, þ.e. héraðsskjalasafn og Þjóðskjalasafn Íslands, annast meðferð þeirra í samræmi við fyrirmæli laga um Þjóðskjalasafn Íslands (nú laga um opinber skjalasöfn) og fyrirmæli sett samkvæmt þeim.

Um skráningu persónuupplýsinga í Mentor

Fyrir liggur að enginn af skólunum hefur sett sér verklagsreglur skráningu persónuupplýsinga í Mentor, né heldur stefnu eða viðmið þar að lútandi. Þó bentu margir viðmælendur Persónuverndar á að fulltrúar frá Mentor ehf. hefðu stöku sinnum haldið kynningar um vefkerfið í skólunum og þá bent á að almennt ætti að gæta hófs við nafngreiningu nemenda í skráningum í dagbókarflipa kerfisins. Þá hefðu sumir stjórnendur bent nýjum starfsmönnum á framangreint og eftir atvikum önnur atriði tengd efnislegri skráningu þegar þeim var úthlutað aðgangi að vefkerfinu í fyrsta sinn. Engu að síður virtist ekki vera samræmi í svörum starfsmanna hjá sama skólanum varðandi slíkar ábendingar stjórnenda. Að undanskildum framangreindum stöku leiðbeiningum Mentor ehf. eða skólastjórnenda virðist skráning persónuupplýsinga í Mentor vera í flestum tilvikum háð persónulegu mati hvers kennara eða starfsmanns sem skráir þar inn upplýsingar um nemendur.

Af framangreindu leiðir að fjöldi skráninga um nemendur getur verið afar mismunandi milli einstakra kennara hjá sama skóla, en einnig geta þau verið mismunandi milli skóla. Einnig getur verið mismunandi milli aðila hvernig skráningu um nemanda er hagað, t.d. hvort þar eru skráðar viðkvæmar persónuupplýsingar um nemendur, hvort lýsing á atburðum er gildishlaðin eða byggð á persónulegu mati kennarans eða hvort hennar er yfirleitt þörf. Því kunna að vera uppi tilvik þar sem skráningu er hagað með mismunandi hætti milli skóla/einstakra starfsmanna enda þótt sömu aðstæður séu uppi um nemendur. Stafar framangreint einkum af því að enginn skóli eða skólastjórnandi hefur mótað sérstaka stefnu í þessum efnum eða viðhaft reglulegt eftirlit með efnislegri skráningu starfsmanna í Mentor.

Niðurstaða um lögmæti vinnslu persónuupplýsinga

Með vísun til alls framangreinds er það mat Persónuverndar að það kunni að teljast málefnalegt og í samræmi við ákvæði 1. mgr. 8. gr. laga nr. 77/2000 að skrá tilteknar persónuupplýsingar um nemendur í rafrænt upplýsingakerfi á borð við Mentor; til að mynda grunnupplýsingar um nemanda, þ.e. nafn, kennitölu, heimilisfang og tengiliðaupplýsingar um nánustu aðstandendur, einkunnir, fjarvistir, heimavinnu og almenna umfjöllun um atburði í skólanum.

Einnig telur Persónuvernd að það kunni að samrýmast reglugerð nr. 897/2009, lögum nr. 91/2008 um grunnskóla og 9. gr. laga nr. 77/2000 að skrá viðkvæmar persónuupplýsingar, t.d. um greiningar eða heilsufarsupplýsingar, um nemendur eða aðstandendur þeirra í rafræn upplýsingakerfi á borð við Mentor. Aftur á móti telur stofnunin að einungis sé unnt að skrá slíkar upplýsingar að öðrum skilyrðum laga nr. 77/2000 uppfylltum, einkum varðandi öryggi og gerð vinnslusamnings, sbr. frekari umfjöllun í kafla 4. Þar til uppfyllt verða slík skilyrði um öryggi upplýsinga telur

Persónuvernd að fremur eigi að skrá viðkvæmar persónuupplýsingar í sérstakar skrár sem ekki eru í Mentor eða sambærilegum rafrænum upplýsingakerfum, þar sem unnt er að gæta öryggis þeirra með fullnægjandi hætti í samræmi við ákvæði 11. gr. laga nr. 77/2000, sbr. umfjöllun neðar í kafla 4.

Jafnframt er það mat Persónuverndar að enda þótt heimilt kunni að vera að skrá almennar persónuupplýsingar um nemendur í Mentor á grundvelli 8. gr. laga nr. 77/2000 verði engu að síður að haga slíkri skráningu í samræmi við ákvæði 7. gr. laga nr. 77/2000, sbr. einnig 7. gr. reglugerðar nr. 897/2009. Nánar tiltekið ber að gæta að því að skráningar séu málefnalegar, sanngjarnar og í samræmi við vandaða vinnsluhætti persónuupplýsinga. Einnig verða þær að vera nægilegar, viðeigandi og ekki umfram það sem nauðsynlegt er miðað við tilgang vinnslunnar. Varðandi skráningu persónuupplýsinga í Mentor telur Persónuvernd að mikilvægt sé að hafa skráningar málefnalegar og viðeigandi, einkum í ljósi þess að allar upplýsingar úr Mentor munu varðveitast hjá opinberu skjalasafni í marga áratugi, sbr. frekari umfjöllun í kafla 2.3.

Þá má ráða af ákvæði 9. gr. reglugerðar nr. 897/2009 að það falli í hlut skólastjóra viðkomandi grunnskóla að hafa eftirlit með framangreindu. Þar sem enginn af skólastjórnendum skólanna sem Persónuvernd heimsótti viðhefur reglulegt eftirlit með efnislegum skráningum starfsmanna í Mentor er ekki unnt að slá því föstu hvort þær skráningar sem þegar hafa verið gerðar í vefkerfið séu í samræmi við framangreind ákvæði. Telur Persónuvernd þetta ámælisvert. Einnig telur Persónuvernd að skortur á slíkri stefnumótun og eftirliti af hálfu skólastjórnenda geti valdið ósamræmi á skráningu persónuupplýsinga milli kennara og nemenda þeirra, sem þar af leiðandi dregur úr áreiðanleika upplýsinganna.

2.3.
Varðveisla gagna í Mentor

Ábyrgðaraðila ber að eyða persónuupplýsingum þegar ekki er lengur málefnaleg ástæða til að varðveita þær, sbr. ákvæði 1. mgr. 26. gr. laga nr. 77/2000. Málefnaleg ástæða til varðveislu upplýsinga getur m.a. byggst á fyrirmælum í lögum.

Í ljósi áðurnefndra ákvæða 5. tölul. 7. gr. og 1. mgr. 26. gr. laga nr. 77/2000 er það lagt í hendur ábyrgðaraðila að meta hvenær ekki er lengur málefnaleg ástæða til að varðveita upplýsingar. Aftur á móti hvíla auknar skyldur á stjórnvöldum og sveitarfélögum um varðveislu gagna sem þau fá í hendur, á grundvelli laga nr. 77/2014 um opinber skjalasöfn.

Samkvæmt 14. gr. laga nr. 77/2014 er afhendingarskyldum aðilum gert skylt að afhenda opinberu skjalasafni skjöl sín í samræmi við ákvæði laganna. Þá segir í 24. gr. laganna að afhendingarskyldum aðilum sé óheimilt að ónýta eða farga nokkru skjali í skjalasöfnum sínum nema það sé gert á grundvelli samþykktar þjóðskjalavarðar, reglna Þjóðskjalasafns Íslands skv. 23. gr. eða 2. mgr. 24. gr. laga nr. 77/2014, eða á grundvelli sérstaks lagaákvæðis.

Er framangreint loks áréttað í 26. gr. upplýsingalaga nr. 140/2012, þar sem segir að um skráningu mála, skjalaskrár og aðra vistun gagna og upplýsinga fari að ákvæðum laga um Þjóðskjalasafn Íslands.

Af framangreindum ákvæðum virðist því liggja fyrir að allar upplýsingar sem hafa verið skráðar í Mentor um nemendur verða afhentar opinberu skjalasafni til varanlegrar varðveislu. Jafnframt verður þeim upplýsingum ekki fargað nema samkvæmt heimild í lögum eða á grundvelli ákvörðunar Þjóðskjalasafns Íslands.

Þótt það falli í hlut Þjóðskjalasafns Íslands, en ekki Persónuverndar, að túlka skilyrði laga nr. 77/2014 um opinber skjalasöfn, telur Persónuvernd engu að síður mikilvægt að ábyrgðaraðilar vinnslu persónuupplýsinga í Mentor hafi framangreind lagaákvæði í huga þegar skráðar eru persónuupplýsingar í vefkerfið og þegar útbúinn er vinnslusamningur við vinnsluaðila. Ber ábyrgðaraðili meðal annars að gæta að því við gerð vinnslusamnings að þau fyrirmæli sem hann veitir vinnsluaðila um varðveislu gagna séu í samræmi við skyldur hans skv. lögum nr. 77/2014.

3.
Fræðsla

Samkvæmt áðurnefndu ákvæði 7. gr. laga nr. 77/2000 ber meðal annars að gæta að því að persónuupplýsingar séu unnar með sanngjörnum, málefnalegum og lögmætum hætti, og að meðferð þeirra sé í samræmi við vandaða vinnsluhætti persónuupplýsinga, sem og að þær séu áreiðanlegar og uppfærðar eftir þörfum.

Þá ber ábyrgðaraðili vinnslu einnig að veita hinum skráða, eða eftir atvikum foreldri hins skráða (ef hinn skráði er ólögráða), fræðslu um tiltekna þætti tengda vinnslunni, skv. ákvæðum 20. og 21. gr. sömu laga.

Til að mynda ber að upplýsa hinn skráða um ýmis atriði þegar persónuupplýsinga er aflað hjá honum, meðal annars um tilgang vinnslunnar og aðrar upplýsingar að því marki sem þær eru nauðsynlegar, með hliðsjón af þeim sérstöku aðstæðum sem ríkja við vinnsluna, svo að hinn skráði geti gætt hagsmuna sinna, sbr. ákvæði 20. gr. laganna.

Þá hefur hinn skráði jafnframt rétt á því að ábyrgðaraðili leiðrétti, eyði eða bæti við persónuupplýsingar sem eru rangar, villandi eða ófullkomnar eða hafa verið skráðar án tilskilinnar heimildar, skv. 1. mgr. 25. gr. laga nr. 77/2000. Sé eyðing eða breyting þeirra upplýsinga óheimil skv. ákvæðum annarra laga getur Persónuvernd bannað notkun þeirra.

Niðurstaða um fræðslu til handa notendum vefkerfisins Mentor

Í því tilviki sem hér er til skoðunar telur Persónuvernd að framangreint geti átt við um alla notendur Mentor, þ. á m. starfsmenn grunnskóla, foreldra nemenda, nemendur eða önnur skyldmenni þess sem hafa fengið úthlutaðan aðgang að Mentor hjá sínum skóla. Til að mynda ætti að fræða foreldra nemenda sérstaklega um það að færslur um börn þeirra kunni að vera skráðar í Mentor sem hafa ekki verið birtar þeim sérstaklega. Þá gæti einnig skipt máli fyrir starfsmenn grunnskóla að vita að allar upplýsingar sem skráðar eru í Mentor verða afhentar opinberu skjalasafni til varðveislu í tugi ára, sbr. frekari umfjöllun í kafla 2.3., enda gæti slík vitneskja eftir atvikum komið í veg fyrir ómálefnalegar eða óviðeigandi skráningar í Mentor.

Í ljósi framangreinds telur Persónuvernd mikilvægt að skólastjórnendur beiti sér fyrir því að veita notendum kerfisins fræðslu sem þeir kunna á að halda varðandi skráningar um nemendur og aðgang að upplýsingunum um þá. Með þeim hætti verða skráningar í Mentor gagnsæjar gagnvart öllum notendum.

4.
Öryggi persónuupplýsinga
4.1.
Almennt um reglur um upplýsingaöryggi

Samkvæmt lögum nr. 77/2000 hvílir sú skylda á ábyrgðaraðila að tryggja öryggi þeirra persónuupplýsinga sem unnið er með, sbr. 11.–13. gr. laganna og reglur Persónuverndar nr. 299/2001 um öryggi persónuupplýsinga.

Í 11. gr. laganna er fjallað um *öryggisráðstafanir* o.fl. Skal ábyrgðaraðili gera viðeigandi tæknilegar og skipulagslegar öryggisráðstafanir til að vernda persónuupplýsingar gegn ólöglegri eyðileggingu, gegn því að þær glatist eða breytist fyrir slysni og gegn óleyfilegum aðgangi, sbr. 1. mgr. 11. gr. laganna. Beita skal ráðstöfunum sem tryggja nægilegt öryggi miðað við áhættu af vinnslunni og eðli þeirra gagna sem verja á, með hliðsjón af nýjustu tækni og kostnaði við framkvæmd þeirra, sbr. 2. mgr. ákvæðisins.

Ábyrgðaraðili ber ábyrgð á því að *áhættumat* og öryggisráðstafanir séu í samræmi við lög, reglur og fyrirmæli Persónuverndar, þ.m.t. þá staðla sem hún ákveður að skuli fylgt, sbr. 3. mgr. 11. gr. laga nr. 77/2000. Ábyrgðaraðili ber og ábyrgð á því að áhættumat sé endurskoðað reglulega og öryggisráðstafanir endurbættar að því marki sem þörf krefur til að uppfylla ákvæði þessarar greinar, sbr. 4. mgr. 11. gr. laganna.

Þá skal ábyrgðaraðili skrá með hvaða hætti hann mótar *öryggisstefnu,* gerir *áhættumat* og *ákveður öryggisráðstafanir,* sbr. 5. mgr. 11. gr. laga nr. 77/2000, sbr. nánar 1. mgr. 3. gr. reglna nr. 299/2001. Í öryggisstefnu er að finna almenna lýsingu á helstu kröfum og áherslum varðandi upplýsingaöryggi; í áhættumati eru greindar þær ógnir sem steðja að vinnslu persónuupplýsinga; og í skráningu öryggisráðstafana eru slíkar ráðstafanir skjalfestar á grundvelli þeirra forsendna sem fram koma í áhættumati.

Samkvæmt 12. gr. laga nr. 77/2000 skal ábyrgðaraðili viðhafa *innra eftirlit* með vinnslu persónuupplýsinga til að ganga úr skugga um að unnið sé í samræmi við gildandi reglur og þær öryggisráðstafanir sem ákveðnar hafa verið.

4.2.
Niðurstaða um upplýsingaöryggi

Samkvæmt reglum nr. 299/2001 skal ábyrgðaraðili útbúa öryggiskerfi og byggja það á skriflegri *öryggisstefnu* og skriflegu *áhættumati*. Á grundvelli áhættumats skal ákveða nauðsynlegar *öryggisráðstafanir.* Í skriflegum svörum grunnskólanna kemur fram að enginn þeirra hefur útbúið áðurnefnd skjöl sem reglur nr. 299/2001 gera ráð fyrir að séu til staðar.

Í III. kafla reglna nr. 299/2001, nánar tiltekið í ákvæðum 4.-7. gr., eru tilgreindar öryggisráðstafanir sem ábyrgðaraðili ætti að grípa til eftir því sem á við hverju sinni. Þá er einnig vikið að kröfum um innra öryggi í IV. kafla þeirra reglna, þ.e. í ákvæði 8. gr. Sá hluti þessa álits sem lýtur að upplýsingaöryggi mun því afmarkast við áðurnefnd ákvæði reglnanna.

Þagnarskylduyfirlýsingar

Í 2. tölul. 5. gr. reglna nr. 299/2001 kemur fram að ábyrgðaraðili skuli, eftir því sem við á, fá skjalfestar þagnarskylduyfirlýsingar frá starfsmönnum í þeim tilgangi að fyrirbyggja og takmarka tjón af völdum mannlegra mistaka eða annarrar misnotkunar. Af starfi starfsmanna grunnskóla verður ráðið að þeir vinna með meðal annars viðkvæmar persónuupplýsingar í starfi sínu og verði því að gera þá kröfu á hendur ábyrgðaraðila, sem í þessu tilviki eru skólastjórnendur, að starfsmenn undirriti áðurnefndar þagnarskylduyfirlýsingar. Fæstir skólanna öfluðu þagnarskylduyfirlýsinga og enginn skólastjórnendanna gat fullyrt að slíkar yfirlýsingar væru til fyrir alla starfsmenn skólanna.

Aðgangsstýringar

Þá kemur fram í 4. tölul. 5. gr. reglna nr. 299/2001 að ábyrgðaraðili skuli, eftir því sem við á, gera nauðsynlegar ráðstafanir til þess að starfsmönnum sé með reglubundnum hætti gerð grein fyrir starfsskyldum sínum og þeim afleiðingum sem það hefur í för með sér að brjóta þær. Í vettvangsathugununum kom fram að starfsmenn ræddu um meðferð persónuupplýsinga í Mentor á kennarafundum og sama ætti hugsanlega við um öryggismál en aðeins í

takmörkuðum mæli. Af svörum viðmælenda í vettvangsathugun verður ekki ráðið að slík fræðsla hafi farið fram með skipulegum og reglubundnum hætti.

Í 1. tölul. 7. gr. reglna nr. 299/2001 kemur fram að ábyrgðaraðila ber, eftir því sem við á, að stýra aðgangi að búnaði með úthlutun aðgangs- og lykilorða. Af svörum grunnskólanna verður ráðið að notendanafn í Mentor er kennitala viðkomandi starfsmanns. Þá kom fram í viðtölum við kennara að notandi geti haft fleiri en einn notendareikning á sama aðgangsnafni og stýrir þá lykilorð því hvaða reikningi viðkomandi tengist. Af þessu má leiða að notkun kennitölu sem notendanafn geti skert öryggi í aðgangsstýringum. Þá kom fram að þegar starfsmönnum er úthlutaður aðgangur að Mentor sé lykilorði úthlutað af skólastjórnendum. Oft sé sama lykilorð notað og af þeim svörum sem fengust við vettvangskönnun virðist mega ráða að vefkerfi Mentor geri ekki kröfu um að lykilorði sé breytt við fyrstu innskráningu. Mentor geri heldur ekki kröfu um styrk lykilorða eða um að þeim sé breytt með reglubundnum hætti.

Með vísun til alls framangreinds verður ráðið að öryggi aðgangsheimilda, svo sem styrkur lykilorða og endurnýjun þeirra með reglubundnum hætti, sé verulega ábótavant.

Aðgerðarskráning

Þá kemur fram í 3. tölul. 7. gr. reglna nr. 299/2001 að ábyrgðaraðili skuli gera ráðstafanir til að tryggja rekjanleika uppflettinga og vinnsluaðgerða, ef við á. Í viðtölum við skólastjórnendur kom fram að þeir væru fæstir meðvitaðir um aðgerðaskráningu sem fram fer í Mentor. Af því leiðir að starfsmenn hafa ekki fengið fræðslu um þær aðgerðarskráningar sem fram fara samhliða notkun kerfisins. Þá virðist vera óljóst hvort og þá hvernig upplýsingar úr aðgerðaskrá séu nýttar.

Innra eftirlit

Samkvæmt 8. gr. í IV. kafla sömu reglna skal ábyrgðaraðili viðhafa innra eftirlit með vinnslu persónuupplýsinga til að ganga úr skugga um að unnið sé í samræmi við gildandi lög og reglur. Skal innra eftirlit meðal annars beinast að athugun á því hvort vinnsla sé heimil skv. lögum nr. 77/2000 (1. tölul.), hvort uppfylltar séu reglur 7. gr. laganna um lögmæti vinnslu (3. tölul.), hvort virt séu í framkvæmd ákvæði um rétt hins skráða samkvæmt lögunum (4. tölul.), hvort fylgt sé þeim öryggisráðstöfunum sem valdar hafi verið skv. c-lið 1. mgr. 3. gr. og III. kafla reglnanna (5. tölul.). Þá segir einnig að innra eftirlit skuli viðhaft með reglubundnum hætti. Tíðni eftirlitsins og umfang þess skuli ákveðið með hliðsjón af áhættunni sem er samfara vinnslunni, eðli þeirra gagna sem unnið er með, þeirri tækni sem notuð er til að tryggja öryggi upplýsinganna og kostnaði af eftirlitinu. Það skuli þó eigi fara fram sjaldnar en árlega. Skal ábyrgðaraðili sjá til þess að gerð sé skýrsla um hverja aðgerð sem er liður í innra eftirliti.

Af viðtölum við skólastjórnendur skólanna mátti ráða að enginn þeirra viðhafi innra eftirlit með reglubundnum hætti um þau atriði sem að framan greinir.

4.3.
Lögmæti afhendingu persónuupplýsinga til vinnsluaðila, Mentor ehf.

Skilyrði laga nr. 77/2000

Í 8. gr. laga nr. 77/2000 eru almennar reglur um heimildir fyrir vinnslu persónuupplýsinga, eins og áður segir. Er vinnsla persónuupplýsinga heimil ef einhverjir þeirra þátta sem þar eru taldir upp eru fyrir hendi. Það á m.a. við um miðlun persónuupplýsinga til þriðja aðila og er hún heimil ef eitthvert af skilyrðum 1. mgr. 8. gr. er uppfyllt. Samkvæmt almennum sönnunarreglum hvílir sönnunarbyrði um það hvort svo sé á ábyrgðaraðila, í þessu tilviki grunnskólunum.

Í þessu máli er ljóst að skólarnir hafa keypt aðgang að vefkerfinu Mentor hjá Mentor ehf. og að hið síðarnefnda félag er hýsingar- og rekstraraðili þess kerfis. Þar sem starfsmenn skólanna skrá persónuupplýsingar um nemendur, og eftir atvikum aðra einstaklinga, í vefkerfið verður að telja að með slíkri aðgerð eigi sér stað miðlun persónuupplýsinga til þriðja aðila, þ.e. Mentor ehf.

Hafa grunnskólarnir hins vegar ekki haldið því fram að hér hafi verið um að ræða miðlun persónuupplýsinga til þriðja aðila, heldur afhendingu til vinnsluaðila. Kemur þá til skoðunar hvort uppfyllt hafi verið þau skilyrði sem gilda um slíka afhendingu.

Almennt er ekki gerð sú krafa að afhending til vinnsluaðila uppfylli skilyrði 1. mgr. 8. gr. laga nr. 77/2000 með sama hætti og þegar um er að ræða miðlun til þriðja aðila. Hins vegar þarf þá að uppfylla skilyrði ákvæðis 13. gr. laganna.

Í 13. gr. laganna kemur fram að ábyrgðaraðila sé heimilt að semja við tiltekinn aðila um að annast, í heild eða að hluta, þá vinnslu persónuupplýsinga sem hann ber ábyrgð á samkvæmt ákvæðum laga nr. 77/2000. Slíkt er í fyrsta lagi háð því að ábyrgðaraðili hafi áður sannreynt að umræddur vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit. Það er í öðru lagi háð því að hann hafi gefið honum fyrirmæli um vinnslu í samræmi við 3. mgr. 13. gr. laga nr. 77/2000 og að þau fyrirmæli komi fram í samningi. Í samningnum skal koma fram að vinnsluaðila sé einungis heimilt að starfa í samræmi við fyrirmæli ábyrgðaraðila. Ákvæði laga nr. 77/2000 um skyldur ábyrgðaraðila gilda einnig um þá vinnslu sem vinnsluaðili annast, sbr. 2. mgr. sama ákvæðis. Slíkur samningur skal vera skriflegur og a.m.k. í tveimur eintökum.

Varðandi samninga skólanna við Mentor ehf.

Um framangreint hafa skólarnir allir vísað til svokallaðs „nytjaleyfis- og þjónustusamnings“ milli hvers skóla og Mentor ehf. Samkvæmt þeim samningi er Mentor ehf. sagður vinnsluaðili vinnslu, en viðkomandi skóli ábyrgðaraðili, og að notandi framkvæmi vinnslu. Að öðru leyti fjallar samningurinn um leyfi þjónustukaupa, þ.e. hvers grunnskóla, til að nota hugbúnaðinn, höfundaréttindi vegna hugbúnaðarins, virkni og takmörkun ábyrgðar þjónustusala, þjónustugjöld, trúnað, gildistíma samnings og varnarþing. Að því er varðar öryggi persónuupplýsinga og meðferð þeirra segir meðal annars í samningnum að þjónustusali, þ.e. Mentor ehf., skuldbindi sig til að gæta fyllsta trúnaðar um hvaðeina sem hann verður áskynja um við framkvæmd samningsins, að hann tryggi að afrit trúnaðarupplýsinga og annarra mikilvægra gagna séu tryggilega geymd og ekki afhent öðrum en þjónustukaupa, að þjónustukaupi beri ábyrgð á að vinnsla samrýmist 7. gr. laga nr. 77/2000 og að gögn þjónustukaupa séu eign hans.

Niðurstaða um lögmæti afhendingar persónuupplýsinga til Mentor ehf.

Að mati Persónuverndar fullnægir framangreindur samningur, sem er efnislega samhljóða hjá öllum skólunum, ekki skilyrðum 13. gr. laga nr. 77/2000 um gerð og efni vinnslusamnings. Byggir sú afstaða einkum á því að enginn skólanna kom að gerð samningsins, enginn skólanna sannreyndi *fyrir* undirritun samningsins að Mentor ehf. gæti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit skv. 12. gr. sömu laga, sbr. einnig umfjöllun neðar í kafla 4. Til viðbótar framangreindum atriðum gaf enginn skólanna fyrirmæli til handa Mentor ehf. í samningunum um meðferð þeirra persónuupplýsinga sem safnast í vefkerfinu, t.d. varðandi varðveislu eða eyðingu þeirra.

Í ljósi framangreinds verður afhending umræddra persónuupplýsinga til Mentor ehf. í gegnum vefkerfið Mentor ekki talin samrýmast ákvæðum laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga.

5.
Samantekt

Af öllu ofangreindu má ráða að einungis er mælt fyrir um það í lögum og reglugerðum að unnt sé að skrá persónuupplýsingar um nemendur grunnskóla í rafrænt upplýsingakerfi. Þá segir einnig í reglugerð hver beri ábyrgð á meðferð slíkra upplýsinga og að þær verði að vera í samræmi lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga. Hefur ekki verið sérstaklega fjallað um í lögum eða reglugerðum hvað eigi að skrá, í hvaða tilvikum, hverjum skuli birta færslur, hvernig haga skuli fræðslu til handa notendum eða hvernig öryggis skuli gætt við notkun slíkra kerfa.

Er það mat Persónuverndar að skráning persónuupplýsinga um nemendur geti verið talin heimil í rafrænu upplýsingakerfi á borð við Mentor. Aftur á móti er það mat stofnunarinnar að ekki sé málefnalegt eða lögmætt að skrá viðkvæmar persónuupplýsingar í slík kerfi, nema uppfylltar séu kröfur laga nr. 77/2000, einkum um öryggi persónuupplýsinga og gerð vinnslusamnings. Verður að ætla að eftir atvikum eigi skráning slíkra upplýsinga fremur heima í upplýsingakerfum þar sem sérstaks öryggis er gætt, eftir atvikum hjá sérfræðiþjónustu í samræmi við lög nr. 91/2008 um grunnskóla.

Þá verður skráning persónuupplýsinga í Mentor að vera í samræmi við ákvæði 7. gr. laga nr. 77/2000 og 7. gr. reglugerðar nr. 897/2009. Telur Persónuvernd það ámælisvert að ekkert eftirlit hafi farið fram hjá grunnskólunum varðandi það hvort skráningar hafi verið í samræmi við skilyrði þessara ákvæða.

Telur Persónuvernd það einnig liggja ljóst fyrir að sá vinnslusamningur sem Mentor ehf. hefur útbúið og látið kaupendur vefkerfisins skrifa undir, þ.e. grunnskólana, sé ekki fullnægjandi með tilliti til ákvæðis 13. gr. laga nr. 77/2000. Er því afhending persónuupplýsinga frá grunnskólunum til félagsins í gegnum vefkerfið ekki í samræmi við ákvæði laga nr. 77/2000.

Loks liggur fyrir að enginn þeirra ábyrgðaraðila sem athugun Persónuverndar náði til hafði útbúið gögn um öryggisstefnu, áhættumat, öryggisráðstafanir eða fyrirkomulag við innra eftirlit varðandi öryggi persónuupplýsinga, sem þeir bera ábyrgð á, líkt og skylt er að gera skv. 11. gr. laga nr. 77/2000 og reglum nr. 299/2001 um öryggi persónuupplýsinga. Telur Persónuvernd það ámælisvert þar sem um er að ræða stofnanir á vegum sveitarfélaga sem vinna daglega með mikið magn persónuupplýsinga, einkum um ólögráða einstaklinga.

6.
Tilmæli til ábyrgðaraðila

Í fyrsta lagi beinir Persónuvernd þeim tilmælum til ábyrgðaraðila að skrá ekki viðkvæmar persónuupplýsingar í Mentor, nema það verði útbúið sérstakt umhverfi fyrir slíka skráningu sem fullnægir framangreindum kröfum Persónuverndar.

Í öðru lagi er þeim tilmælum beint til ábyrgðaraðila að haga að öðru leyti vinnslu persónuupplýsinga í Mentor í samræmi við ákvæði 7. gr. laga nr. 77/2000, sbr. 7. gr. reglugerðar nr. 897/2009.

Í þriðja lagi ber ábyrgðaraðilum að gæta að lögmæti þeirra upplýsinga sem eru skráðar í kerfið, m.a. með því að setja sér verklagsreglur þar sem fjallað er um hvenær megi skrá upplýsingar um nemendur í Mentor (einkum í dagbókarflipa), hvað megi skrá um nemendur, hverjum eigi að birta færslur sem skráðar eru í dagbókarflipa og hvernig fræða beri notendur (einkum foreldra nemenda og kennara) um notkun kerfisins og færslur sem þar eru skráðar. Þá ber einnig að fjalla um það í verklagsreglum hvernig eftirliti skuli háttað með framangreindu hjá ábyrgðaraðila.

Í fjórða lagi er þeim tilmælum beint til ábyrgðaraðila að útbúa öryggisstefnu, áhættumat og öryggisráðstafanir, og lýsingu á fyrirkomulagi innra eftirlits í samræmi við ákvæði 11. gr. laga nr. 77/2000 og reglur nr. 299/2001 um öryggi persónuupplýsinga. Við gerð slíkra öryggisráðstafana mælist Persónuvernd til þess að hugað verði sérstaklega að eftirfarandi atriðum;

1. Undirritun þagnarskylduyfirlýsinga.
2. Reglubundinni fræðslu til handa starfsmönnum þar sem þeim er gerð grein fyrir starfsskyldum sínum og afleiðingum þess að brjóta þær. Halda skal skrá um þessa fræðslu, sem sýnir hvenær fræðsla fór fram, um hvað var fjallað og hverjir fengu fræðslu.
3. Notkun kennitölu sem notendanafn í Mentor verði hætt.
4. Gerð verði krafa um að lykilorði notanda sé breytt við fyrstu innskráningu og það fullnægi skilyrðum til að teljast sterkt.
5. Öryggisráðstöfunum tengdum fjaraðgangi starfsmanna að Mentor.
6. Upplýsingagjöf til handa starfsmönnum um skráningu aðgerða í Mentor og að settar verði reglur um notkun upplýsinga úr aðgerðaskrá.

Í fimmta og síðasta lagi ber ábyrgðaraðilum að semja við vinnsluaðila í samræmi við ákvæði 13. gr. laga nr. 77/2000, sem felur m.a. í sér að sannreyna hvort vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit áður en samið er við vinnsluaðilann. Í því ljósi vill Persónuvernd benda á að þrátt fyrir að ábyrgðaraðili, þ.e. hver grunnskóli, beri ábyrgð á að framangreind skilyrði laga nr. 77/2000 séu uppfyllt ber engu að síður að líta svo á, í ljósi sveitarstjórnarlaga nr. 138/2011 og almennra meginreglna um hvernig sveitarfélög eru starfrækt, að sveitarfélag geti komið fram fyrir hönd ábyrgðaraðila í sínu sveitarfélagi og útbúið sameiginleg fyrirmæli til handa vinnsluaðila, t.d. með gerð verklagsreglna sem gilda fyrir grunnskóla í viðkomandi sveitarfélagi. Lýsir Persónuvernd sig reiðubúna til að veita álit um efni slíkra reglna við undirbúning þeirra.

Ber ábyrgðaraðilum að senda Persónuvernd afrit af framangreindum skjölum eigi síðar en 1. apríl 2016. Þá ber jafnframt að senda Persónuvernd fyrir sama dag skriflega lýsingu á því hvernig eftirliti verði háttað hjá ábyrgðaraðilum framvegis svo að skráningar í Mentor samrýmist ákvæðum laga nr. 77/2000 og reglugerð nr. 897/2009.

Í ljósi framangreinds telur Persónuvernd að ákjósanlegt kunni að vera að setja almenn viðmið um framangreind atriði í reglugerð nr. 897/2009, í ljósi viðfangsefnis þeirrar reglugerðar. Gætu slík viðmið tekið til allra rafrænna upplýsingakerfa á borð við Mentor, enda er ljóst að nánast allir grunnskólar landsins nota Mentor eða önnur sambærileg rafræn upplýsingakerfi á grundvelli heimildar í áðurnefndri reglugerð. Telur Persónuvernd að sú leið gæti verið skilvirkust til að tryggja gagnsæi við skráningu persónuupplýsinga og samræmi milli skóla, enda ættu þá sömu viðmið við um alla grunnskóla, en ekki bara þá grunnskóla sem valdir voru af handahófi til athugunar hjá Persónuvernd í þetta sinn. Gætu mögulegar breytingar á reglugerð til að mynda fjallað um gerð vinnslusamnings, hvaða upplýsingar megi skrá í vefkerfið og hvenær, hvernig fræðslu skuli háttað til þeirra sem nota kerfið, og hvernig tryggja skuli öryggi þeirra gagna. Lýsir Persónuvernd sig reiðubúna til að koma að slíkri samvinnu við hlutaðeigandi aðila, sé þess óskað, svo unnt verði að ná framangreindum markmiðum með markvissum og skjótum hætti.

Loks er vakin athygli á því að afrit af áliti þessu verður sent mennta- og menningarmála-ráðuneytinu, Mentor ehf. og Sambandi íslenskra sveitarfélaga til upplýsinga.

Álitsorð:

Vinnsla persónuupplýsinga í Mentor hjá [A-skóla], [B-skóla], [C-skóla], [D-skóla], [E-skóla] er ekki í samræmi við lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga og reglur nr. 299/2001 um öryggi persónuupplýsinga. Beinir Persónuvernd sérstökum tilmælum til skólanna um úrbætur sem tengjast vinnslu persónuupplýsinga í Mentor og öryggi þeirra. Ber skólunum að senda Persónuvernd afrit af skjölum þess efnis eigi síðar en 1. apríl 2016.