

**Starfshópur um skoðun á skráningum upplýsinga um
nemendur grunnskóla í rafræn upplýsingakerfi í tengslum
við álit Persónuverndar í máli nr. 2015/1203.**

Nóvember 2016

I.

Hinn 3. nóvember 2015 var í kjölfar álits Persónuverndar í máli nr. 2015/1203, stofnaður starfshópur um skoðun á skráningum upplýsinga um nemendur grunnskóla í rafræn upplýsingakerfi.

Starfshópurinn hefur síðustu mánuði unnið að tillögum að lausnum í samræmi við framangreint álit, m.a. í samstarfi við Persónuvernd. Þá hefur mennta- og menningarmálaráðuneytið verið upplýst um framvindu málsins við meðferð þess. Með afhendingu meðfylgjandi skjala og upplýsinga tilkynnist hlutaðeigandi að starfshópurinn hefur nú lokið störfum sínum.

II.

Hlutverk starfshópsins var að fara yfir álit Persónuverndar frá 25. september 2015 varðandi vinnslu persónuupplýsinga og öryggi þeirra í vefkerfinu Mentor, samræma viðbrögð við áliti Persónuverndar, greina þætti sem þurfti að bæta, leggja til breytingar á framkvæmd þegar við átti, stuðla að því að gerðar yrðu breytingar á reglum ef þörf væri á og taka þátt í samstarfi með öllum aðilum sem sýsla með persónuupplýsingar nemenda í grunnskólum og að sú meðferð sé í samræmi við lög.

Helstu verkefni starfshópsins voru að:

- ✓ Greina álit Persónuverndar nr. 2015/1203 og þá þætti sem grunnskólar sveitarfélaganna þyrftu að bæta
- ✓ Leggja til breytingar á framkvæmd skráningar og gerð leiðbeininga fyrir grunnskólanna
- ✓ Stuðla að því að gerðar yrðu breytingar á reglum ef þörf væri á
- ✓ Samræma viðbrögð grunnskólanna við áliti Persónuverndar
- ✓ Leggja til úrbætur sem tryggja að meðferð persónuupplýsinga nemenda verði í samræmi við lög.

Í starfshópnum sátu Guðrún Sigtryggsdóttir, yfirlögfræðingur á skóla- og frístundasviði Reykjavíkurborgar, sem er formaður hópsins, Flosi H. Kristjánsson, verkefnastjóri á fagskrifstofu grunnskóla í Reykjavík þar til í júlí 2016 en þá tók Þorbjörg St. Þorsteinsdóttir sæti hans, Ásgeir Beinteinsson skólastjóri Háteigsskóla til 1. júlí 2016 og Vigdís Häsler, lögfræðingur á lögfræði- og velferðarsviði Sambands Íslenskra sveitarfélaga. Starfshópurinn hefur einnig notið fulltingis og aðstoðar upplýsingatæknideildar Reykjavíkurborgar.

Á starfstíma átti starfshópurinn fjölmarga fundi um málið auk þess sem fundað var með fulltrúum Mentor, Persónuvernd og mennta- og menningarmálaráðuneytinu. Þá var gerð könnun meðal skólastjóra um notkun rafrænna upplýsingakerfa.

III.

Starfshópurinn telur nauðsynlegt að gerðar verði úrbætur á reglugerð nr. 897/2009 um miðlun og meðferð upplýsinga um nemendur í grunnskólum og rétt foreldra til aðgangs að upplýsingum um börn sín. Setja þarf fram skýrari og nánari reglur um meðferð persónuupplýsinga nemenda og er mikilvægt að tekin verði skýr samræmd afstaða til mikilvægra þátta líkt og hvort skrá skuli viðkvæmar persónuupplýsingar í rafræn upplýsingakerfi. Vísað er til þess að mennta- og menningarmálaráðuneytið hefur í bréfi, dags. 27. september 2016 lýst skoðunum ráðuneytisins á ýmsum þáttum er snúa að álitaefninu, þ.e. að skoðað verði sérstaklega hvort rétt sé og nauðsynlegt að skrá með rafrænum hætti viðkvæmar persónuupplýsingar um nemendur í Mentor, goldinn er varhugur við svokölluðum fjaraðgangi að Mentor, þ.e. að engar skráningar skuli fram hjá starfsmanni utan starfsstöðvar. Þá er lýst þeirri skoðun að ávallt skuli birta foreldrum allar upplýsingar í Mentor sem skráðar eru af starfsfólki skóla. Þá sé einnig þörf á viðmiðum um viðfangsefni álits Persónuverndar og að rétt kunni að vera að ráðuneytið gangi lengra í leiðsögn sinni til grunnskóla, til að mynda með gerð og útgáfu handbókar til grunnskólanna, ekki síst með

tilliti til nýrrar löggjafar um persónuvernd. Áhersla er lögð á að mikilvægt er að ráðuneytið hraði framangreindri vinnu.

Á árinu 2018 er áætlað að ný persónuverndarlöggjöf taki gildi á Íslandi þegar ný reglugerð Evrópusambandsins um persónuvernd leysir af hólmi núgildandi Evrópulöggjöf. Allir sem vinna með persónuupplýsingar ættu að hefja undirbúning vegna gildistöku laganna nú þegar. Til að auðvelda innleiðingu nýju löggjafarinnar er mikilvægt að farið sé eftir þeim kröfum sem eru í gildandi persónuverndarlögum nr. 77/2000. Mikilvægt er að fyrir hendi séu góðar verklagsreglur og leiðbeiningar sem þjóna tilgangi sínum og sem starfsmenn þekkja. Þá er mikilvægt að grunnskólarnir hafi yfirsýn yfir hvaða upplýsingar það eru sem verið er að vinna með, hvaðan þær koma og á hvaða lagalega grundvelli meðhöndlun þeirra er byggð.

Ný löggjöf mun mæla fyrir um fleiri og strangari skuldbindingar en áður. Þess er m.a. krafist að nýr hugbúnaður og upplýsingakerfi séu útfærð með sérstaka áherslu á friðhelgi einstaklinga og á þann hátt að hún sé innbyggð í viðkomandi lausn. Þá er gert ráð fyrir að allar opinberar stofnanir hafi sérstakan persónuverndarfulltrúa sem er ætlað það hlutverk að vera sérfræðingur aðila í persónuvernd og tengiliður milli stjórnenda, hinna skráðu og Persónuverndar. Til viðbótar má nefna að nýja löggjöfin mun skylda vinnsluaðila til þess að setja sér verklagsreglur um vinnslu og meðferð persónuupplýsinga.

IV.

Eftirfarandi eru upplýsingar um stöðu einstakra liða í álit Persónuverndar á vinnslu persónuupplýsinga og öryggi þeirra í vefkerfinu Mentor auk þess sem settar eru fram tillögur þar sem við á, um úrbætur og eftir atvikum, tillögur að tímasettri áætlun um lok verkefnis.

Samantekt tillagna og drög að ferli:

1. Vinnsluaðilum verður sent bréf í þeim tilgangi að sannreyna að vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit.
2. Komi í ljós að vinnsluaðili uppfylli kröfur ábyrgðaraðila verður gerður vinnslusamningur við vinnsluaðila.
3. Gefnar verða út leiðbeiningar til grunnskóla um notkun rafrænna upplýsingakerfa sem er ætlað að vera grunnskólum til aðstoðar við undirbúning að setningu eigin leiðbeininga.
4. Ráðinn verði sérfræðingur í upplýsingaöryggi og áhættumati til að skrifa öryggishandbók vegna notkunar grunnskólanna á rafrænum upplýsingakerfum og til að aðstoða við setningu upplýsingaöryggisstefnu.
5. Í kjölfar vinnu sérfræðings fari fram endurskoðun á leiðbeiningum skv. lið 3.
6. Hafinn verði nú þegar undirbúningur að breytingum er verða í tengslum við nýja persónuverndarlöggjöf.

V.

Hér á eftir koma nánari útfærslur á tillögum starfshópsins og viðbrögð við álit Persónuverndar. Það skal athugast að búið er að bera tillögur þessar undir Persónuvernd, Samband íslenskra sveitarfélaga og mennta- og menningarmálaráðuneytið.

1. Viðkvæmar persónuupplýsingar verði ekki skráðar nema útbúið verði sérstakt umhverfi fyrir slíkar skráningar.

Fram kemur í álit Persónuverndar að það sé 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 vinnslusamninga. Verður að ætla að eftir atvikum eigi skráning slíkra upplýsinga fremur heima í upplýsingakerfum þar sem sérstaks öryggis er gætt, eftir atvikum hjá sérfræðipjónustu í samræmi við lög um grunnskóla.

Staða:

Í kjölfar álits Persónuverndar frá 25. september 2015, var öllum grunnskólum í Reykjavík og utan sent bréf þar sem fram kom að ekki megi skrá viðkvæmar persónuupplýsingar, t.d. um greiningar eða heilsufar, um nemendur eða aðstandendur þeirra í rafræn upplýsingakerfi á borð við Mentor nema útbúið verði sérstakt umhverfi fyrir slíka skráningu sem fullnægir skilyrðum laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga.

Í bréfinu til skólanna kom fram að Persónuvernd mælist til þess að þar til að skilyrðum er fullnægt verði slíkar upplýsingar í sérstökum skráum sem ekki eru í Mentor eða sambærilegum upplýsingakerfum. Fram kom að skráning slíkra upplýsinga eigi fremur heima í upplýsingakerfum þar sem gætt er sérstaks öryggis, eftir atvikum hjá sérfræðipjónustu í samræmi við lög nr. 91/2008 um grunnskóla. Voru skólastjórar í grunnskólum Reykjavíkur minntir á að upplýsingar um nemendur skuli geymdar í persónumöppu nemenda til samræmis við leiðbeiningar um skjalavörslu fyrir grunnskóla Reykjavíkurborgar, útg. í apríl 2011. Þegar persónuupplýsingar eru skráðar og varðveittar í tölvu skuli þess gætt að viðkomandi skrá sé læst með tryggilegum hætti og að aðgengi að henni sé takmarkað við þá sem þurfa aðgang vegna starfa sinna.

Í bréfi mennta- og menningarmálaráðuneytis, dags. 28. september sl., til skóla- og frístundasviðs kemur fram að tilefni sé til að skoða sérstaklega hvort rétt og nauðsynlegt sé að skrá með rafrænum hætti viðkvæmar persónuupplýsingar um nemendur í Mentor.

Aðgerðir:

Á meðan ekki er til staðar kerfi sem uppfyllir kröfur laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga, einkum hvað varðar öryggi persónuupplýsinga og gerð vinnslusamninga, þá verði viðkvæmar persónuupplýsingar unnar og vistaðar með óbreyttum hætti sbr. framangreint. Telji sveitarfélag þörf á vinnslu viðkvæmra persónuupplýsinga í rafrænum kerfum verður sveitarfélag að tryggja að skilyrði laga nr. 77/2000 og gerð vinnslusamninga sé uppfyllt og að aðgengi verði takmarkað með sérstökum aðgangi og að hann verði bundinn við t.d. skólastjóra, umsjónarkennara og foreldra.

Hvenær lokið:

Ekki er þörf á tímatakmörkunum þar sem grunnskólum ber að vista umrædd gögn með tryggum hætti nema sveitarfélag komi því til leiðar að rafrænu kerfi verði breytt.

2. Haga ber vinnslu persónuupplýsinga í Mentor í samræmi við ákvæði 7. gr. laga nr. 77/2000.

Setja þarf verklagsreglur/leiðbeiningar um hvernig haga beri vinnslu persónuupplýsinga og skráningu þeirra í Mentor. Starfshópurinn hefur unnið fyrirmynd að leiðbeiningum sem grunnskólar geta nýtt sem grunn við undirbúning að setningu eigin leiðbeininga, sbr. **fskj. 1**.

Aðgerðir:

Grunnskólar fá afhentar meðfylgjandi leiðbeiningar um hvernig haga beri vinnslu persónuupplýsinga í samræmi við 7., 8. og 9. gr. laga nr. 77/2000, sbr. **fskj. 1**.

Hvenær lokið:

Leiðbeiningar sendar grunnskólum með fyrirmælum um kynningu fyrir starfsfólki.

Sveitarfélög fái þann frest sem talinn er nauðsynlegur til að gera skýrari viðmið með tilliti til mögulegra skýrari viðmiða í reglugerð og með tilliti til gerðar öryggishandbókar sem unnin verði af sérfræðingi í upplýsingaöryggi og áhættumati.

3. Verklagsreglur um skráningar.

Gæta ber að lögmæti þeirra upplýsinga sem eru skráðar í kerfið, m.a. með því að setja verklagsreglur þar sem fjallað er um *hvenær* megi skrá upplýsingar um nemendur í Mentor (einkum í dagbókarflípan), *hvað* megi skrá um nemendur, *hverjum* eigi að birta færslu sem skráðar eru í dagbókarflípa 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 ábyrgðaraðilum.

Aðgerðir:

Í leiðbeiningum til grunnskóla koma fram upplýsingar sem til greina kemur að setja í rafræn upplýsingakerfi. Þá geyma leiðbeiningarnar nánari skýringar á flokkun upplýsinga; hvar upplýsingarnar eru skráðar, hver má skrá upplýsingarnar og hver megi sjá þær. Auk þess eru settar fram almennar leiðbeiningar um skráningar í dagbók, sbr. **fskj. 1**.

Hvenær lokið:

Grunnskólar fá afhentar meðfylgjandi leiðbeiningar sem eru að finna í **fskj. 1**.

Starfshópurinn leggur til að leiðbeiningarnar verði endurskoðaðar þegar og ef skýrari viðmið verða sett í reglugerð og tekið hefur verið tillit til öryggishandbókar þegar hún verður tilbúin.

4. Gerð er krafa um að ábyrgðaraðilar útbúi öryggisstefnu, áhættumat og öryggisráðstafanir og lýsingu á fyrirkomulagi innra eftirlits.

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 auk þess sem lýsa skal fyrirkomulagi innra eftirlits.

Það er mat starfshópsins að ráða þurfi sérfræðing í upplýsingaöryggi og áhættumati til að skrifa öryggishandbók fyrir grunnskólana um notkun á upplýsingaskráningarkerfum líkt og Mentor og að ráða þurfi sérfræðing til að aðstoða við setningu upplýsingaöryggisstefnu. Fram hefur komið hjá mennta- og menningarmálaráðuneytinu að í tengslum við setningu reglugerðar nr. 235/2012 um upplýsingaskyldu framhaldsskóla um skólahald, aðra kerfisbundna skráningu og meðferð persónuupplýsinga um nemendur, hafi ráðuneytið fengið til liðs við sig sérfræðing í upplýsingaöryggi og áhættumati sem kom að undirbúningi upplýsingaöryggisstefnu og gerð

Öryggishandbókar en sú vinna nýttist síðan við nánari útfærslu einstakra ákvæða reglugerðarinnar. Starfshópurinn leggur til að sveitarfélögin sameinist um þessa vinnu.

Hvenær lokið:

Sveitarfélög fái 6 mánaða frest til að útbúa handbók þar sem fjallað verði um öryggiskerfi, skriflega öryggisstefnu og skriflegt áhættumat auk ákvörðunar um nauðsynlegar öryggisráðstafanir og lýsingu innra eftirlits.

Hvað varðar öryggisstefnu, áhættumat, öryggisráðstafanir og fyrirkomulag innra eftirlits þarf í samræmi við álit Persónuverndar nr. 1203/2015, sérstaklega að huga að eftirfarandi atriðum:

A. Undirritun þagnarskylduyfirlýsinga.

Meðfylgjandi eru drög að þagnarskylduyfirlýsingu, sbr. **fskj. 2.**

Hvenær lokið:

Sent grunnskólum til notkunar á sama tíma og leiðbeiningar sbr. **fskj. 1.**

B. Reglubundin fræðsla fyrir starfsmenn þar sem þeim er gerð grein fyrir starfsskyldum sínum og afleiðingum þess að brjóta þær.

Í leiðbeiningum í **fskj. 1** koma fram upplýsingar um nauðsyn reglubundinnar fræðslu til handa starfsmönnum þar sem þeim er gerð grein fyrir starfsskyldum sínum og afleiðingum þess að brjóta þær.

Hvenær lokið:

Leiðbeiningar í **fskj. 1** verða sendar grunnskólum til notkunar.

C. Notkun kennitölu sem notendanafn í Mentor verður hætt.

Óskað er staðfestingar á því frá Persónuvernd um að gerð sé krafa um að hætt verði að nota kennitölu sem notendanafn. Fyrir liggur að kennitala er notuð í mjög mörgum rafrænum þjónustukerfum á vegum sveitarfélaganna.

Hvenær lokið:

Ef staðfest er að hætta eigi að nota kennitölu sem notendanafn verði óskað eftir fresti til 1. júní 2017 til að fá þessu breytt.

D. Gerð verður krafa um að lykilorð notanda verði breytt við fyrstu innskráningu og það fullnægi skilyrðum til að teljast sterkt.

Umrædd öryggisaðgerð er þegar til staðar í kerfinu og því ekki þörf á frekari aðgerðum, allir notendur þurfa að breyta lykilorði við fyrstu innskráningu. Krafa er gerð um sterkt lykilorð. Tryggja þarf að lykilorði sé breytt með reglubundnum hætti.

Hvenær lokið:

Óskað eftir fresti til 1. júní 2017 til að tryggja að lykilorði sé breytt með reglubundnum hætti.

E. Öryggisráðstafanir tengdar fjaraðgangi starfsmanna.

Það er mat starfshópsins að hér vanti skýrari viðmið til að sveitarfélög geti í kjölfarið metið þörf og áhættu á fjaraðgangi starfsmanna að Mentor. Fram kemur í bréfi mennta- og menningarmálaráðuneytis, dags. 27. september 2016, að það sé mat ráðuneytisins að gildið skuli varhug við svokölluðum fjaraðgangi að Mentor, þ.e. skráningum starfsmanna utan starfsstöðvar, sem kann að skapa hættu á misnotkun kerfisins og

ónákvæmumskráningum. Rétt er að hafa í huga að aðgangur að Mentor er vefaðgangur og því fjaraðgangur í eðli sínu og þarfnast athugasemdin nánari útskýringa.

Hvenær lokið:

Tilfni er til þess að mennta- og menningarmálaráðuneyti skoði breytingar á reglugerð með tilliti til þess að kveðið verði skýrt á um hvort rétt sé að banna fjaraðgang að skráningarkerfum sem innihalda persónuupplýsingar um nemendur og forsjáraðila þeirra. Útskýra þarf nánar við hvað er átt þar sem þar sem t.d. aðgangur að Mentor er vefaðgangur og því fjaraðgangur í eðli sínu. Fram að þeim tíma verði kveðið á um í leiðbeiningum að meginreglan skuli vera sú að ekki skuli vera fjaraðgangur að rafrænum upplýsingakerfum.

F. Upplýsingagjöf til handa starfsmönnum um skráningu aðgerða í Mentor og að settar verði reglur um notkun upplýsinga úr aðgerðaskrá.

Það er mat starfshópsins að hér vanti skýrari viðmið. Sveitarfélög fái 6 mánaðar frest til að útbúa handbók þar sem fjallað verði um öryggiskerfi, skriflega öryggisstefnu og skriflegt áhættumat auk ákvörðunar um nauðsynlegar öryggisráðstafanir og lýsingu innra eftirlits.

5. Ábyrgðaraðila ber að semja við vinnsluaðila í samræmi við ákvæði 13. gr. laga nr. 77/2000.

Fram kemur í álit Persónuverndar að í 13. gr. laga nr. 77/2000 komi 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.

Starfshópurinn hefur með aðstoð upplýsinga- og tæknideildar Reykjavíkurborgar unnið meðfylgjandi bréf til vinnsluaðila í þeim tilgangi að sannreynt verði að umræddur vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit, sbr. **fskj. 3.**

Starfshópurinn hefur einnig gert drög að meðfylgjandi samningi við vinnsluaðila auk leiðbeininga um vinnslusamninga, sbr. **fskj. 4 og 5.**

Hvenær lokið:

Starfshópurinn leggur til að vinnsluaðilum verði send nú þegar framangreind könnun þar sem þeim verður gert að sannreyna að þeir geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit. Ef í ljós kemur að vinnsluaðili stenst kröfur verði gerður við þá vinnslusamningur. Ferlinu verði lokið innan þriggja mánaða.

VI.

Því fylgir mikil ábyrgð fyrir opinberar stofnanir að fjalla um persónulega hagi fólks og eru leik- og grunnskólar, börn og foreldrar þeirra þar engin undantekning. Í erindi þessu og fylgiskjöllum hefur starfshópurinn tekið fyrstu skrefin í þá átt að tryggja meðferð persónuupplýsinga um nemendur í grunnskólum landsins í samræmi við álit Persónuverndar frá 23. september 2015. Öryggi varðandi skráningar persónuupplýsinga þarf að vera í stöðugri endurskoðun og lítur starfshópurinn svo á

að huga þurfi að öryggiskröfum með reglubundnum hætti. Athugasemdir Persónuverndar í álit
stofnunarinnar nr. 1203/2015, voru tímabærar og mikilvægar.

Virðingarfyllst,
f.h. starfshóps

Guðrún Sigtryggisdóttir
yfirlögfræðingur skóla- og frístundasviðs

Leiðbeiningar um notkun rafrænna upplýsingakerfa við meðferð persónuupplýsinga nemenda í grunnskólum

(Starfshópur um skoðun á skráningum upplýsinga um nemendur grunnskóla í rafræn upplýsingakerfi í tengslum við álit Persónuverndar í máli nr. 2015/1203).

Nóvember 2016

Efnisyfirlit

1. Gildissvið og markmið	3
2. Almennt	3
3. Skilgreining hugtaka og ábyrgð á meðferð persónuupplýsinga í grunnskólum.	4
4. Greining upplýsinga í persónuupplýsingar og viðkvæmar persónuupplýsingar	5
5. Skilyrði vinnslu persónuupplýsinga	5
5.1 Almenn skilyrði vinnslu persónuupplýsinga	5
5.2 Skilyrði vinnslu viðkvæmra persónuupplýsinga	6
6. Meginreglur sem gilda um gæði gagna og vinnslu	6
7. Réttur foreldra á aðgangi að upplýsingum og fræðsla til foreldra og nemenda	7
7.1 Réttur á aðgangi að upplýsingum	7
7.2 Fræðsla til foreldra, forsjármanna og nemenda	7
8. Leiðbeiningar um skráningu upplýsinga í rafræn upplýsingakerfi	8
3. Námsárangur	11
9. Öryggi upplýsinga	15
9.1 Almennt um áhættumat, öryggi og gæði persónuupplýsinga.	15
9.2 Öryggisstefna	16
9.3 Áhættumat	16
9.4 Öryggisráðstafanir	16
9.5 Öryggisráðstafanir varðandi starfsmannamál og fræðsla til starfsfólks	16
9.6 Ytra öryggi	17
9.7 Skipulagslegar og tæknilegar öryggisráðstafanir	17
9.8 Endurskoðun áhættumats og öryggisráðstafana	17
9.9 Innra eftirlit	18
10. Eyðing og leiðrétting	18
11. Varsla gagna og afhending til þjóðskjalasafns	19
12. Samningur við utanaðkomandi aðila um vinnslu persónuupplýsinga	19
13. Öryggisráðstafanir vinnsluaðila og sannreying	20
FYLGISKJÖL	20

1. Gildissvið og markmið

Leiðbeiningar þessar fjalla um notkun rafrænna upplýsingakerfa við skráningu, miðlun og meðferð persónuupplýsinga nemenda í grunnskóla.

Markmið leiðbeininganna er að tryggja að farið sé að lögum, reglugerðum og reglum við meðferð persónuupplýsinga við notkun rafrænna upplýsingakerfa í grunnskólum. Tekið er fram að lög og reglur sem getið er í leiðbeiningunum gilda um alla vinnslu og miðlun upplýsinga í tölvuskýjum.

Leiðbeiningarnar eiga að tryggja að við meðferð og öflun persónuupplýsinga sé þess gætt að þær séu unnar með sanngjörnum, málefnalegum og lögmætum hætti og að öll meðferð þeirra sé í samræmi við vandaða vinnsluhætti persónuupplýsinga samkvæmt fyrirmælum laga um persónuvernd og meðferð persónuupplýsinga og þeirra laga sem nefnd hafa verið. Leiðbeiningarnar eiga að tryggja að gætt sé að því að upplýsingar sem aflað er séu viðeigandi og ekki umfram það sem nauðsynlegt er miðað við tilgang vinnslu þeirra. Þær séu áreiðanlegar og uppfærðar eftir þörfum.

Um meðferð persónuupplýsinga nemenda í grunnskólum gilda lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga. Jafnframt gilda lög um grunnskóla nr. 91/2008, og reglugerðir settar skv. þeim svo sem reglugerð nr. 897/2009 um miðlun og meðferð upplýsinga um nemendur í grunnskólum og rétt foreldra til aðgangs að upplýsingum um börn sín, sbr. breyting nr. 657/2011 og reglugerð þar um. Auk þess þarf m.a. að taka tillit til laga um samning Sameinuðu þjóðanna um réttindi barnsins nr. 19/2013, stjórnsýslulaga nr. 37/1993, upplýsingalaga nr. 140/2012, barnalaga nr. 76/2003 og laga um opinber skjalasöfn nr. 77/2014. Auk þessa þarf að tryggja að farið sé að reglum 299/2001 um öryggi persónuupplýsinga.

2. Almenn

Samkvæmt 2. mgr. 18. gr. grunnskólalaga, með síðari breytingum, er foreldrum skylt að veita grunnskóla upplýsingar um barn sitt sem nauðsynlegar eru fyrir skólastarfið og velferð barnsins. Um persónuupplýsingar sem þannig er aflað eða fylgt hafa barni úr leikskóla er krafist fullrar þagnarskyldu og málsmeðferðar í samræmi við gildandi lög um persónuvernd og meðferð persónuupplýsinga. Foreldrum skal gerð grein fyrir þessum upplýsingum og skal samþykki um miðlun þeirra liggja fyrir í upphafi hvers skólaárs. Meðferð upplýsinga skal vera á hendi skólastjóra eða annarra sérfræðinga á vegum sveitarfélagsins.

Í framangreindu ákvæði grunnskólalaga kemur fram að ráðherra gefur út reglugerð um meðferð, eyðingu og miðlun upplýsinga og um rétt foreldra til aðgangs að upplýsingum um börn sín. Sveitarstjórnnum er jafnframt heimilt að setja reglur um skráningu, meðferð og miðlun þessara upplýsinga.

Við setningu og framkvæmd reglna skulu sveitarfélög taka mið af lögum um persónuvernd og meðferð persónuupplýsinga og alþjóðlegum skuldbindingum sem íslensk stjórnvöld hafa gengist undir og leidd hafa verið inn í íslenska löggjöf, einkum samningur Sameinuðu þjóðanna um réttindi barnsins. Reglur sveitarfélaganna eiga að koma í veg fyrir að skráning persónuupplýsinga um nemendur í rafræn upplýsingakerfi séu háð persónulegu mati hvers kennara eða starfsmanns sem skráir þar inn upplýsingar um nemendur.

Grunnskólum er heimilt að nota rafrænt upplýsingakerfi til skráningar og miðlunar upplýsinga um nemendur samkvæmt reglugerð um miðlun og meðferð upplýsinga um nemendur í grunnskólum og rétt foreldra til aðgangs að upplýsingum um börn sín nr. 897/2009 með síðari breytingum. Enn fremur getur skóli notað slíkt kerfi til þess að veita foreldrum aðgang að upplýsingum og til samskipta við þá.

Ákveði grunnskóli að samið verði við tiltekinn aðila um að annast, í heild eða að hluta, vinnslu persónuupplýsinga, þá er slíkt háð því skilyrði að grunnskóli hafi áður sannreynt að umræddur vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit skv. 12. gr. laga um meðferð persónuupplýsinga og persónuvernd, sjá umfjöllun í lið 12 í leiðbeiningum þessum.

Samningur skv. framangreindu, vinnslusamningur, skal vera skriflegur og a.m.k. í tveimur eintökum. Þar skal m.a. koma fram að vinnsluaðili sé einungis heimilt að starfa í samræmi við fyrirmæli ábyrgðaraðila og að ákvæði laga um persónuvernd og meðferð persónuupplýsinga um skyldur ábyrgðaraðila gildi einnig um þá vinnslu sem vinnsluaðili annast, sjá umfjöllun í lið 13 í leiðbeiningum þessum.

Gæta skal fullrar þagnarskyldu um meðferð persónuupplýsinga sem aflað er um nemendur í grunnskóla eða hafa fylgt barni úr leikskóla. Um þagnarskyldu starfsmanna sveitarfélaga fer samkvæmt 2. mgr. 57. gr. sveitarstjórnarlaga nr. 138/2011 og 12. gr. laga nr. 91/2008 um grunnskóla.

Grunnskóli skal tryggja að farið sé með persónuupplýsinga um nemendur af þeirri varúð sem reglur um þagnarskyldu og tilgangur vinnslunnar krefjast.

3. Skilgreining hugtaka og ábyrgð á meðferð persónuupplýsinga í grunnskólum.

Lög um meðferð persónuupplýsinga og persónuvernd gilda um sérhverja rafræna vinnslu persónuupplýsinga. Lögin gilda einnig um handvirka vinnslu persónuupplýsinga sem eru eða eiga að verða hluti af skrá um viðkomandi nemanda.

Persónuupplýsingar eru sérhverjar persónugreindar eða persónugreinanlegar upplýsingar um hinn skráða, þ.e. upplýsingar sem beint eða óbeint má rekja til tiltekins einstaklings, látins eða lifandi.

Vinnsla persónuupplýsinga er sérhver aðgerð eða röð aðgerða þar sem unnið er með persónuupplýsingar, hvort heldur sem vinnslan er handvirk eða rafræn.

Ábyrgðaraðili á meðferð upplýsinga er sá aðili sem ákveður tilgang vinnslu persónuupplýsinga, þann búnað sem notaður er, aðferð við vinnsluna og aðra ráðstöfun upplýsinganna. Með vísan til þessa eru það skólastjórar í grunnskólum sem bera ábyrgð á meðferð persónuupplýsinga nemenda og að farið sé að framangreindum lögum.

Grunnskólum ber að fara að lögum um meðferð persónuupplýsinga og persónuvernd og öðrum lögum sem nefnd voru hér að framan.

4. Greining upplýsinga í persónuupplýsingar og viðkvæmar persónuupplýsingar

Skv. lögum um meðferð persónuupplýsinga og persónuvernd eru persónuupplýsingar greindar í tvo þætti, annarsvegar *persónuupplýsingar* og hinsvegar *viðkvæmar persónuupplýsingar*.

Persónuupplýsingar eru: Sérhverjar persónugreindar eða persónugreinanlegar upplýsingar um hinn skráða, þ.e. upplýsingar sem beint eða óbeint má rekja til tiltekins einstaklings, látins eða lifandi.

Viðkvæmar persónuupplýsingar eru:

- a. Upplýsingar um uppruna, litarhátt, kynþátt, stjórnmalaskoðanir, svo og trúar- eða aðrar lífsskoðanir.
- b. Upplýsingar um hvort maður hafi verið grunaður, kærður, ákærður eða dæmdur fyrir refsiverðan verknað.
- c. Upplýsingar um heilsuhagi, þar á meðal um erfðaeiginleika, lyfja-, áfengis- og vímuefnanotkun.
- d. Upplýsingar um kynlíf manna og kynhegðun.
- e. Upplýsingar um stéttarfélagsaðild.

5. Skilyrði vinnslu persónuupplýsinga

5.1 Almenn skilyrði vinnslu persónuupplýsinga

Til þess að vinnsla almennra persónuupplýsinga sé heimil verður grunnskóli að gæta þess að eitthvert af skilyrðum 8. gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga sé uppfyllt. Þegar grunnskóli vinnur 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.

Með vísan til framangreinds þarf skólastjóri að tryggja að áður en skóla er heimilt að vinna með persónuupplýsingar nemenda sé uppfyllt í það minnsta eitt af eftirtöldum skilyrðum:

1. [hinn skráði hafi ótvírætt samþykkt vinnsluna eða veitt samþykki skv. 7. tölul. 2. gr.]1)
2. vinnslan sé nauðsynleg til að efna samning sem hinn skráði er aðili að eða til að gera ráðstafanir að beiðni hins skráða áður en samningur er gerður;
3. vinnslan sé nauðsynleg til að fullnægja lagaskyldu sem hvílir á ábyrgðaraðila;
4. vinnslan sé nauðsynleg til að vernda brýna hagsmuni hins skráða;
5. vinnslan sé nauðsynleg vegna verks sem unnið er í þágu almannahagsmuna;
6. vinnslan sé nauðsynleg við beitingu opinbers valds sem ábyrgðaraðili, eða þriðji maður sem upplýsingum er miðlað til, fer með;
7. vinnslan sé nauðsynleg til að ábyrgðaraðili, eða þriðji maður eða aðilar sem upplýsingum er miðlað til, geti gætt lögmætra hagsmuna nema grundvallarréttindi og frelsi hins skráða sem vernda ber samkvæmt lögum vegi þyngra.

5.2 Skilyrði vinnslu viðkvæmra persónuupplýsinga

Áður en skóli vinnur með viðkvæmar persónuupplýsingar þarf jafnframt að uppfylla eitt ef eftirtöldum skilyrðum:

1. hinn skráði samþykki vinnsluna;
2. sérstök heimild standi til vinnslunnar samkvæmt öðrum lögum;
3. ábyrgðaraðila beri skylda til vinnslunnar samkvæmt samningi aðila vinnumarkaðarins;
4. vinnslan sé nauðsynleg til að verja verulega hagsmuni hins skráða eða annars aðila sem ekki er sjálfur fær um að gefa samþykki sitt skv. 1. tölul.;
5. vinnslan sé framkvæmd af samtökum sem hafa stéttarfélagsleg markmið eða af öðrum samtökum sem ekki starfa í hagnaðarskyni, svo sem menningar-, líknar-, félagsmála- eða hugsjónasamtökum, enda sé vinnslan liður í lögmætri starfsemi samtakanna og taki aðeins til félagsmanna þeirra eða einstaklinga sem samkvæmt markmiðum samtakanna eru, eða hafa verið, í reglubundnum tengslum við þau; slíkum persónuupplýsingum má þó ekki miðla áfram án samþykkis hins skráða;
6. vinnslan taki einungis til upplýsinga sem hinn skráði hefur sjálfur gert opinberar;
7. vinnslan sé nauðsynleg til að krafa verði afmörkuð, sett fram eða varin vegna dómsmáls eða annarra slíkra laganauðsynja;
8. vinnslan sé nauðsynleg vegna læknismeðferðar eða vegna venjubundinnar stjórnsýslu á sviði heilbrigðisþjónustu, enda sé hún framkvæmd af starfsmanni heilbrigðisþjónustunnar sem bundinn er þagnarskyldu;
9. vinnslan sé nauðsynleg vegna tölfræði- eða vísindarannsóknar, enda sé persónuvernd tryggð með tilteknum ráðstöfunum eftir því sem við á.

Eftir að staðreynt hefur verið að eitt af ofangreindum skilyrðum sé fyrir hendi er heimilt að vinna viðkvæmar persónuupplýsingar en ávallt verður að huga að meginreglunum fimm um gæði gagna og vinnslu sem fjallað er um í tölulið 6 í þessum leiðbeiningum.

6. Meginreglur sem gilda um gæði gagna og vinnslu

Hverjum grunnskóla fyrir sig ber að gæta að þeim fimm meginreglum sem gilda um gæði gagna og vinnslu við meðferð persónuupplýsinga en gæta verður að þeim öllum:

1. að persónuupplýsingarnar séu unnar með sanngjörnum, málefnalegum og lögmætum hætti og að öll meðferð þeirra sé í samræmi við vandaða vinnsluhætti persónuupplýsinga;
2. að persónuupplýsingarnar séu fengnar í yfirlýstum, skýrum, málefnalegum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi, en frekari vinnsla í sagnfræðilegum, tölfræðilegum eða vísindalegum tilgangi telst ekki ósamrýmanleg að því tilskildu að viðeigandi öryggis sé gætt;
3. að persónuupplýsingarnar séu nægilegar, viðeigandi og ekki umfram það sem nauðsynlegt er miðað við tilgang vinnslunnar;
4. að persónuupplýsingarnar séu áreiðanlegar og uppfærðar eftir þörfum. Þær persónuupplýsingar sem eru hins vegar óáreiðanlegar eða ófullkomnar, miðað við tilgang vinnslu þeirra, skal afmá eða leiðrétta;
5. að persónuupplýsingarnar séu varðveittar í því formi að ekki sé unnt að bera kennsl á skráða aðila lengur en þörf krefur miðað við tilgang vinnslu.

Skólastjóri ber ábyrgð á því að vinnsla persónuupplýsinga uppfylli ávallt ofangreint.

7. Réttur foreldra á aðgangi að upplýsingum og fræðsla til foreldra og nemenda

7.1 Réttur á aðgangi að upplýsingum

Foreldrar eiga rétt á aðgangi að upplýsingum um börn sín. Um takmarkanir á upplýsingarétti þeirra fer samkvæmt fyrirmælum 17. gr. stjórnsýslulaga nr. 37/1993 og 9. gr. upplýsingalaga nr. 50/1996. Í framangreindum ákvæðum kemur fram að þegar sérstaklega stendur á er stjórnvaldi heimilt að takmarka aðgang aðila máls að gögnum ef hagsmunir hans af því að notfæra sér vitneskju úr þeim þykja eiga að víkja fyrir mun ríkari almanna- eða einkahagsmunum.

Það foreldri sem ekki hefur forsjá barns á rétt á að fá upplýsingar um barnið frá grunnskóla. Um rétt foreldris til upplýsinga fer samkvæmt fyrirmælum 52. gr. barnalaga nr. 76/2003. Í 2. mgr. 52. gr. barnalaga kemur fram að það foreldri sem ekki hefur forsjá barns eigi rétt á að fá aðgang að skriflegum gögnum um barnið frá skólum og leikskólum. Það foreldri á einnig rétt á að fá munnlegar upplýsingar um barnið frá öðrum aðilum sem fara með mál þess, svo sem sjúkrahúsum, heilsugæslu- og félagsmálastofnunum, félagsmálanefndum, barnaverndarnefndum og lögreglu. Réttur samkvæmt þessari málsgrein felur ekki í sér heimild til að fá upplýsingar um hagi forsjárforeldris.

Í 3. mgr. 52. gr. barnalaga kemur fram að stofnunum og stjórnvöldum, sem nefnd eru í 2. mgr., sé þó heimilt að synja um upplýsingar ef hagsmunir foreldris af því að notfæra sér þær þykja eiga að víkja fyrir mun ríkari almanna- eða einkahagsmunum, þar á meðal ef telja verður að upplýsingagjöf sé skaðleg fyrir barn. Í greinargerð með lögum um framangreint ákvæði kemur fram að hér sé að finna mikilvægt nýmæli um að forsjárlaust foreldri eigi rétt á aðgangi að skriflegum gögnum um barnið frá skóla og leikskóla. Vert sé að taka fram að hér sé eingöngu um að ræða aðgang að gögnum sem þegar eru fyrir hendi en ekki rétt til að láta útbúa fyrir sig sérstök gögn.

Þegar grunnskóli notar rafrænt upplýsingakerfi til þess að veita foreldrum aðgang að upplýsingum og til samskipta við þá getur skóli, komi fram rökstudd beiðni frá foreldrum, veitt aðgang að upplýsingum með öðrum hætti, s.s. með tölvupósti, símleiðis eða bréfleiðis. Skal þá 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. Þegar fallist er á slíkar beiðnir þarf að tryggja að upplýsingar séu veittar með öruggum hætti. Þannig er, sem dæmi, lokuð Facebook síða ekki öruggur vettvangur til miðlunar persónuupplýsinga.

Það skal vera meginregla að foreldrum séu birtar allar upplýsingar sem skráðar eru í rafræn upplýsingakerfi grunnskóla um börn þeirra.

Upplýsingar sem kennarinn hefur til minnis fyrir sig sjálfan er ekki skylt að birta foreldrum eða forsjármanna.

7.2 Fræðsla til foreldra, forsjármanna og nemenda

Þegar grunnskóli notar rafrænt upplýsingakerfi til skráningar og miðlunar upplýsinga um nemendur getur skólinn notað kerfið til þess að veita foreldrum aðgang að upplýsingum og til samskipta við þá. Fræða ber foreldra og nemendur um að skóli noti rafrænt upplýsingakerfi

og að þar séu skráðar persónuupplýsingar um nemendur. Upplýsingar um notkun rafræns upplýsingakerfis skulu birtar á heimasíðu skóla og jafnframt leiðbeiningar þessar.

Geti foreldrar átt samskipti við foreldra annarra barna í bekk barna sinna með rafrænu upplýsingakerfi grunnskóla bera foreldrar ábyrgð á þeim samskiptum og að farið sé að lögum um persónuvernd og meðferð persónuupplýsinga.

Skólastjóra bera að halda skrá um fræðslu til foreldra og nemenda þar sem fram kemur hvenær fræðsla fór fram, um hvað var fjallað og hverjir fengu fræðslu.

Í 8. lið leiðbeininganna eru upplýsingar um hvað er heimilt að skrá um nemendur og hverjum eigi að birta færslur.

Þegar grunnskóli aflar persónuupplýsinga hjá foreldrum nemenda eða nemanda sjálfum skal hann upplýsa þau um eftirtalin atriði:

- a. nafn og heimilisfang ábyrgðaraðila og eftir atvikum fulltrúa hans skv. 6. gr. laga um persónuvernd og meðferð persónuupplýsinga,
- b. tilgang vinnslunnar,
- c. aðrar upplýsingar, að því marki sem þær eru nauðsynlegar, með hliðsjón af þeim sérstöku aðstæðum sem ríkja við vinnslu upplýsinganna, svo að hinn skráði geti gætt hagsmuna sinna, svo sem upplýsingar um:
 - i. viðtakendur eða flokka viðtakenda upplýsinganna,
 - ii. hvort honum sé skylt eða valfrjálst að veita umbeðnar upplýsingar og hvaða afleiðingar það kunni að hafa veiti hann þær ekki,
 - iii. ákvæði laganna um upplýsingarétt hins skráða, svo og rétt hins skráða til leiðréttingar og eyðingar rangra eða villandi persónuupplýsinga um hann.

Þegar ábyrgðaraðili aflar persónuupplýsinga frá öðrum en foreldrum eða nemandanum skal hann samtímis láta foreldra vita af því. Sé ætlun ábyrgðaraðila hins vegar að miðla upplýsingunum innan hæfilegra tímamarka frá öflun þeirra má hann þó fresta því þar til hann miðlar upplýsingunum í fyrsta sinn. Í tilkynningu til hins skráða skal veita sömu upplýsingar og nefnt hefur verið samkvæmt framangreindu.

Ekki þarf að tilkynna foreldrum ef:

1. óframkvæmanlegt er að láta hinn skráða vita eða það leggur þyngri byrðar á ábyrgðaraðila en með sanngirni má krefjast,
2. ætla má að hinum skráða sé þegar kunnugt um vinnsluna,
3. lagaheimild stendur til skráningar eða miðlunar upplýsinganna eða
4. hagsmunir hins skráða af því að fá vitneskju um upplýsingarnar þykja eiga að víkja fyrir veigamiklum almannahagsmunum eða einkahagsmunum, þ.m.t. hagsmunum hans sjálfs.

8. Leiðbeiningar um skráningu upplýsinga í rafræn upplýsingakerfi

Við innritun barns í grunnskóla skulu foreldrar upplýstir um skyldu sína til þess að veita grunnskóla nauðsynlegar upplýsingar um barn sitt. Gefa skal foreldrum kost á að tilgreina sérstaklega nauðsynlegar upplýsingar um börn sín, sem máli skipta fyrir skólagöngu þess.

Hyggist skólastjórnendur afla upplýsinga um dvöl barns í öðrum skóla, eða slíkar upplýsingar hafa fylgt barni úr leikskóla með öðrum hætti en greinir í 1. mgr., skal foreldrum gerð grein fyrir þeim og um rétt þeirra til aðgangs að þeim. Sama á við um aðrar nauðsynlegar persónuupplýsingar sem grunnskóli aflar um barn meðan á skólagöngu þess stendur.

Sé ekki annað ákveðið af hálfu sveitarstjórnar ber skólastjóri ábyrgð á að foreldrum barns sé tilkynnt um upplýsingar sem aflað hefur verið um barn þeirra.

Til nauðsynlegra upplýsinga um nemanda teljast m.a. persónuupplýsingar um heilsufar, sérþarfir, líkamlega og andlega getu til náms eða annars skólastarfs sem afla þarf við undirbúning ákvarðana um réttindi og skyldur nemenda samkvæmt lögum um grunnskóla eða til að sveitarstjórn, eða skólanefnd í umboði hennar og eftir atvikum skólastjórnendur, geti sinnt skyldum sínum samkvæmt þeim lögum. Persónuupplýsingar geta verið:

- a. kennslufræðilegar, læknisfræðilegar, sálfræðilegar, sérkennslufræðilegar greiningar og aðrar greiningar og sérúrræði fyrir nemanda,
- b. sérkennsluumsóknir, námsáætlanir vegna sérúrræða og einstaklingsnámskrár,
- c. prófeinkunnir og vitnisburðir,
- d. mætingar og agabrot.

Persónuupplýsingar geta verið hvers konar skrifleg gögn svo sem skýrslur, greinargerðir og umsagnir eða gögn sem vistuð eru í tölvu og varða velferð og skólagöngu barns. Óheimilt er að miðla persónuupplýsingum um nemendur til annarra en þeirra sem þess þurfa vegna starfa sinna. Málsmeðferð skal vera í samræmi við gildandi lög um persónuvernd og meðferð persónuupplýsinga og ber starfsfólki grunnskóla að gæta að þagnarskyldu.

Eins og fjallað er um í lið 4 í leiðbeiningum þessum, teljast allar upplýsingar um nemendur vera persónuupplýsingar en aðeins hluti þeirra telst vera viðkvæmar persónuupplýsingar. Við skráningu persónuupplýsinga ber ávallt að gæta að meginreglunum fimm sem koma fram í lið 6 í leiðbeiningum þessum, sérstaklega um að vinnsla sé sanngjörn, gætt sé að meðalhófi, vinnsla sé málefnaleg og að ekki sé unnið með upplýsingar í öðrum tilgangi en upphaflega var stefnt að.

Upplýsingar um nemendur má flokka með eftirfarandi hætti:

1. Nemendaspjaldskrár

Nemendaspjaldskrá				
Upplýsingar	<i>nafn nemanda</i> kennitala kyn móðurmál	<i>móðir</i> kennitala heimilisfang póstnúmer lögheimili póstnúmer sími vinnusími farsími netfang	<i>faðir</i> kennitala heimilisfang póstnúmer lögheimili póstnúmer sími vinnusími farsími netfang	<i>aðrir</i> <i>forráðamenn</i> kennitala heimilisfang póstnúmer lögheimili póstnúmer sími vinnusími farsími netfang
Meðferð	Upplýsingar í rafrænum upplýsingakerfum eru aðgengilegar þeim sem þær þurfa starfa sinna vegna innan grunnskólans, viðkomandi nemanda og foreldra			
Hver má skrá?	Skrifstofa	Hver þarf aðgang?	- Skrifstofa - Stjórnendur - Umsjóunar-kennarar - Kennarar - Sérkennarar - Deildarstjóri sérkennslu - Námsráðgjafar - Þroskaþjálfar - Foreldrar - Nemendur	
Tilkynning		Athugasemd um verndun upplýsinga	Persónu-upplýsingar	

2. Skólaferill

Skólaferill				
Upplýsingar	Upphafsdagur skólagöngu. -Væntanlegur lokadagur skólagöngu. -Dagsetning útskriftar.	Skólaár – sundurgreining frá ári til árs. -Heimili – hvert ár. -Heimilis- eða farsími – hvert ár. -Póstnúmer.	-Skóli – hvert ár. -Bekkjardeild hvert ár. -Umsjónar-kennari hvert ár. -Fjöldi daga í skóla – hvert ár. -Upplýsingar um fjölda veikindadaga – hvert ár. -Upplýsingar um leyfisdaga – hvert ár.	-Reitur fyrir stutta almenna athugasemd – hvert ár. -Upplýsingar um frávík frá hefðbundinni skólagöngu.
Meðferð	Upplýsingar eru aðgengilegar þeim sem þurfa starfa sinna vegna auk viðkomandi nemanda og foreldra í rafrænum upplýsingakerfum			
Hver má skrá?	Skrifstofa	Hver þarf aðgang?	-Skrifstofa -Stjórnendur -Deildarstjóri sérkennslu -Foreldrar -Nemendur	
Tilkynning		Athugasemd um verndun upplýsinga	Persónuupplýsingar	

3. Námsárangur

Námsárangur			
Upplýsingar	Skólaár	Námsárangur sundurliðaður eftir námsgreinum eins og skilað er í námsáföngum skólans.	Námsárangur úr samræmdum könnunarprófum
Meðferð	Upplýsingar í rafrænum upplýsingakerfum eru aðgengilegar þeim sem þær þurfa starfa sinna vegna innan grunnskólans, viðkomandi nemanda og foreldra		
Hver má skrá?	Skrifstofa Umsjónarkennarar	Hver þarf aðgang?	Skrifstofa Stjórnendur -Deildarstjóri sérkennslu

			Umsjónarkennarar Kennarar Sérkennarar Námsráðgjafar Foreldrar Nemendur
Tilkynning		Athugasemd um verndun upplýsinga	Persónu- upplýsingar

4. Greiningar, úrlausn vegna barna með fjölþættan vanda

Greiningar, úrlausn vegna barna með fjölþættan vanda			
Upplýsingar	-Upplýsingar um greiningar á vegum opinberra greiningaraðila.	-Upplýsingar um greiningar á vegum skólajónustu.	- Upplýsingar um greiningar á vegum skólans.
Meðferð	Upplýsingar í rafrænum upplýsingakerfum eru aðgengilegar þeim sem þær þurfa starfa sinna vegna innan grunnskólans, viðkomandi nemanda og foreldra (eftir að skilyrði eru uppfyllt skv. lögum nr. 77/2000).		
Hver má skrá?	-Deildarstjóri sérkennslu	Hver má sjá?	-Stjórnendur -Umsjónarkennarar -Deildarstjóri sérkennslu -Sérkennarar -Námsráðgjafar -Foreldrar
Tilkynning		Athugasemd um verndun upplýsinga	Viðkvæmar persónuupplýsingar

5. Heilsufarsupplýsingar

Heilsufarsupplýsingar			
Upplýsingar	Upplýsingar um heilsufar sem hefur áhrif á skólagöngu.		
Meðferð	Upplýsingar í rafrænum upplýsingakerfum eru aðgengilegar þeim sem þær þurfa starfa sinna vegna innan grunnskólans, viðkomandi nemanda og foreldra (eftir að skilyrði eru uppfyllt skv. lögum nr. 77/2000).		
Hver má skrá?	-Deildarstjóri sérkennslu	Hver má sjá?	-Stjórnendur -Umsjónar-kennarar -Deildarstjóri sérkennslu

			-Sérkennarar -Námsráðgjafar -Foreldrar
Tilkynning		Athugasemd um verndun upplýsinga	Viðkvæmar persónuupplýsingar

6. Sérkennsla

Sérkennsla			
Upplýsingar	-Vísun í greiningar eða athuganir sem rökstyðja sérkennslu.	-Fjöldi kennslustunda í sérkennslu.	-Kennslugreinar í sérkennslu
Meðferð	Upplýsingar í rafrænum upplýsingakerfum eru aðgengilegar þeim sem þær þurfa starfa sinna vegna innan grunnskólans, viðkomandi nemanda og foreldra (eftir að skilyrði eru uppfyllt skv. lögum nr. 77/2000).		
Hver má skrá?	-Deildarstjóri sérkennslu	Hver má sjá?	-Stjórnendur -Umsjónar-kennarar -Deildarstjóri sérkennslu -Sérkennarar -Námsráðgjafar -Foreldrar
Tilkynning		Athugasemd um verndun upplýsinga	Viðkvæmar persónuupplýsingar

7. Sérkennsla – fötlun

Sérkennsla - fötlun			
Upplýsingar	-Upplýsingar um stuðningsaðila.	-Upplýsingar um sérkennslu.	-Upplýsingar um aðkomu sérfræðinga svo sem þroskajálfa.
Meðferð	Upplýsingar í rafrænum upplýsingakerfum eru aðgengilegar þeim sem þær þurfa starfa sinna vegna innan grunnskólans, viðkomandi nemanda og foreldra (eftir að skilyrði eru uppfyllt skv. lögum nr. 77/2000).		
Hver má skrá?	-Deildarstjóri sérkennslu	Hver má sjá?	-Stjórnendur -Umsjónar-kennarar -Deildarstjóri sérkennslu -Sérkennarar -Námsráðgjafar

			-Foreldrar
Tilkynning		Athugasemd um verndun upplýsinga	Viðkvæmar persónuupplýsingar

8. Dagbóarskráningar

Varðandi skráningu í dagbók þá er hún ætluð til skráninga á stærri atburðum, lýsingar eiga að vera hnitmiðaðar og gæta verður að því að lýsingin sé ekki gildishlaðin og aðrir nemendur ekki nafngreindir. Sem dæmi má taka að ekki á að skrá í dagbók lítil mál sem leyst eru á staðnum. Ekki á að skrá í dagbók upplýsingar sem teljast til viðkvæmra persónuupplýsinga svo sem umfjöllun um greiningar nemenda.

Gæta verði að reglunum 5 um gæði og gagna og vinnslu sem fjallað er um hér að framan. Hafa verður í huga að hlutaðeigandi eiga rétt á upplýsingunum og að meginreglan er sú að foreldrum skuli birt skráningin.

Dagbóarskráningar			
Upplýsingar	-Fundargerðir teymisfunda. -Fundargerðir vegna sérstakra funda með foreldrum. -Afrit af upplýsingum til Barnaverndar.	-Upplýsingar um úrvinnslu svo sem í einelti. -Upplýsingar um fyrirtöku í nemendaverndarráði.	-Skráningar með formlegu samþykki foreldra þegar unnið með frávík af einhverjum toga til að halda upplýsingum til haga á einum stað.
Meðferð	Upplýsingar í rafrænum upplýsingakerfum eru aðgengilegar þeim sem þær þurfa starfa sinna vegna innan grunnskólans, viðkomandi nemanda og foreldra (eftir að skilyrði eru uppfyllt skv. lögum nr. 77/2000).		
Hver má skrá?	- Umsjónarkennarar - Stjórnendur - Deildarstjóri sérkennslu	Hver má sjá?	-Stjórnendur -Umsjónar-kennarar -Deildarstjóri sérkennslu -Sérkennarar -Námsráðgjafar -Foreldrar
Tilkynning		Athugasemd um verndun upplýsinga	Viðkvæmar persónuupplýsingar

8. Dagbók umsjónarkennara, sérkennara og skólastjórnenda

Dagbók umsjónarkennara, sérkennara og skólastjórnenda			
Upplýsingar	-Atvikalýsingar vegna árekstra í skólastarfi. -Sérstakar upplýsingar sem skrá þarf vegna framvindu í námi.	-Frávíkshæðun sem bent getur til vanda sem hindrað gæti skólagöngu.	- Minnispointar um samskipti við nemendur.
Meðferð	Upplýsingar í rafrænum upplýsingakerfum eru aðgengilegar þeim sem þær þurfa starfa sinna vegna innan grunnskólans, viðkomandi nemanda og foreldra (eftir að skilyrði eru uppfyllt skv. lögum nr. 77/2000).		
Hver má skrá?	- Umsjónar-kennarar - Stjórnendur - Deildarstjóri sérkennslu - Sérkennarar	Hver má sjá?	-Stjórnendur -Umsjónar-kennarar -Deildarstjóri sérkennslu -Sérkennarar -Námsráðgjafar -Foreldrar
Tilkynning		Athugasemd um verndun upplýsinga	Viðkvæmar persónuupplýsingar

9. Öryggi upplýsinga

Samband íslenskra sveitarfélaga hefur óskað eftir því að Persónuvernd veiti 6 mánaða frest til að útbúa handbók þar sem fjallað verði um öryggiskerfi, skriflega öryggisstefnu og skriflegt áhættumat auk ákvörðunar um nauðsynlegar öryggisráðstafanir og lýsingu innra eftirlits. Engu að síður ber grunnskólum að tryggja öryggi upplýsinga og beita öllum tiltækum ráðum til að framfylgja lögum og reglum sem fjallað er um í leiðbeiningum þessum.

9.1 Almennt um áhættumat, öryggi og gæði persónuupplýsinga.

Grunnskólar skulu gera viðeigandi tæknilegar og skipulagslegar öryggisráðstafanir til að vernda persónuupplýsingar gegn ólöglegri eyðileggingu, gegn því að þær glattist eða breytist fyrir slysi og gegn óleyfilegum aðgangi.

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. Grunnskólar bera ábyrgð á því að áhættumat og öryggisráðstafanir við vinnslu persónuupplýsinga séu í samræmi við lög, reglur og fyrirmæli Persónuverndar um hvernig tryggja skuli öryggi upplýsinga, þ.m.t. þá staðla sem hún ákveður að skuli fylgt.

Grunnskólar bera ábyrgð á því að áhættumat sé endurskoðað reglulega og öryggisráðstafanir endurbættar að því marki sem þörf krefur til að uppfylla ákvæði þessarar greinar. Grunnskólar

skulu skrá með hvaða hætti þeir móta öryggisstefnu, gera áhættumat og ákveður öryggisráðstafanir.

9.2 Öryggisstefna

Ábyrgðaraðili setur sér skriflega öryggisstefnu. Í henni skal m.a. koma fram almenn lýsing á afstöðu æðsta stjórnanda ábyrgðaraðila til öryggismála. Við mótun öryggisstefnu skal taka mið af því hvaða persónuupplýsingar skuli vernda, hvernig skuli vernda þær og þeirri aðferð sem viðhöfð verður við vinnslu þeirra.

9.3 Áhættumat

Ábyrgðaraðili gerir skriflegt áhættumat. Áhættumat er mat á hættunni á því að óviðkomandi fái aðgang að persónuupplýsingum, geti breytt upplýsingunum eða skert öryggi þeirra að öðru leyti. Áhættumat tekur einnig til athugunar á umfangi og afleiðingum hættunnar m.t.t. eðlis þeirra persónuupplýsinga sem unnið er með. Markmið áhættumats er að skapa forsendur fyrir vali á öryggisráðstöfunum, sbr. III. kafla reglna þessara. Þá skal tilgreina hvað geti farið úrskeiðis, hvaða áhrif slíkt geti haft á öryggi upplýsinganna og hvaða líkur séu á slíku. Áhættumat skal endurskoðað reglulega.

9.4 Öryggisráðstafanir

Grunnskólar velja hvaða öryggisráðstafanir skulu viðhafðar í samræmi við III. kafla reglna nr. 299/2001 um öryggi persónuupplýsinga og setja fram skriflega lýsingu á þeim. Í lýsingunni skal m.a. koma fram afstaða ábyrgðaraðilans til þess hvað sé ásættanleg áhætta við vinnsluna. Þá skal rakið hvaða öryggisráðstöfunum verði beitt og hvernig þær verði útfærðar, þ.á m. við hönnun, þróun, rekstur, prófun og viðhald þess kerfis, þ.m.t. hugbúnaðar, sem notað verður við vinnslu upplýsinganna. Þar skal og tekið fram hvernig brugðist verði við áföllum í rekstri vinnslukerfisins, hvernig flutningi persónuupplýsinga milli vinnslukerfa verði hagað, þ. á m. mögulegum flutningi gagna milli ábyrgðar- og vinnsluaðila. Öryggisráðstafanir skal endurskoðað reglulega.

Ábyrgðaraðili skal gera viðeigandi öryggisráðstafanir og ber ábyrgð á því að vinnsla persónuupplýsinga séu í samræmi við lög, reglur og fyrirmæli Persónuverndar um hvernig tryggja skuli öryggi upplýsinga, þ.m.t. þá staðla sem hún ákveður. Markmið skipulags- og tæknilegra öryggisráðstafana er til að tryggja nægilegt öryggi og vernda persónuupplýsingar gegn ólöglegri eyðileggingu, gegn því að þær glatist eða breytist fyrir slysi, gegn óleyfilegum aðgangi og gegn allri annarri ólögmætri vinnslu. Við val öryggisráðstafana skal taka mið af áhættu af vinnslunni og eðli þeirra gagna sem verja á. Skulu þær tryggja nægilegt öryggi með hliðsjón af nýjustu tækni og kostnaði við framkvæmd þeirra. Sé persónuupplýsingum miðlað um internetið skal taka mið af þeirri auknu áhættu sem sú aðferð hefur í för með sér.

9.5 Öryggisráðstafanir varðandi starfsmannamál og fræðsla til starfsfólks

Í þeim tilgangi að fyrirbyggja og takmarka tjón af völdum mannlegra mistaka, þjófnaðar, svika og annarrar misnotkunar, skal ábyrgðaraðili grípa til þeirra öryggisráðstafana sem við eiga hverju sinni, t.d.:

1. Kanna feril umsækjenda um störf.
2. Fá skjalfestar þagnaryfirlýsingar starfsmanna. Í **fskj. 1** er fyrirmynd að yfirlýsingu um trúnaðar- og þagnarskyldu starfsfólks grunnskóla.
3. Skilgreina með skýrum hætti hlutverk og skyldur hvers starfsmanns sem hefur aðgang að persónuupplýsingum, þ.á m. hverjir beri ábyrgð á einstökum skráasöfnum.

4. Gera nauðsynlegar ráðstafanir til þess að starfsmönnum sé með reglubundnum hætti gerð grein fyrir starfsskyldum sínum og þeim afleiðingum sem það getur haft í för með sér að brjóta þær.

Grunnskólum ber að veita starfsfólki sem nýtir rafræn upplýsingakerfi reglubundna fræðslu 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. Lagt er til að fræðslan fari fram árlega og ávallt þegar nýr starfsmaður fær aðgang að rafrænu upplýsingakerfi.

Upplýsa ber starfsmenn um skráningu aðgerða þeirra í rafrænum upplýsingakerfum og setja reglur um notkun upplýsinga úr aðgerðaskrá. Upplýsa skal starfsfólk um að gæta skuli fullrar þagnarskyldu um meðferð persónuupplýsinga sem aflað er um nemendur í grunnskóla eða hafa fylgt barni úr leikskóla. Um þagnarskyldu starfsmanna sveitarfélaga fer samkvæmt 2. mgr. 57. gr. sveitarstjórnarlaga nr. 138/2011 og 12. gr. laga nr. 91/2008 um grunnskóla. Brot á þagnarskyldu varðar refsingu skv. 136. gr. almennra hegningarlaga. Þagnarskyldan helst þótt látið sé af starfi.

Óheimilt er að miðla persónuupplýsingum um nemendur til annarra en þeirra sem þess þurfa vegna starfa sinna.

Athygli er vakin á að fjaraðgangur eða skráning starfsfólks að rafrænum upplýsingakerfum kann að vera varhugaverður og getur skapað hættu á misnotkun kerfisins. Meginreglan skal því vera sú að starfsmönnum skuli ekki veittur aðgangur að rafrænum upplýsingakerfum utan starfsstöðvar.

9.6 Ytra öryggi

Í þeim tilgangi að fyrirbyggja og takmarka tjón af völdum óheimils aðgangs, skal ábyrgðaraðili grípa til þeirra öryggisráðstafana sem við eiga hverju sinni, t.d.:

1. Stýra aðgangi að húsnaði með úthlutun lykla, aðgangskorta o.þ.h.
2. Viðhafa öryggisvörslu, t.d. með öryggisvörðum, viðvörunarkerfum eða rafrænni vöktun.

9.7 Skipulagslegar og tæknilegar öryggisráðstafanir

Í þeim tilgangi að fyrirbyggja og takmarka tjón af völdum bilana og óheimils aðgangs að vinnslubúnaði, skal ábyrgðaraðili grípa til þeirra öryggisráðstafana sem við eiga hverju sinni, t.d.:

1. Stýra aðgangi að búnaði með úthlutun aðgangs- og lykilorða.
2. Dulkóða eða eyða persónuauðkennum, eða að setja númer í stað persónuauðkenna og varðveita greiningarlykil með trygghum hætti.
3. Tryggja rekjanleika uppfléttinga og vinnsluaðgerða.
4. Varðveita persónuupplýsingar á ónettengdri tölvu.
5. Takmarka aðgang að persónuupplýsingum við lesaðgang (uppfléttaaðgang), svo sem í þeim tilgangi að hindra óheimila eyðingu, afritun eða samkeyrslu.
6. Viðhafa virkar vírusvarnir.

9.8 Endurskoðun áhættumats og öryggisráðstafana

Endurskoðun áhættumats og öryggisráðstafana skal fara fram með reglubundnum hætti og þó eigi sjaldnar en á tveggja ára fresti.

9.9 Innra eftirlit

Grunnskólar skulu viðhafa innra eftirlit með vinnslu persónuupplýsinga til að ganga úr skugga um að unnið sé í samræmi við gildandi lög og reglur og þær öryggisráðstafanir sem ákveðnar hafa verið.

Innra eftirlit skal viðhaft með reglubundnum hætti. Tíðni eftirlitsins og umfang þess skal 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 framkvæmd eftirlitsins. Það skal þó eigi fara fram sjaldnar en árlega.

Ábyrgðaraðili skal sjá til þess að gerð sé skýrsla um hverja aðgerð sem er liður í innra eftirliti. Í slíkri skýrslu skal lýsa niðurstöðu hvers þáttar eftirlitsins. Skýrslur um innra eftirlit skal varðveita tryggilega. Persónuvernd hefur rétt til að aðgangs að þeim hvenær sem er. Persónuvernd getur sett frekari fyrirmæli um framkvæmd innra eftirlits og veitt undanþágu frá því að slíkt innra eftirlit skuli viðhaft eða takmarkað til hvaða þátta í vinnslunni það skuli taka.

10. Eyðing og leiðrétting

Samkvæmt IV. kafli. laga um persónuvernd og meðferð persónuupplýsinga ber ábyrgðaraðila skylda til að leiðrétta, eyða, bæta við eða stöðva notkun á röngum, villandi eða ófullkomnum persónuupplýsingum eða persónuupplýsingum sem skráðar hafa verið án heimildar. Um þessi atriði er fjallað í nefndum kafla persónuverndarlaganna, sbr. ákvæði 25. gr., 26. og 27. gr. laganna:

Leiðrétting og eyðing rangra og villandi persónuupplýsinga.

Ef skráðar hafa verið persónuupplýsingar sem eru rangar, villandi eða ófullkomnar, eða persónuupplýsingar hafa verið skráðar án tilskilinnar heimildar, skal ábyrgðaraðili sjá til þess að upplýsingarnar verði leiðréttar, þeim eytt eða við þær aukið ef umræddur annmarki getur haft áhrif á hagsmuni hins skráða. Hafi slíkum upplýsingum verið miðlað eða þær notaðar ber ábyrgðaraðila, eftir því sem honum er frekast unnt, að hindra að það hafi áhrif á hagsmuni hins skráða.

Ef eyðing eða breyting þeirra upplýsinga sem um ræðir í 1. mgr. er óheimil samkvæmt ákvæðum annarra laga getur Persónuvernd bannað notkun upplýsinganna.

Eyðing og bann við notkun persónuupplýsinga sem hvorki eru rangar né villandi.

Þegar ekki er lengur málefnaleg ástæða til að varðveita persónuupplýsingar skal ábyrgðaraðili óska eftir því að þeim verði eytt. Málefnaleg ástæða til varðveislu upplýsinga getur m.a. byggst á fyrirmælum í lögum eða á því að ábyrgðaraðili vinni enn með upplýsingarnar í samræmi við upphaflegan tilgang með söfnun þeirra.

Ef ákvæði annarra laga standa því ekki í vegi getur skráður aðili engu síður krafist þess að upplýsingum um hann skv. 1. mgr. sé eytt eða notkun þeirra bönnuð ef slíkt telst réttlætanlegt út frá heildstæðu hagsmunamati. Við slíkt hagsmunamat skal taka tillit til hagsmuna annarra, almennra persónuverndarhagsmuna, almannahagsmuna og þeirra aðgerða sem þörf er á til að verða við kröfunni.

Persónuvernd getur, bæði í einstökum tilvikum eða með setningu almennra reglna, bannað notkun slíkra upplýsinga eða mælt fyrir um eyðingu þeirra.

11. Varsla gagna og afhending til Þjóðskjalasafns

Grunnskólum ber að fylgja leiðbeiningum sveitarfélags um skjalavörslu.

Athygli er vakin á að skylt er þeim sem falla undir 1. og 2. mgr. laga um opinber skjalasöfn nr. 77/2014 að afhenda opinberu skjalasafni skjöl sín í samræmi við ákvæði laganna. Þeir afhendingarskyldu aðilar sem heyra undir stjórnsýslu ríkisins geta eingöngu afhent Þjóðskjalasafni Íslands skjöl sín. Afhendingarskyldir aðilar sem heyra undir stjórnsýslu sveitarfélags skulu afhenda Þjóðskjalasafni Íslands skjöl sín ef sveitarfélagið rekur ekki héraðsskjalasafn á eigin vegum eða á ekki aðild að slíku safni. Sveitarfélag sem afhendir Þjóðskjalasafni Íslands skjöl sín til vörslu greiðir fyrir vörslu þeirra samkvæmt gjaldskrá sem ráðherra setur.

12. Samningur við utanaðkomandi aðila um vinnslu persónuupplýsinga.

Skólastjóra er 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 um persónuvernd og meðferð persónuupplýsinga. Slíkt er þó háð því skilyrði að ábyrgðaraðili hafi áður sannreynt að umræddur vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit skv. 12. gr. laga um meðferð persónuupplýsinga og persónuvernd.

Samningur skv. framangreindu skal vera skriflegur og a.m.k. í tveimur eintökum. Þar skal m.a. koma fram að vinnsluaðili sé einungis heimilt að starfa í samræmi við fyrirmæli ábyrgðaraðila og að ákvæði laga þessara um skyldur ábyrgðaraðila gildi einnig um þá vinnslu sem vinnsluaðili annast. Ábyrgðaraðili og vinnsluaðili skulu hvor varðveita sitt eintak af samningnum.

Hverjum þeim er starfar í umboði ábyrgðaraðila eða vinnsluaðila, að vinnsluaðila sjálfum meðtöldum, og hefur aðgang að persónuupplýsingum, er aðeins heimilt að vinna með persónuupplýsingar í samræmi við fyrirmæli ábyrgðaraðila nema lög mæli fyrir á annan veg.

Hafi vinnsluaðili staðfestu í öðru ríki á Evrópska efnahagssvæðinu en ábyrgðaraðili, sbr. umfjöllun hér á eftir, skal jafnframt mælt svo fyrir í samningi að lög og reglur þess ríkis þar sem vinnsluaðili hefur staðfestu gildi um öryggisráðstafanir við vinnslu persónuupplýsinga. Getur Persónuvernd t.d. í auglýsingu í Stjórnartíðindum áskilið að slíkur samningur innihaldi stöðluð ákvæði sem séu í samræmi við ákvörðun framkvæmdastjórnar Evrópubandalagsins. Sama á við þegar ábyrgðaraðili hefur staðfestu í ríki á Evrópska efnahagssvæðinu en vinnsluaðili ekki fari vinnslan fram í landi eða á stöðum sem upp eru taldir í auglýsingu sem Persónuvernd gefur út.

Framangreint gildir einnig þegar vinnsluaðili á staðfestu í öðru aðildarríki stofnsamnings Fríverslunarsamtaka Evrópu en ábyrgðaraðili, sbr. umfjöllun hér á eftir og þegar ábyrgðaraðili hefur staðfestu í aðildarríki stofnsamnings Fríverslunarsamtaka Evrópu en vinnsluaðili ekki. Lögin gilda um vinnslu persónuupplýsinga á vegum ábyrgðaraðila sem hefur staðfestu hér á landi, enda fari vinnsla persónuupplýsinganna fram á Evrópska efnahagssvæðinu, [í aðildarríki stofnsamnings Fríverslunarsamtaka Evrópu] eða í landi eða á stöðum sem Persónuvernd auglýsir í Stjórnartíðindum.

Athygli er vakin á að þegar notaður er hugbúnaður sem vistar upplýsingar í skýjum við kennslu gæti þurft að haga að framangreindum ákvæðum persónuverndarlaganna. Bent er á fræðslu breskra skólayfirvalda um upplýsingaöryggi þegar kennsluhugbúnaður og upplýsingar eru vistaðar í tölvuskýi;

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557739/Cloud-services-software-dept-advice-July_23_2015.pdf

Auk þess er vísað til leiðbeininga til ríkisstofnana um notkun á tölvuskýjalausnum;

<https://www.fjarmalaraduneyti.is/media/frettatengt2016/Leidbeiningar-til-rikisstofnana-um-notkun-tolvuskyja-nov-2016.pdf>

Í **fskj. 2** má sjá leiðbeiningar um vinnslusamninga og í **fskj. 3** er fyrirmynd að vinnslusamningi grunnskóla. Sveitarfélag getur komið fram f.h. ábyrgðaraðila í sveitarfélaginu og útbúið sameiginleg fyrirmæli til handa vinnsluaðila, t.d. með gerð verklagsreglna sem gilda fyrir grunnskóla í viðkomandi sveitarfélagi.

13. Öryggisráðstafanir vinnsluaðila og sannreyning

Áður en grunnskóli gerir samning við tiltekinn aðila um að annast, í heild eða að hluta, þá vinnslu persónuupplýsinga sem hann ber ábyrgð á ber honum að sannreyna að umræddur vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit skv. 12. gr. laga um meðferð persónuupplýsinga og persónuvernd.

Sannreyning getur m.a. farið fram með þeim hætti óskað verði svara við tilgreindum spurningum og upplýsinga en sjá má fyrirmynd að bréfi til aðila sem fyrirhugað er að gera vinnslusamning við í **fskj. 4**.

FYLGISKJÖL

Fskj. 1, yfirlýsing um trúnaðar- og þagnarskyldu

Fskj. 2, leiðbeiningar varðandi vinnslusamninga

Fskj. 3, fyrirmynd að vinnslusamningi

Fskj. 4, Fyrirmynd að bréfi til aðila sem fyrirhugað er að gera við vinnslusamning

Fskj. 5, lög um persónuvernd og meðferð persónuupplýsinga.

Fskj. 6, reglur nr. 299/2001 um öryggi persónuupplýsinga.

Yfirlýsing um trúnaðar- og þagnarskyldu

Ég, undirrituð/undirritaður starfsmaður [grunnskóli] og notandi að rafrænu upplýsinga- og námskerfi sem til notkunar er í [grunnskóli], staðfesti hér með að mér er skylt að gæta þagmælsku um atriði, sem ég fæ vitneskju um í starfi mínu og leynt skulu fara samkvæmt lögum og fyrirmælum yfirmanna.

Þagnarskyldan nær til allrar vitneskju um skráða nemendur [nafn grunnskóla] og forsjármenn þeirra er varða heilbrigði, sjúkdóma, meðferð, persónuleg málefni og aðrar persónulegar upplýsingar í rafrænu upplýsinga- og námskerfi grunnskólans.

Þá mun ég gæta þess að vanda til allrar skráningar í rafrænt upplýsinga- og námskerfi [grunnskóli] og setja ekki þar inn atriði sem leynt skulu fara að lögum. Þá er mér jafnframt ljóst að mér er óheimilt að afla upplýsinga um nemendur og forsjármenn þeirra sem eru mér ekki nauðsynlegar starfs míns vegna og ber mér einnig að halda öllum skráningum í rafrænt upplýsinga- og námskerfi [grunnskóli] leyndum fyrir óviðkomandi.

Þagnarskylda þessi helst þótt ég láti af starfi mínu.

Að lokum er mér ljós ábyrgð mín samkvæmt lögum um persónuvernd og meðferð persónuupplýsinga nr. 77/2000 og geri mér grein fyrir að brot á þagnarskyldu varðar refsingu skv. 136. gr. almennra hegningarlaga nr. 19/1940.

Ég heiti því að virða þagnarskyldu þá sem lýst er hér að framan. Ég hef lesið og skilið þessa yfirlýsingu og samþykki hana.

Nafn

kennitala

netfang

grunnskóli

GERÐ VINNSLUSAMNINGS

Á grundvelli laga nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga, er aðila heimilt að útvista skráarhaldi sínu til þriðja aðila.

Ábyrgðaraðili – hver grunnskóli

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 ber hann ábyrgðina, svo fremi hann hafi áfram ákvörðunarvaldið.

Vinnsluaðili – fyrirtæki sem sér um rekstur á rafrænu upplýsingakerfi

Vinnsluaðili er 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 en þar kemur fram að ábyrgðaraðili 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 þó háð því að ábyrgðaraðili hafi áður sannreynt að umræddur vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit. Það er einnig 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 vinnsluaðili 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.

Vinnslusamningur

Í vinnslusamningi milli ábyrgðaraðila og vinnsluaðila er nauðsynlegt að fjallað sé um eftirtalin atriði:

1. Lýsing á hlutverki og ábyrgð vinnsluaðila.
2. Lýsing á vinnslunni, s.s. hvaða gögn eru afhent vinnsluaðila, afhendingarmáta, afhendingartíma og uppfærsla upplýsinga.
3. Gerð sjálfstæðs og aðgreinds gagnagrunns vegna vinnslu upplýsinga fyrir hvern og einn ábyrgðaraðila, séu þeir fleiri en einn.
4. Upplýsingar um skráningarsnið og aðrar nauðsynlegar upplýsingar um tæknilýsingar og tæknisniðfleti.
5. Öryggi vinnslunnar og að vinnsluaðili uppfylli kröfur samkvæmt 11. gr. laga, nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga, sbr. og reglur nr. 299/2001, um öryggi persónuupplýsinga.
6. Tilgreining á þeim grunnupplýsingum sem vinnslan lýtur að.
7. Hafi vinnsluaðili heimild ábyrgðaraðila til að skrá breytingar á grunnupplýsingum skal þeim miðlað aftur til ábyrgðaraðila.
8. Miðlun upplýsinga til þriðja aðila er óskar aðgangs, afhendingarmáta, afhendingartíma og uppfærslu upplýsinganna.
9. Bann vinnsluaðila við að nýta upplýsingar í öðrum tilgangi en símaskrá og upplýsingaþjónustu fyrir símanúmer.

Varðandi núgildandi samninga

Í kjölfar álits Persónuverndar í máli nr. 2015/1203, frá 23. september 2015 hefur mennta- og menningarmálaráðuneytið á grundvelli yfirstjórnunar- og eftirlitsheimilda sinna sem eiga sér stoð í 4.

gr. grunnskólalaga nr. 91/2008 og Persónuvernd gert þá kröfu til grunnskóla landsins, sem ábyrgðaraðila um meðferð persónuupplýsinga að gerðir verða nýir vinnslusamningar við vinnsluaðila þar sem „nytjaleyfis- og þjónustusamningur“ við Mentor fullnægir ekki skilyrðum 13. gr. laga nr. 77/2000 um gerð og efni vinnslusamnings. Byggir sú afstaða Persónuverndar einkum á því að enginn skólanna kom að gerð samningsins, enginn skólanna sannreynði fyrir undirritun samningsins að Mentor ehf. gæti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit skv. 12. gr. sömu laga. 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.

Bent er á að rétt er að skoða núgildandi samning grunnskóla og vinnsluaðila og meta þörf á uppsögn hans áður en kemur til gerðar nýs samnings. Verið getur að núgildandi samningur við vinnsluaðila geti haldið gildi sínu en að gerður verði sérstakur vinnslusamningur.

Í ljósi framangreinds lítur Persónuvernd svo á að afhending umræddra persónuupplýsinga til Mentor ehf. í gegnum vefkerfið Mentor er ekki talin samrýmast ákvæðum laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga og beinir þeim tilmælum til hvers og eins grunnskóla að sannreyna fyrir undirritun vinnslusamnings að vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og að vinnslusamningur uppfylli að lágmarki þau skilyrði sem nefnd hafa verið hér fyrir í erindi þessu.

Virðingarfyllst,

Samningur milli ábyrgðaraðila persónuupplýsinga og vinnsluaðila persónuupplýsinga

Inngangur

Samningur þessi, á milli ábyrgðaraðila persónuupplýsinga og vinnsluaðila persónuupplýsinga er gerður á grundvelli 13. gr. laga um persónuvernd og meðferð persónuupplýsinga, nr. 77/2000. Vinnsluaðila, eða þeim sem starfar í umboði hans, er einungis heimilt að starfa í samræmi við fyrirmæli ábyrgðaraðila og í samræmi við gildandi lög og reglur. Að öðru leyti gilda ákvæði laga um persónuvernd og meðferð persónuupplýsinga, nr. 77/2000 um samning þennan og reglugerð nr. 299/2001 um öryggi persónuupplýsinga, eftir því sem við á og trúnaðarskyldur vinnsluaðila við meðferð persónuupplýsinga.

1. Lögmæti og heimild til vinnslu persónuupplýsinga í [heiti vefkerfis]

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.

Allir grunnskólar landsins sem eru ábyrgðaraðilar samkvæmt samningi þessu, hafa heimild á grundvelli 1. mgr. 8. gr. laga nr. 77/2000 að skrá tilteknar persónuupplýsingar um nemendur í rafrænt upplýsingakerfi. Hér er um að ræða grunnupplýsingar um nemanda.

Á grundvelli reglugerðar nr. 897/2009, lögum nr. 91/2008 um grunnskóla og 9. gr. laga nr. 77/2000, er ábyrgðaraðilum einnig heimilt að skrá viðkvæmar persónuupplýsingar um nemendur eða aðstandendur þeirra í rafræn upplýsingakerfi.

Gæta ber að því að skráningar séu málefnalegar, sanngjarnar og í samræmi við vandaða vinnsluhætti persónuupplýsinga. Skólastjóri viðkomandi grunnskóla skal hafa eftirlit með framangreindum upplýsingum skv. 9. gr. reglugerðar nr. 897/2009. Skólastjóri getur hvenær sem honum hentar sent [Heiti fyrirtækis] skriflegar spurningar sem tengjast verklagi og/eða ráðstöfunum og öðrum atriðum sem talin eru nauðsynleg til að uppfylla samning þennan og lagaskyldu.

2. Aðilar samnings – ábyrgðaraðili og vinnsluaðili

Aðilar samnings þessa eru:

Ábyrgðaraðili persónuupplýsinga: [Heiti grunnskóla], kt. [xxxxxx-xxxx], [heimilisfang og póstfang], í samningi þessum nefndur ábyrgðaraðili.

Vinnsluaðili persónuupplýsinga: [Heiti fyrirtækis], kt. [xxxxxx-xxxx], [heimilisfang og póstfang], í samningi þessum nefndur vinnsluaðili.

3. Tilgangur vinnslu og tegundir upplýsinga

Tilgangur vinnslu persónuupplýsinga er að uppfylla lagaskyldu samkvæmt ákvæði 2. mgr. 18. gr. laga nr. 91/2008 um grunnskóla.

Eftir fyrirmælum ábyrgðaraðila og á grundvelli samnings þessa hefur vinnsluaðili aðgang og heimild til þess að vinna með persónuupplýsingar um nemendur á vegum ábyrgðaraðila. Skuldbindur [Heiti fyrirtækis] sig til að vinna með og meðhöndla umræddar upplýsingar í samræmi við skilmála samningsins, eftirfarandi upplýsingar:

Grunnupplýsingar:

Um er að ræða grunnupplýsingar um nemanda, þ.e. nafn, kennitölu, heimilisfang og tengiliðaupplýsingar um nánustu aðstandendur, einkunnir, fjarvistir, heimavinnu og almenna umfjöllun um atburði sem eiga sér stað á skólatíma.

Viðkvæmar persónuupplýsingar:

Um er að ræða viðkvæmar persónuupplýsingar, t.d. um greiningar eða heilsufar, um nemendur eða aðstandendur þeirra í rafræn upplýsingakerfi.

4. Skilgreiningar

Um samning þennan er hvort tveggja notuð heitin „samningur“ eða „vinnslusamningur.“

Samningur þessi inniheldur samskonar skilgreiningar og finna má í ákvæðum laga um persónuvernd og meðferð persónuupplýsinga, nr. 77/2000, reglugerð nr. 897/2009 um miðlun og meðferð upplýsinga um nemendur í grunnskólum og rétt foreldra til aðgangs að upplýsingum um börn sín og reglugerð nr. 299/2001 um öryggi persónuupplýsinga, sbr. neðangreint:

- a) **Ábyrgðaraðili** persónuupplýsinga (ábyrgðaraðili) er sá aðili sem ákveður tilgang og vinnslu persónuupplýsinga, þann búnað sem notaður er, aðferð við vinnsluna og aðra ráðstöfun upplýsinganna. Sá grunnskóli sem notast við rafrænt upplýsingakerfi til þess að skrá upplýsingar um nemendur sína í vefkerfið sem síðan eru færðar inn í grunn **[heiti fyrirtækis]** er ábyrgðaraðili.
- b) **Vinnsluaðili** persónuupplýsinga (vinnsluaðili) er sá aðili sem vinnur persónuupplýsingarnar á vegum ábyrgðaraðila. **[Heiti fyrirtækis]**, sem hýsingar- og rekstraraðili vefkerfisins **[heiti vefkerfis]**, er vinnsluaðili sem vinnur með persónuupplýsingarnar á vegum hvers ábyrgðaraðila, þ.e. hvers grunnskóla sem notar vefkerfið **[heiti vefkerfis]**.
- c) **Vinnsla** er sérhver aðgerð eða röð aðgerða þar sem unnið er með persónuupplýsingar, hvort heldur sem vinnslan er handvirk eða rafræn.
- d) **Persónuupplýsingar** vísa til sérhverja persónugreindra eða persónugreinanlegra upplýsinga um hinn skráða, þ.e. upplýsingar sem beint eða óbeint má rekja til tiltekins einstaklings.
- e) **Viðkvæmar persónuupplýsingar** teljast til upplýsinga um uppruna, litarhátt, kynþátt og trúar- eða lífsskoðanir. Til viðkvæmra persónuupplýsinga teljast einnig upplýsingar um heilsuhagi, þ. á m. um lyfja-, áfengis- og vímuefnanotkun og hvers kyns ákvarðanir sem afmarka rétt og/eða skyldur eins eða fleiri tilgreindra aðila.

5. Gildissvið og markmið samnings

Samningur þessi hefur það markmið að uppfylla ákvæði 13. gr. laga um persónuvernd og meðferð persónuupplýsinga samkvæmt lögum nr. 77/2000 þar sem m.a. er kveðið á um gerð skriflegs samnings á milli ábyrgðaraðila og vinnsluaðila um vinnslu persónuupplýsinga að uppfylltum viðeigandi öryggisráðstöfunum.

Samningur þessi, sem gerður er á milli ábyrgðaraðila og vinnsluaðila snýr að þeirri þjónustu sem vinnsluaðili mun inna af hendi fyrir ábyrgðaraðila og hvaða vinnsluþætti vinnsluaðili ábyrgist að framkvæma.

Samkvæmt samningi þessum ber vinnsluaðila að sannreyna og tryggja að hann geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit vegna þeirra persónuupplýsinga sem ábyrgðaraðili ber ábyrgð á og hefur frumkvæði að því að óska eftir að vinnsluaðili vinni.

Vinnsluaðila er einungis heimilt að vinna þær persónuupplýsingar sem ábyrgðaraðili felur honum, í samræmi við fyrirmæli ábyrgðaraðila og í samræmi við vinnslusamninginn.

Notkun hugbúnaðarins fellur m.a. undir lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga.

6. Trúnaður

Öll gögn, þ. á m. persónuupplýsingar um nemendur og aðstandendur þeirra, og aðrar upplýsingar sem **[Heiti fyrirtækis]** hefur aðgang að frá ábyrgðaraðila eða er með öðrum hætti látið í té frá ábyrgðaraðila, nefnast einu nafni „trúnaðarupplýsingar“.

Með því að undirrita samning þennan lýsir **[Heiti fyrirtækis]** því yfir gagnavart ábyrgðaraðila að fyrirtækið muni gæta fyllsta trúnaðar varðandi allar þær upplýsingar sem það fær aðgang að eða vitneskju um hjá ábyrgðaraðila og tengjast rekstri viðkomandi grunnskóla.

7. Notkun og meðferð trúnaðarupplýsinga

Þagnarskylda

Allir starfsmenn vinnsluaðila skulu bundnir þagnarskyldu um hvaðeina sem þeir fá vitneskju um í starfi sínu og leynt skal fara samkvæmt lögum, fyrirmælum eða eðli máls. Vinnsluaðili skuldbindur sig til að sjá til þess að undirverktakar og starfsmenn hans séu einnig bundnir slíkri skyldu.

Trúnaðarskylda

Vinnsluaðili og starfsmenn hans skulu virða trúnaðarskyldu sína við meðferð persónuupplýsinga og láta þriðja aðila aldrei í té trúnaðarupplýsingar um vinnslu persónuupplýsinga nema þegar lög kveða á um slíkt eða ábyrgðaraðili óski þess sérstaklega.

Ábyrgðaraðili veitir vinnsluaðila leyfi til vinnslu og meðferð persónuupplýsinga og meðferð viðkvæmra persónuupplýsinga á nemendum í **[nafn grunnskóla]**, enda uppfyllir ábyrgðaraðili kröfur Persónuverndar um öryggi og afritun gagna.

Báðum aðilum er heimilt að gefa trúnaðarupplýsingar til þeirra starfsmanna sem nauðsynlegt þykir vegna verks og einnig til þeirra ráðgjafa sem aðili verður að leita til við verk, enda tryggi hann að þeir gæti þagmælsku. Allir starfsmenn vinnsluaðila hafa skrifað undir trúnaðarsamning við fyrirtækið þar sem kveður á um þagmælsku.

[Heiti fyrirtækis] skal gera ráðstafanir til að kanna bakgrunn starfsmanna og verktaka, t.d. staðfesta upplýsingar um menntun og þá reynslu sem varða starfið og eftir því sem við á skila inn sakavottorði, í samræmi við ákvæði 7.-9. gr. laga nr. 77/2000. Jafnframt skal **[Heiti fyrirtækis]** viðhafa agaferli sem tekur á óheimilum aðgangi að gögnum og óheimilli notkun þeirra.

[Heiti fyrirtækis] er óheimilt að nýta trúnaðarupplýsingar frá ábyrgðaraðila í öðrum tilgangi en samningur þessi tilgreinir.

8. Öryggi trúnaðarupplýsinga

Vinnsluaðila er skylt að viðhafa viðeigandi öryggisráðstafanir til að tryggja öryggi upplýsinga frá ábyrgðaraðila og vernda þær gegn ólöglegri eyðileggingu, gegn því að þær glatist eða breytist fyrir slysn, gegn óleyfilegum aðgangi og gegn allri annarri ólögmati vinnslu.

Jafnframt er [nafn fyrirtækis] skyld að tryggja öryggi starfsstöðva, pappírgagna, gagnavera, afritunarkerfa, netþjóna, tölvukerfa og færanlegra geymslumiðla eins og farsíma sem geymt geta upplýsingar.

Vinnsluaðili skal tryggja að öll meðferð upplýsinga sem aflað er við framkvæmd samnings þessa sé í samræmi við lög um persónuvernd og verndun persónuupplýsinga nr. 77/2000.

Meðal þeirra ráðstafana sem [heiti fyrirtækis] er skyld að fara eftir eru eftirfarandi:

Vírusvarnir o.fl.

- a) Notkun eldveggja og vírusvarna á þeim tölvum sem notaðar eru til að tengjast kerfum ábyrgðaraðila. Þessum hugbúnaði skal viðhaldið eins og kostur er.
- b) Að bregðast tafarlaust við tölvuvírusum eða spilli hugbúnaði þegar hann uppgötvast með því að láta tengiliði sína hjá ábyrgðaraðila vita strax og varast að opna skjöl sem gætu verið sýkt.

Aðgangsstýring kerfa

- a) Óheimilt er að lána öðrum aðgang sinn að kerfum ábyrgðaraðila, hvort sem það eru samstarfsmenn [heiti fyrirtækis] eða starfsmenn ábyrgðaraðila.
- b) Starfsmaður ábyrgðaraðila getur ekki skráð sig inn á fjaraðgang þegar hann er ekki á starfsstöð sinni.
- c) Lykilorð má ekki skrifa niður þannig að óviðkomandi gæti komist yfir lykilorðið.
- d) Lykilorð eiga að uppfylla eftirfarandi skilyrði:
 - Bæði há- og lágstafir
 - Tölustafir
 - Sami stafur/tala ekki tvisvar sinnum í röð
 - 8 stafir á lengd eða meira
- e) Þegar farið er frá starfsstöð skal starfsmaður ávallt aftengjast eða læsa skjá.
- f) Starfsmaður [heiti fyrirtækis] ber fulla ábyrgð á þeim aðgangi sem honum er veittur og afleiðingum þess ef aðrir komast yfir aðgang hans.
- g) Aðgangsorðum skal tafarlaust breytt ef starfsmaður telur að aðrir viti um aðgangsorðið eða ef hann tekur eftir einhverju óvanalegu í tölvukerfinu.

Öryggi gagna og hugbúnaðar

- a) [Heiti fyrirtækis] er óheimill aðgangur að tölvukerfum ábyrgðaraðila eða tölvutækum upplýsingum og gögnum án viðeigandi heimildar. Enn fremur er þeim óheimilt að gera ósamþykktar breytingar á efni tölvukerfa ábyrgðaraðila, þar á meðal að eyða eða breyta gögnum.
- b) Kæmi upp sú staða að [Heiti fyrirtækis] þyrfti að varðveita gögn frá ábyrgðaraðila, t.d. í þeim tilvikum sem starfsmenn hafa prentað út upplýsingar á starfsstöð ábyrgðaraðila eða skráð upplýsingar á pappír eða í tölvu, ber [Heiti fyrirtækis] að gæta þess að varðveita slíkar trúnaðarupplýsingar frá ábyrgðaraðila á öruggum stað.
- c) Skyldi [Heiti fyrirtækis] þurfa að senda trúnaðarupplýsingar um almenningsnet eða þráðlaus net skal [Heiti fyrirtækis] gæta að dulritun slíkra gagna fyrir sendingu. Þetta gæti átt við trúnaðargögn send til ábyrgðaraðila með tölvupósti eða innskráningu á kerfi ábyrgðaraðila frá útstöð sem er tengd yfir þráðlaus net. Slíka dulkóðun má koma á með notkun dulkóðaðra vpn sambanda eða notkun dulkóðunar í þráðlausum samskiptum.

Efnislegt öryggi

- a) Tryggja skal að öll gögn í umsjá [Heiti fyrirtækis] séu varin gegn þjófnaði og skemmdum, hvort sem er af ásetningi, fyrir slysi eða af öðrum orsökum, s.s. af völdum náttúruafla. Meðal ráðstafana sem [Heiti fyrirtækis] ætti að nota í þessu samhengi eru þjófavarnakerfi, læsingar að vinnusvæðum og/eða starfsstöðvum fyrirtækisins og/eða notkun aðgangskortakerfis.
- b) Ef tölvubúnaður glatast, skemmist eða er stolið skal það tilkynnt strax.

- c) Ekki skal veita óviðkomandi aðgang að lokuðum svæðum.
- d) Aðgangsbúnaður, aðgangskort eða aðgangslyklar starfsmanna, skuli geymdir á öruggum stað.

Öryggisatvik

- a) Ef öryggisatvik kemur upp hjá [Heiti fyrirtækis] sem talið er geta haft áhrif á öryggi upplýsinga ábyrgðaraðila skal upplýsa ábyrgðaraðila um slíkt umsvifalaust. Með öryggisatviki er átt vði atvik eins og öryggisbrot, innbrot í tölvukerfi eða húsnæði, óviljaverk, óheimilan aðgang eða veikleika í kerfum.
- b) [Heiti fyrirtækis] skal afhenda ábyrgðaraðila skriflega skýrslu um atvikið, eigi síðar en sjö dögum frá því að öryggisatvikið átti sér stað, þar sem fram kemur nánari lýsing, hvaða aðgerða verði gripið til svo atvikið endurtaki sig ekki og innan hvaða tímamarka.

Vinnsluaðili og starfsmenn hans skulu kynna sér öryggisstefnu ábyrgðaraðila: [tengill inn á öryggisstefnu grunnskólans ef hún er fyrir hendi]

Vinnsluaðili skal beita 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.

Vinnsluaðili skal vera reiðubúinn að fara að áliti eða ákvörðun Persónuverndar um aðgerðir sem uppfylla öryggiskröfur laga um meðferð persónuupplýsinga. Vinnsluaðili er óheimilt að láta af hendi persónuupplýsingar eða vitneskju um vinnslu þeirra án þess að fyrir liggi skrifleg heimild frá ábyrgðaraðila.

Ábyrgðaraðili er heimilt að ganga úr skugga um að vinnsluaðili viðhafi þær öryggisráðstafanir sem að framan getur. Vinnsluaðili er skylt að veita eðlilega aðstoð við slíkt eftirlit.

9. Bótaábyrgð

Vinnsluaðili getur sjálfur borið bótaábyrgð á verkum sem hann einn hefur ákveðið og ekki rúmast innan samnings þessa. Þá getur stofnast refsíábyrgð hjá honum, bæði vegna brota gegn lögum nr. 77/2000 og öðrum lögum, s.s. um þagnarskyldu.

Ábyrgðaraðili getur gert fjárkröfu á hendur vinnsluaðila vegna tjóns eða stjórnvaldssektar sem hugbúnaðurinn kann að valda með beinum eða óbeinum hætti, enda sé ekki um að ræða ásetning eða stórkostlegt gáleysi af hans hálfu.

10. Ábyrgð

Vinnsluaðili ber ábyrgð á framkvæmd samnings þessa og tekur að sér að tryggja fullnægjandi starfsemi og öryggisráðstafanir er varðar alla þá þjónustubætti sem samningurinn nær til. Jafnframt skuldbindur hann sig til að uppfylla öll þau skilyrði og kröfur sem gerðar eru til starfseminnar og vinnslusamningurinn fjallar um og fara eftir þeim lögum, reglum og stöðlum sem við eiga um starfsemina.

Miðað er við að vinnsluaðili annist fyrst og fremst sjálfur með eigin starfsliði skipulagningu, stjórnun og stefnumótun þjónustunnar. Vinnsluaðili er þó heimilt að ráða undirverktaka til að annast tiltekin verkefni við framkvæmd samnings þessa eða hluta þjónustunnar. Vinnsluaðili ber ábyrgð á framkvæmd verka undirverktaka og aðstoðarfólks hans gagnvart ábyrgðaraðila.

Vinnsluaðili skal bæta ábyrgðaraðila þann skaða sem ábyrgðaraðili verður fyrir og leiðir af meðferð vinnsluaðila á upplýsingum sem stangast á við gildandi lög og reglur, fyrirmæli ábyrgðaraðila eða vinnslusamninginn.

11. Lok á vinnslu persónuupplýsinga

Þegar skólagöngu barns er lokið og ekki eru lengur fyrir hendi málefnalegar ástæður til varðveislu upplýsinga um það skal sá aðili sem falin er meðferð og varsla upplýsinga, þ.e. héraðsskjalasafn eða Þjóðskjalasafn Íslands, annast meðferð þeirra í samræmi við fyrirmæli laga um Þjóðskjalasafn Íslands og fyrirmæli sett samkvæmt þeim.

Vinnsluaðili skal innan tveggja vikna frá tilkynningu, afhenda ábyrgðaraðila öll gögn um viðkomandi nemanda/nemendur sem síðan verða afhentar opinberu skjalasafni til varanlegrar varðveislu.

Þegar vinnsluaðili hefur afhent ábyrgðaraðila öll gögn, skal vinnsluaðili farga þeim upplýsingum sem hann á að hætta að vinna að beiðni ábyrgðaraðila.

12. Vanefndir, vanefndaúrræði og varnarþing

Uppfylli vinnsluaðili ekki skyldur sínar samkvæmt samningi þessum eða samkvæmt álitni eða ákvörðun Persónuverndar, getur ábyrgðaraðili með tilkynningu krafist tafarlausra úrbóta og sett hæfilega tímafresti.

Hafi vinnsluaðili ekki bætt úr annmörkum samkvæmt tilkynningu innan tímafrests hefur ábyrgðaraðili heimild til að fresta greiðslum eða beita öðrum vanefndaúrræðum laga þar til úrbætur hafa sannanlega verið gerðar. Vinnsluaðili á ekki rétt á dráttarvöxtum þótt greiðslum sé frestað samkvæmt þessari grein.

Ef vinnsluaðili vanefnir frekar samningsskyldur sínar getur ábyrgðaraðili rift samningnum. Samningi þessum verður þó ekki rift nema vanefnd sé veruleg enda hafi ábyrgðaraðili áður gert vinnsluaðila viðvart með skriflegri tilkynningu og sett honum hæfilegan frest til úrbóta.

Mál er kunna að rísa vegna brota og vanefnda á samningi þessum skulu rekin fyrir Héraðsdómi Reykjavíkur.

13. Gildistaka, gildistími, endurnýjun og uppsögn

Samningur þessi öðlast gildi við undirritun og skal þá vinnsluaðili taka við öllum réttindum og skyldum samkvæmt vinnslusamningi þessum.

Samningurinn er ótímabundinn en er uppsegjanlegur af beggja hálfu með eins mánaðar fyrirvara og er uppsögnin bundin við mánaðarmót. Uppsögn skal vera skrifleg.

Segi ábyrgðaraðili upp samningi við vinnsluaðila er lokað á hugbúnaðinn 30 dögum eftir móttöku uppsagnar á samningi. Áður en vinnsluaðili lokar á notkun hugbúnaðarins skal ábyrgðaraðili fá gögn sín afhent á rafrænu formi.

Tilkynningar sem samningsaðilar þurfa að beina hvor til annars samkvæmt samningi þessum skulu vera skriflegar. Skal hvor aðili um sig tilnefna formlegan tengilið sem beina má slíkum orðsendingum til með pósti, tölvupósti eða símbréfi.

Telji samningsaðili forsendur samningsins breytast getur hann farið fram á viðræður um endurskoðun á einstaka ákvæðum samningsins á samningstímabilinu.

Samningur þessi er gerður í tveim eintökum og varðveiti hvor samningsaðili sitt eintak.

Staður og dags.

f.h. vinnsluaðila,
[heiti fyrirtækis],

f.h. ábyrgðaraðila,
[grunnskólans (þgf.)]

[Nafn, kt.]

[Nafn, kt.]

.....
Staður og dagsetning

.....
Nafn fyrirtækis/stofnunar

.....
Undirritun

.....
Nafn/Nöfn í bókstöfum

Til: [Vinnsluaðili]

Frá: [Nafn grunnskóla]

[staðsetning], [dagsetning] 2016

Efni: Staðfesting á því að vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og innra eftirlit í samræmi við 11.-13. gr. laga um persónuvernd og meðferð persónuupplýsinga nr. 77/2000 og reglur Persónuverndar nr. 299/2001 um öryggi persónuupplýsinga.

Skv. 13. gr. laga um persónuvernd og meðferð persónuupplýsinga nr. 77/2000 er ábyrgðaraðili heimilt að semja við tiltekinn aðila um að annast, í heild eða að hluta, þá vinnslu persónuupplýsinga sem hann ber ábyrgð á samkvæmt ákvæðum laganna. Slíkt er þó háð því skilyrði að ábyrgðaraðili hafi áður sannreynt að umræddur vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit skv. 12. gr. laganna.

Í tengslum við samning aðila um vinnslu persónuupplýsinga vegna [nafn grunnskóla] vegna viðræðna um samning aðila um vinnslu persónuupplýsinga nemenda í [nafn grunnskóla] er óskað eftir upplýsingum og gögnum er staðreyna eftirfarandi þætti:

1. Er upplýsingaöryggisstefna kynnt innan fyrirtækisins?
2. Hefur ábyrgð og völdum hvað varðar upplýsingaöryggi verið úthlutað eftir hlutverkum og hefur upplýsingum um þau verið miðlað?
3. Er ferlið við áhættumat skjalað þar með talið viðmið fyrir áhættusamþykki og viðmið fyrir framkvæmd áhættumats?
4. Er starfsfólk meðvitað um upplýsingaöryggisstefnu skólans, hvaða hlutverk það hefur og afleiðingar þess að ekki fara eftir kröfum stjórnunarkerfis um upplýsingaöryggi?
5. Er til ferill fyrir miðlun upplýsinga tengdum upplýsingaöryggi þar með talið ábyrgðir og hverju eigi að miðla?
6. Eru þær áhættur sem borin hafa verið kennsl á, eigendur þeirra, líkur, afleiðingar og áhættustig – niðurstöður skjalaðar?
7. Er rýni stjórnenda framkvæmd reglulega og eru niðurstöðurnar skjalaðar í fundargerð?
8. Eru til reglur sem skilgreina hvernig upplýsingar skólans eru verndaðar á fjarvinnustöðvum?
9. Eru gerðar ferilkannanir á starfsumsækjendum og verktökum?
10. Er til stefna um aðgangsstýringu sem skilgreinir rekstar og öryggis kröfur fyrir aðgangsstýringu?
11. Er aðgangur að gagngrunnum og hugbúnaði takmarkaður í samræmi við stefnu um aðgangsstýringu?
12. Eru til og farið eftir skilgreindum vinnureglum fyrir örugg svæði?
13. Hafa notendur einungis aðgengi að þeim netkerfum og þjónustum sem þeir hafa sérstaklega fengið heimild fyrir?
14. Eru aðgengisréttindi veitt í gegnum formlegan skráningarferil?

15. Hafa aðgangsréttindi starfsmann og verktaka verið fjarlægð við starfslok eða samningslok?
16. Er til afritunarstefna; fer afritataka fram í samræmi við þessa stefnu?
17. Eru til formlegir ferlar fyrir breytingarstjórnun?
18. Eru persónugreinanlegar upplýsingar verndaðar einsog kveðið er á um í lögum og reglum?
19. Er rekjaneiki uppflættinga og vinnsluaðgerða tryggður?
20. Er vinnsluaðili með staðfestu á Evrópska efnahagssvæðinu?

Að öllu framangreindu virtu er jafnframt óskað eftir gögnum til stuðnings framangreindum svörum, svo sem öryggisstefnu, áhættumati og öðrum upplýsingum um öryggisráðstafanir sem gerðar hafa verið auka annarra gagna. Farið er fram á að umbeðnar upplýsingar berist innan 14 daga frá dagsetningu bréfs þessa.

Virðingarfyllst,



Lagasafn. Íslensk lög 1. nóvember 2016. Útgáfa 145b. Prenta í tveimur dálkum.

Lög um persónuvernd og meðferð persónuupplýsinga

2000 nr. 77 23. maí

Ferill málsins á Alþingi. Frumvarp til laga.

Tóku gildi 1. janúar 2001. *EES-samningurinn*: XI. viðauki tilskipun 95/46/EB, XIX. viðauki tilskipun 97/7/EB og XI. viðauki tilskipun 97/66/EB. *Breytt með* l. 90/2001 (tóku gildi 15. júní 2001; *EES-samningurinn*: XI. viðauki tilskipun 95/46/EB), l. 30/2002 (tóku gildi 16. apríl 2002), l. 81/2002 (tóku gildi 17. maí 2002; *EES-samningurinn*: XI. viðauki tilskipun 95/46/EB), l. 46/2003 (tóku gildi 7. apríl 2003) l. 72/2003 (tóku gildi 10. apríl 2003), l. 50/2006 (tóku gildi 1. júlí 2006), l. 77/2010 (tóku gildi 1. júlí 2010), l. 162/2010 (tóku gildi 1. jan. 2011), l. 126/2011 (tóku gildi 30. sept. 2011), l. 44/2014 (tóku gildi 1. jan. 2015 nema brákv. I sem tók gildi 29. maí 2014) og l. 77/2014 (tóku gildi 12. júní 2014).

Ef í lögum þessum er getið um ráðherra eða ráðuneyti án þess að málefnasvið sé tilgreint sérstaklega eða til þess vísað, er átt við **innanríkisráðherra** eða **innanríkisráðuneyti** sem fer með lög þessi. Upplýsingar um málefnasvið ráðuneyta skv. forsetaúrskurði er að finna hér.

I. kafli. Markmið, skilgreiningar og gildissvið.

■ 1. gr. Markmið.

☐ Markmið laga þessara er að stuðla að því að með persónuupplýsingar sé farið í samræmi við grundvallarsjónarmið og reglur um persónuvernd og friðhelgi einkalífs og að tryggja áreiðanleika og gæði slíkra upplýsinga og frjálst flæði þeirra á innri markaði Evrópska efnahagssvæðisins.

☐ Sérstök stofnun, Persónuvernd, annast eftirlit með framkvæmd laga þessara og reglna sem settar verða samkvæmt þeim, sbr. nánar ákvæði 36. gr.

■ 2. gr. Skilgreiningar.

☐ Merking orða og hugtaka í lögum þessum er sem hér segir:

1. *Persónuupplýsingar*: Sérhverjar persónugreindar eða persónugreinanlegar upplýsingar um hinn skráða, þ.e. upplýsingar sem beint eða óbeint má rekja til tiltekins einstaklings, látins eða lifandi.

2. *Vinnsla*: Sérhver aðgerð eða röð aðgerða þar sem unnið er með persónuupplýsingar, hvort heldur sem vinnslan er handvirk eða rafræn.

3. *Skrá*: Sérhvert skipulagsbundið safn persónuupplýsinga þar sem finna má upplýsingar um einstaka menn.

4. *Ábyrgðaraðili*: Sá aðili sem ákveður tilgang vinnslu persónuupplýsinga, þann búnað

sem notaður er, aðferð við vinnsluna og aðra ráðstöfun upplýsinganna.

5. *Vinnsluaðili*: Sá sem vinnur persónuupplýsingar á vegum ábyrgðaraðila.

6. [*Rafræn vöktun*]: Vöktun sem er viðvarandi eða endurtekin reglulega og felur í sér eftirlit með einstaklingum með fjarstýrðum eða sjálfvirkum búnaði, og fer fram á almannafæri eða á svæði sem takmarkaður hópur fólks fer um að jafnaði. Hugtakið tekur til:

a. vöktunar sem leiðir, á að leiða eða getur leitt til vinnslu persónuupplýsinga, og

b. sjónvarpsvöktunar sem fer fram með notkun sjónvarpsmyndavéla, vefmyndavéla eða annars samsvarandi búnaðar, án þess að fram fari söfnun myndefnis eða aðrar aðgerðir sem jafngilda vinnslu persónuupplýsinga.]¹⁾

7. *Samþykki*: Sérstök, ótvíræð yfirlýsing sem einstaklingur gefur af fúsum og frjálsum vilja um að hann sé samþykkur vinnslu tiltekinna upplýsinga um sig og að honum sé kunnugt um tilgang hennar, hvernig hún fari fram, hvernig persónuvernd verði tryggð, um að honum sé heimilt að afturkalla samþykki sitt o.s.frv.

8. *Viðkvæmar persónuupplýsingar*:

a. Upplýsingar um uppruna, litarhátt, kynþátt, stjórnmalaskoðanir, svo og trúar- eða aðrar lífsskoðanir.

b. Upplýsingar um hvort maður hafi verið grunaður, kærður, ákærður eða dæmdur fyrir refsiverðan verknað.

c. Upplýsingar um heilsuhagi, þar á meðal um erfðaeiginleika, lyfja-, áfengis- og vímuefnanotkun.

d. Upplýsingar um kynlíf manna og kynhegðan.

e. Upplýsingar um stéttarfélagsaðild.

9. *Sértæk ákvörðun*: Ákvörðun sem afmarkar rétt og/ eða skyldur eins eða fleiri tilgreindra einstaklinga.

¹⁾L. 46/2003, 1. gr.

■ 3. gr. *Efnislegt gildissvið*.

□ Lögin gilda um sérhverja rafræna vinnslu persónuupplýsinga. Lögin gilda einnig um handvirka vinnslu persónuupplýsinga sem eru eða eiga að verða hluti af skrá.

□ Ákvæði 16., 18.-21., 24., 26., 31. og 32. gr. laganna gilda ekki um vinnslu persónuupplýsinga sem varða almannaoðryggi, landvarnir, öryggi ríkisins og starfsemi ríkisins á sviði refsivörslu. Lögin gilda ekki um meðferð einstaklings á persónuupplýsingum sem eingöngu varða einkahagi hans eða eru einvörðungu ætlaðar til persónulegra nota.

■ 4. gr. [*Rafræn vöktun*].

□ Rafræn vöktun er ávallt háð því skilyrði að hún fari fram í málefnalegum tilgangi.

Rafræn vöktun svæðis þar sem takmarkaður hópur fólks fer um að jafnaði er jafnframt háð því skilyrði að hennar sé sérstök þörf vegna eðlis þeirrar starfsemi sem þar fer fram.

□ Vinnsla persónuupplýsinga sem á sér stað í tengslum við rafræna vöktun skal uppfylla ákvæði laga þessara.

□ Um sjónvarpsvöktun fer, auk ákvæðis 1. mgr., samkvæmt ákvæðum 7., 24., 40. og 41. gr. laganna, svo og eftir því sem við á ákvæðum 31., 32. og 38. gr. laganna.]¹⁾

¹⁾L. 46/2003, 2. gr.

■ 5. gr. *Tengsl við tjáningarfrelsi*.

□ Að því marki sem það er nauðsynlegt til að samræma sjónarmið um rétt til einkalífs annars vegar og tjáningarfrelsis hins vegar má víkja frá ákvæðum laganna í þágu

fjölmiðlunar, lista eða bókmennta. Þegar persónuupplýsingar eru einvörðungu unnar í þágu fréttamennsku eða bókmenntalegrar eða listrænnar starfsemi gilda aðeins ákvæði 4. gr., 1. og 4. tölul. 7. gr., 11.–13. gr. og 24., 28., 42. og 43. gr. laganna.

■ **6. gr.** *Landfræðilegt gildissvið.*

□ [Lögin gilda um vinnslu persónuupplýsinga á vegum ábyrgðaraðila sem hefur staðfestu hér á landi, enda fari vinnsla persónuupplýsinganna fram á Evrópska efnahagssvæðinu, [í aðildarríki stofnsamnings Fríverslunarsamtaka Evrópu]¹⁾ eða í landi eða á stöðum sem Persónuvernd auglýsir í Stjórnartíðindum.²⁾

□ [Lögin gilda einnig um vinnslu persónuupplýsinga þótt ábyrgðaraðili hafi hvorki staðfestu í ríki á Evrópska efnahagssvæðinu né í aðildarríki stofnsamnings Fríverslunarsamtaka Evrópu ef hann notar tæki og búnað sem er hér á landi.]¹⁾

□ Lögin gilda einnig um vinnslu upplýsinga um fjárhagsmálefni og lánstraust lögaðila, sbr. 45. gr. laganna, enda þótt ábyrgðaraðili hafi ekki staðfestu hér á landi, ef hann notar tæki og búnað sem er hér á landi.

□ Ákvæði 2. og 3. mgr. gilda ekki ef umræddur tækjabúnaður er einungis notaður til að flytja persónuupplýsingar um Ísland.

□ Þegar svo hagar til sem greinir í 2. og 3. mgr. skal ábyrgðaraðili tilnefna fulltrúa sinn sem hefur staðfestu hér á landi og gilda þá ákvæði laganna varðandi ábyrgðaraðila um þann fulltrúa eftir því sem við á.³⁾

¹⁾L. 72/2003, 5. gr. ²⁾Augl. 228/2010, sbr. augl. 108/2012, augl. 419/2013, augl. 1316/2013 og augl. 1036/2015. ³⁾L. 90/2001, 1. gr.

II. kafli. Almennar reglur um vinnslu persónuupplýsinga.

■ **7. gr.** *[Meginreglur um gæði gagna og vinnslu.]¹⁾*

□ Við meðferð persónuupplýsinga skal allra eftirfarandi þátta gætt:

1. að þær séu unnar með sanngjörnum, málefnalegum og lögmætum hætti og að öll meðferð þeirra sé í samræmi við vandaða vinnsluhætti persónuupplýsinga;

2. að þær séu fengnar í yfirlýstum, skýrum, málefnalegum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi, en frekari vinnsla í sagnfræðilegum, tölfraðilegum eða vísindalegum tilgangi telst ekki ósamrýmanleg að því tilskildu að viðeigandi öryggis sé gætt;

3. að þær séu nægilegar, viðeigandi og ekki umfram það sem nauðsynlegt er miðað við tilgang vinnslunnar;

4. að þær séu áreiðanlegar og uppfærðar eftir þörfum, persónuupplýsingar sem eru óáreiðanlegar eða ófullkomnar, miðað við tilgang vinnslu þeirra, skal afmá eða leiðrétta;

5. að þær séu varðveittar í því formi að ekki sé unnt að bera kennsl á skráða aðila lengur en þörf krefur miðað við tilgang vinnslu.

□ [Ábyrgðaraðili ber ábyrgð á því að vinnsla persónuupplýsinga uppfylli ávallt ákvæði 1. mgr.]¹⁾

¹⁾L. 90/2001, 2. gr.

■ **8. gr.** *[Almennar reglur um heimildir fyrir vinnslu persónuupplýsinga.]¹⁾*

□ Vinnsla persónuupplýsinga er því aðeins heimil að einhverjir eftirfarandi þátta séu fyrir hendi:

1. [hinn skráði hafi ótvírætt samþykkt vinnsluna eða veitt samþykki skv. 7. tölul. 2. gr.]¹⁾

2. vinnslan sé nauðsynleg til að efna samning sem hinn skráði er aðili að eða til að gera ráðstafanir að beiðni hins skráða áður en samningur er gerður;
3. vinnslan sé nauðsynleg til að fullnægja lagaskyldu sem hvílir á ábyrgðaraðila;
4. vinnslan sé nauðsynleg til að vernda brýna hagsmuni hins skráða;
5. vinnslan sé nauðsynleg vegna verks sem unnið er í þágu almannahagsmuna;
6. vinnslan sé nauðsynleg við beitingu opinbers valds sem ábyrgðaraðili, eða þriðji maður sem upplýsingum er miðlað til, fer með;
7. vinnslan sé nauðsynleg til að ábyrgðaraðili, eða þriðji maður eða aðilar sem upplýsingum er miðlað til, geti gætt lögmætra hagsmuna nema grundvallarréttindi og frelsi hins skráða sem vernda ber samkvæmt lögum vegi þyngra.

□ ...²⁾

□ [Persónuvernd getur heimilað vinnslu persónuupplýsinga í öðrum tilvikum en greinir í 1. og 2. mgr. ef sýnt þykir að brýnir almannahagsmunir eða hagsmunir einstaklinga, þar með taldir hagsmunir hins skráða, krefjist þess. Skal þá ótvírætt að þörfin fyrir vinnsluna vegi þyngra en tillitið til þess að hún fari ekki fram. Getur Persónuvernd bundið slík leyfi þeim skilyrðum sem hún metur nauðsynleg hverju sinni til að tryggja hagsmuni hins skráða.]¹⁾

¹⁾L. 90/2001, 3. gr. ²⁾L. 46/2003, 3. gr.

■ **9. gr.** [Sérstök skilyrði fyrir vinnslu viðkvæmra persónuupplýsinga.]¹⁾

□ [Vinnsla viðkvæmra persónuupplýsinga er óheimil nema uppfyllt sé eitthvert af skilyrðum 1. mgr. 8. gr. og enn fremur eitthvert af eftirfarandi skilyrðum:]¹⁾

1. hinn skráði samþykki vinnsluna;
2. sérstök heimild standi til vinnslunnar samkvæmt öðrum lögum;
3. ábyrgðaraðila beri skylda til vinnslunnar samkvæmt samningi aðila vinnumarkaðarins;
4. vinnslan sé nauðsynleg til að verja verulega hagsmuni hins skráða eða annars aðila sem ekki er sjálfur fær um að gefa samþykki sitt skv. 1. tölul.;
5. vinnslan sé framkvæmd af samtökum sem hafa stéttarfélagsleg markmið eða af öðrum samtökum sem ekki starfa í hagnaðarskyni, svo sem menningar-, líknar-, félagsmála- eða hugsjónasamtökum, enda sé vinnslan liður í lögmætri starfsemi samtakanna og taki aðeins til félagsmanna þeirra eða einstaklinga sem samkvæmt markmiðum samtakanna eru, eða hafa verið, í reglubundnum tengslum við þau; slíkum persónuupplýsingum má þó ekki miðla áfram án samþykkis hins skráða;
6. vinnslan taki einungis til upplýsinga sem hinn skráði hefur sjálfur gert opinberar;
7. vinnslan sé nauðsynleg til að krafa verði afmörkuð, sett fram eða varin vegna dómsmáls eða annarra slíkra laganauðsynja;
8. vinnslan sé nauðsynleg vegna læknismeðferðar eða vegna venjubundinnar stjórnsýslu á sviði heilbrigðisþjónustu, enda sé hún framkvæmd af starfsmanni heilbrigðisþjónustunnar sem bundinn er þagnarskyldu;
9. vinnslan sé nauðsynleg vegna tölfræði- eða vísindarannsóknar, enda sé persónuvernd tryggð með tilteknum ráðstöfunum eftir því sem við á.

□ [Þrátt fyrir að skilyrði 1. mgr. séu ekki uppfyllt er heimilt, í tengslum við framkvæmd rafrænnar vöktunar, að safna efni sem verður til við vöktunina, svo sem hljóð- og myndefni, með viðkvæmum persónuupplýsingum ef eftirfarandi skilyrði eru uppfyllt:

1. að vöktunin sé nauðsynleg og fari fram í öryggis- og eignavörsluskyni;
2. að það efni sem til verður við vöktunina verði ekki afhent öðrum eða unnið frekar nema með samþykki þess sem upptaka er af eða samkvæmt ákvörðun Persónuverndar; heimilt er þó að afhenda lögreglu efni með upplýsingum um slys eða refsiverðan verknað

en þá skal þess gætt að eyða öllum öðrum eintökum af efninu;

3. að því efni sem safnast við vöktunina verði eytt þegar ekki er lengur málefnaleg ástæða til að varðveita það, nema sérstök heimild Persónuverndar skv. 3. mgr. standi til frekari varðveislu.]²⁾

☐ Persónuvernd getur heimilað vinnslu viðkvæmra persónuupplýsinga í öðrum tilvikum en greinir í [1. og 2. mgr.]²⁾ telji hún brýna almannahagsmunum mæla með því. Persónuvernd bindur slíka heimild þeim skilyrðum sem hún telur nauðsynleg hverju sinni til að tryggja hagsmunum hinna skráðu.

☐ ...³⁾

☐ Persónuvernd leysir úr ágreiningi um hvort persónuupplýsingar skuli teljast viðkvæmar eða ekki.

¹⁾L. 90/2001, 4. gr. ²⁾L. 81/2002, 1. gr. ³⁾L. 44/2014, 36. gr.

■ 10. gr. Notkun kennitölu.

☐ Notkun kennitölu er heimil eigi hún sér málefnalegan tilgang og sé nauðsynleg til að tryggja örugga persónugreiningu. Persónuvernd getur bannað eða fyrirskipað notkun kennitölu.

■ 11. gr. [Áhættumat, öryggi og gæði persónuupplýsinga.

☐ Ábyrgðaraðili skal gera viðeigandi tæknilegar og skipulagslegar öryggisráðstafanir til að vernda persónuupplýsingar gegn ólöglegri eyðileggingu, gegn því að þær glatist eða breytist fyrir slysi og gegn óleyfilegum aðgangi.

☐ 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.

☐ Ábyrgðaraðili ber ábyrgð á því að áhættumat og öryggisráðstafanir við vinnslu persónuupplýsinga séu í samræmi við lög, reglur¹⁾ og fyrirmæli Persónuverndar um hvernig tryggja skuli öryggi upplýsinga, þ.m.t. þá staðla sem hún ákveður að skuli fylgt.

☐ Ábyrgðaraðili ber ábyrgð á því að áhættumat sé endurskoðað reglulega og öryggisráðstafanir endurbættar að því marki sem þörf krefur til að uppfylla ákvæði þessarar greinar.

☐ Ábyrgðaraðili skal skrá með hvaða hætti hann mótar öryggisstefnu, gerir áhættumat og ákveður öryggisráðstafanir. Skal Persónuvernd hafa aðgang að upplýsingum um framangreind atriði hvenær sem hún óskar.]²⁾

¹⁾Rgl. 299/2001, sbr. 551/2013. ²⁾L. 90/2001, 5. gr.

■ 12. gr. Innra eftirlit.

☐ [Ábyrgðaraðili skal viðhafa innra eftirlit með vinnslu persónuupplýsinga til að ganga úr skugga um að unnið sé í samræmi við gildandi lög og reglur og þær öryggisráðstafanir sem ákveðnar hafa verið.

☐ Innra eftirlit skal viðhaft með reglubundnum hætti. Tíðni eftirlitsins og umfang þess skal 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 framkvæmd eftirlitsins. Það skal þó eigi fara fram sjaldnar en árlega.

☐ Ábyrgðaraðili skal sjá til þess að gerð sé skýrsla um hverja aðgerð sem er liður í innra eftirliti. Í slíkri skýrslu skal lýsa niðurstöðu hvers þáttar eftirlitsins. Skýrslur um innra

eftirlit skal varðveita tryggilega. Persónuvernd hefur rétt til að aðgangs að þeim hvenær sem er.

□ Persónuvernd getur sett frekari fyrirmæli¹⁾ um framkvæmd innra eftirlits og veitt undanþágu frá því að slíkt innra eftirlit skuli viðhaft eða takmarkað til hvaða þátta í vinnslunni það skuli taka.]²⁾

¹⁾Rgl. 299/2001, sbr. 551/2013. ²⁾L. 90/2001, 6. gr.

■ **13. gr.** [Trúnaðarskylda vinnsluaðila við meðferð persónuupplýsinga.

□ Ábyrgðaraðila er 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 þessara. Slíkt er þó háð því skilyrði að ábyrgðaraðili hafi áður sannreynt að umræddur vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit skv. 12. gr. laga þessara.

□ Samningur skv. 1. mgr. skal vera skriflegur og a.m.k. í tveimur eintökum. Þar skal m.a. koma fram að vinnsluaðila sé einungis heimilt að starfa í samræmi við fyrirmæli ábyrgðaraðila og að ákvæði laga þessara um skyldur ábyrgðaraðila gildi einnig um þá vinnslu sem vinnsluaðili annast. Ábyrgðaraðili og vinnsluaðili skulu hvor varðveita sitt eintak af samningnum.

□ Hverjum þeim er starfar í umboði ábyrgðaraðila eða vinnsluaðila, að vinnsluaðila sjálfum meðtöldum, og hefur aðgang að persónuupplýsingum, er aðeins heimilt að vinna með persónuupplýsingar í samræmi við fyrirmæli ábyrgðaraðila nema lög mæli fyrir á annan veg.

□ Hafi vinnsluaðili staðfestu í öðru ríki á Evrópska efnahagssvæðinu en ábyrgðaraðili, sbr. 1. mgr. 6. gr., skal jafnframt mælt svo fyrir í samningi að lög og reglur þess ríkis þar sem vinnsluaðili hefur staðfestu gildi um öryggisráðstafanir við vinnslu persónuupplýsinga. Getur Persónuvernd t.d. í auglýsingu¹⁾ í Stjórnartíðindum áskilið að slíkur samningur innihaldi stöðluð ákvæði sem séu í samræmi við ákvörðun framkvæmdastjórnar Evrópubandalagsins. Sama á við þegar ábyrgðaraðili hefur staðfestu í ríki á Evrópska efnahagssvæðinu en vinnsluaðili ekki fari vinnslan fram í landi eða á stöðum sem upp eru taldir í auglýsingu sem Persónuvernd gefur út.]²⁾

□ [Ákvæði 4. mgr. gilda einnig þegar vinnsluaðili á staðfestu í öðru aðildarríki stofnsamnings Fríverslunarsamtaka Evrópu en ábyrgðaraðili, sbr. 1. mgr. 6. gr., og þegar ábyrgðaraðili hefur staðfestu í aðildarríki stofnsamnings Fríverslunarsamtaka Evrópu en vinnsluaðili ekki.]³⁾

¹⁾Augl. 228/2010. ²⁾L. 90/2001, 7. gr. ³⁾L. 72/2003, 6. gr.

■ **14. gr.** Frestur til að fullnægja skyldum.

□ Ábyrgðaraðili skal afgreiða erindi samkvæmt ákvæðum 16., 18., 22., 25., 26., 27. og 28. gr. svo fljótt sem verða má og eigi síðar en innan eins mánaðar frá móttöku þess.

□ Ef sérstakar ástæður valda því að ómögulegt er fyrir ábyrgðaraðila að afgreiða erindi innan eins mánaðar er honum heimilt að gera það síðar. Þegar svo hagar til skal ábyrgðaraðili innan mánaðarfrestsins gefa hlutaðeigandi skriflegar skýringar á ástæðum tafarinnar og hvenær svars sé að vænta.

■ **15. gr.** Greiðsla kostnaðar.

□ Verða skal við erindi samkvæmt ákvæðum 16., 18., 22., 25., 26., 27. og 28. gr. án þess að taka fyrir það sérstakt gjald. Þó má, ef um er að ræða mikinn kostnað, svo sem vegna

ljósritunar skjala, taka greiðslu fyrir samkvæmt gjaldskrá sem ákveðin er af [ráðherra]¹⁾ með reglugerð.

¹⁾L. 162/2010, 164. gr.

■ [15. gr. a. Heimilt er að afhenda opinberu skjalasafni upplýsingar, sem falla undir lög þessi, til varðveislu í samræmi við ákvæði laga um opinber skjalasöfn.]¹⁾

¹⁾L. 77/2014, 50. gr.

III. kafli. Upplýsingaréttur og upplýsingaskylda. Fræðslu- og viðvörðunarskylda. Réttur til rökstuðnings.

■ 16. gr. *Réttur til almennrar vitneskju um vinnslu persónuupplýsinga.*

□ Ábyrgðaraðila er skylt að veita hverjum sem þess óskar almenna vitneskju um þá vinnslu persónuupplýsinga sem fram fer á hans vegum.

□ Þeim sem þess óskar skal enn fremur, að því er varðar tiltekna tegund vinnslu, veitt vitneskja um eftirtalin atriði:

1. nafn og heimilisfang ábyrgðaraðila og eftir atvikum fulltrúa hans skv. 6. gr.;

2. hver ber daglega ábyrgð á því að fullnægt sé skyldum ábyrgðaraðila samkvæmt lögum þessum;

3. tilgang vinnslunnar;

4. skilgreiningu og aðra lýsingu á þeim tegundum persónuupplýsinga sem unnið er með;

5. hvaðan upplýsingar koma;

6. viðtakendur upplýsinga, þar á meðal um hvort ætlunin sé að flytja upplýsingar úr landi og þá til hverra.

□ Kröfu skv. 1. mgr. skal beint til ábyrgðaraðila, eða fulltrúa hans skv. 6. gr., og má krefjast skriflegrar greinargerðar um þau atriði sem óskað er vitneskju um.

■ 17. gr. *Opinber skrá um veittar heimildir og móttæknar tilkynningar.*

□ Persónuvernd skal halda skrá yfir alla vinnslu sem henni er tilkynnt um í samræmi við 31. gr. og þá vinnslu sem hún heimilar skv. 33. gr. Þar skulu að lágmarki koma fram þau atriði sem talin eru í 2. mgr. 16. gr.

□ Skráin skal vera aðgengileg almenningi með þeirri aðferð sem Persónuvernd ákveður.

■ 18. gr. *Upplýsingaréttur hins skráða.*

□ Hinn skráði á rétt á að fá frá ábyrgðaraðila vitneskju um:

1. hvaða upplýsingar um hann er eða hefur verið unnið með;

2. tilgang vinnslunnar;

3. hver fær, hefur fengið eða mun fá upplýsingar um hann;

4. hvaðan upplýsingarnar koma;

5. hvaða öryggisráðstafanir eru viðhafðar við vinnslu, enda skerði það ekki öryggi vinnslunnar.

□ Kröfu um vitneskju skv. 1. mgr. skal beina til ábyrgðaraðila eða fulltrúa hans skv. 6. gr. Veita skal vitneskju skriflega sé þess óskað.

■ 19. gr. *Takmarkanir á upplýsingarétti hins skráða.*

□ Réttur hins skráða til að fá vitneskju skv. 18. gr. nær ekki til upplýsinga sem einvörðungu eru notaðar til tölfraðivinnslu eða vísindarannsókna, enda geti vinnsla þeirra ekki haft bein áhrif á hagsmuni hans.

□ Ákvæði 18. gr. eiga ekki við ef réttur hins skráða samkvæmt því ákvæði þykir eiga að víkja að nokkru eða öllu fyrir hagsmunum annarra eða hans eigin. Skal þá m.a. tekið tillit til heilsu hins skráða og hagsmuna venslamanna hans. Þó má samkvæmt beiðni veita umboðsmanni hins skráða vitneskjuna, enda mæli engar sérstakar ástæður gegn því.

□ Réttur hins skráða til að fá vitneskju samkvæmt ákvæðum 18. gr. nær ekki til upplýsinga sem eru undanþegnar aðgangi samkvæmt upplýsinga- eða stjórnsýslulögum. Þegar um er að ræða gögn í vörslu annarra ábyrgðaraðila en stjórnvalda ná ákvæði 18. gr. ekki til vitneskju um efni vinnuskjala eða annarra sambærilegra gagna sem unnin eru af ábyrgðaraðila sjálfum eða aðilum á hans vegum, t.d. sérstökum ráðgjöfum eða sérfræðingum.

□ Þótt gögn séu undanþegin upplýsingarétti hins skráða skv. 3. mgr. getur hann óskað greinargerðar um efnislegt innihald þeirra, útdráttar eða annars konar samantektar nema hann geti kynnt sér staðreyndir málsins með öðrum hætti.

□ Dragi veiting vitneskju um tiltekna upplýsingar úr möguleikum á að leiða til lykta mál sem er til meðferðar má fresta veitingu upplýsinganna þar til lokið er undirbúningi málsmeðferðar.

□ Persónuvernd getur sett skilmála um beitingu upplýsingaréttar hins skráða í reglum sem ráðherra staðfestir.

■ **20. gr.** *[Fræðsluskyllda þegar persónuupplýsinga er aflað hjá hinum skráða.*

□ Þegar ábyrgðaraðili aflar persónuupplýsinga hjá hinum skráða sjálfum skal hann upplýsa hinn skráða um eftirtalin atriði:

1. nafn og heimilisfang ábyrgðaraðila og eftir atvikum fulltrúa hans skv. 6. gr.,
2. tilgang vinnslunnar,
3. aðrar upplýsingar, að því marki sem þær eru nauðsynlegar, með hliðsjón af þeim sérstöku aðstæðum sem ríkja við vinnslu upplýsinganna, svo að hinn skráði geti gætt hagsmuna sinna, svo sem upplýsingar um:
 - a. viðtakendur eða flokka viðtakenda upplýsinganna,
 - b. hvort honum sé skylt eða valfrjálst að veita umbeðnar upplýsingar og hvaða afleiðingar það kunni að hafa veiti hann þær ekki,
 - c. ákvæði laganna um upplýsingarétt hins skráða, svo og rétt hins skráða til leiðréttingar og eyðingar rangra eða villandi persónuupplýsinga um hann.

□ Ákvæði 1. mgr. gilda ekki hafi hinn skráði þegar fengið vitneskju um þau atriði sem fram koma í 1.–3. tölul. 1. mgr.]¹⁾

¹⁾L. 81/2002, 2. gr.

■ **21. gr.** *[Skylða til að láta hinn skráða vita um vinnslu persónuupplýsinga þegar þeirra er aflað hjá öðrum en honum sjálfum.*

□ Þegar ábyrgðaraðili aflar persónuupplýsinga frá öðrum en hinum skráða skal hann samtímis láta hinn skráða vita af því og greina honum frá þeim atriðum sem talin eru í 3. mgr. Sé ætlun ábyrgðaraðila hins vegar að miðla upplýsingunum innan hæfilegra tímamarka frá öflun þeirra má hann þó fresta því þar til hann miðlar upplýsingunum í fyrsta sinn.

□ Þrátt fyrir 2. málsl. 1. mgr. skal ábyrgðaraðili sem annast miðlun upplýsinga um fjárhagsmálefni og lánstraust láta hinn skráða vita 14 dögum áður en slíkum upplýsingum er miðlað í fyrsta sinn.

- ☐ Í tilkynningu til hins skráða skal veita upplýsingar um:
1. nafn og heimilisfang ábyrgðaraðila og eftir atvikum fulltrúa hans skv. 6. gr.,
 2. tilgang vinnslunnar,
 3. aðrar upplýsingar, að því marki sem þær eru nauðsynlegar, með hliðsjón af þeim sérstöku aðstæðum sem ríkja við vinnslu upplýsinganna, svo að hinn skráði geti gætt hagsmuna sinna, svo sem upplýsingar um:
 - a. tegundir eða flokka þeirra upplýsinga sem unnið er með,
 - b. hvaðan upplýsingarnar koma,
 - c. viðtakendur eða flokka viðtakenda upplýsinganna,
 - d. ákvæði laganna um upplýsingarétt hins skráða, svo og rétt hins skráða til leiðréttingar og eyðingar rangra eða villandi persónuupplýsinga um hann.
- ☐ Ákvæði 1. mgr. gilda ekki ef:
1. óframkvæmanlegt er að láta hinn skráða vita eða það leggur þyngri byrðar á ábyrgðaraðila en með sanngirni má krefjast,
 2. ætla má að hinum skráða sé þegar kunnugt um vinnsluna,
 3. lagaheimild stendur til skráningar eða miðlunar upplýsinganna eða
 4. hagsmunir hins skráða af því að fá vitneskju um upplýsingarnar þykja eiga að víkja fyrir veigamiklum almannahagsmunum eða einkahagsmunum, þ.m.t. hagsmunum hans sjálfs.]¹⁾

¹⁾L. 81/2002, 3. gr.

■ **22. gr.** *Rökstuðningur sértækra ákvarðana sem byggjast á sjálfvirkri upplýsingavinnslu.*

- ☐ Ef fyrir liggur sértæk ákvörðun sem að öllu leyti er byggð á rafrænni vinnslu persónuupplýsinga getur sá sem ákvörðunin beinist að krafist rökstuðnings fyrir niðurstöðunni. Í rökstuðningi skal ábyrgðaraðili gera grein fyrir þeim reglum sem hin rafræna vinnsla byggist á og liggja ákvörðuninni til grundvallar.

■ **23. gr.** *Viðvaranir um notkun persónusniða.*

- ☐ Þegar persónusnið sem skilgreinir tiltekið háttarni, smekk, hæfileika eða þarfir er lagt til grundvallar:
1. við sértæka ákvörðun skv. 9. tölul. 2. gr. eða
 2. við að nálgast hinn skráða, velja úrtak, markhóp o.s.frv.,
- getur Persónuvernd, þegar henni berst tilkynning um slíka vinnslu, ákveðið að ábyrgðaraðili geri hinum skráða viðvart og greini frá því hver sé ábyrgðaraðili vinnslunnar, hvaða upplýsingar hann noti og hvaðan þær komi.
- ☐ Við ákvörðun skv. 1. mgr. skal Persónuvernd m.a. líta til þess hvort viðvörðun er að hennar mati óframkvæmanleg eða leggi þyngri byrðar á ábyrgðaraðila en með sanngirni má krefjast.

■ **24. gr.** *Viðvaranir um rafræna vöktun.*

- ☐ Þegar rafræn vöktun fer fram á vinnustað eða á almannaþæri skal með merki eða á annan áberandi hátt gera glögglega viðvart um þá vöktun og hver sé ábyrgðaraðili.

IV. kafli. Leiðrétting, eyðing, lokun o.fl.

■ **25. gr.** *Leiðrétting og eyðing rangra og villandi persónuupplýsinga.*

- ☐ Ef skráðar hafa verið persónuupplýsingar sem eru rangar, villandi eða ófullkomnar, eða persónuupplýsingar hafa verið skráðar án tilskilinnar heimildar, skal ábyrgðaraðili sjá til þess að upplýsingarnar verði leiðréttar, þeim eytt eða við þær aukið ef umræddur

annmarki getur haft áhrif á hagsmuni hins skráða. Hafi slíkum upplýsingum verið miðlað eða þær notaðar ber ábyrgðaraðila, eftir því sem honum er frekast unnt, að hindra að það hafi áhrif á hagsmuni hins skráða.

☐ Ef eyðing eða breyting þeirra upplýsinga sem um ræðir í 1. mgr. er óheimil samkvæmt ákvæðum annarra laga getur Persónuvernd bannað notkun upplýsinganna.

■ **26. gr.** *Eyðing og bann við notkun persónuupplýsinga sem hvorki eru rangar né villandi.*

☐ Þegar ekki er lengur málefnaleg ástæða til að varðveita persónuupplýsingar skal ábyrgðaraðili eyða þeim. Málefnaleg ástæða til varðveislu upplýsinga getur m.a. byggst á fyrirmælum í lögum eða á því að ábyrgðaraðili vinni enn með upplýsingarnar í samræmi við upphaflegan tilgang með söfnun þeirra.

☐ Ef ákvæði annarra laga standa því ekki í vegi getur skráður aðili engu síður krafist þess að upplýsingum um hann skv. 1. mgr. sé eytt eða notkun þeirra bönnuð ef slíkt telst réttlæt看legt út frá heildstæðu hagsmunamati. Við slíkt hagsmunamat skal taka tillit til hagsmuna annarra, almennra persónuverndarhagsmuna, almannahagsmuna og þeirra aðgerða sem þörf er á til að verða við kröfunni.

☐ Persónuvernd getur, bæði í einstökum tilvikum eða með setningu almennra reglna, bannað notkun slíkra upplýsinga eða mælt fyrir um eyðingu þeirra.

■ **27. gr.** *Réttur til að fá ákvörðun sem byggist á handvirkri vinnslu upplýsinga.*

☐ Ef fyrir liggur sértæk ákvörðun í skilningi 9. tölul. 2. gr., sem að öllu leyti hefur byggst á sjálfvirkri vinnslu persónuupplýsinga, getur sá sem ákvörðun beinist að, eða mál varðar beinlínis með öðrum hætti, krafist þess að fá ákvörðunina handunna, enda sé um að ræða ákvörðun sem varðar persónulega hagi eða eiginleika hans og hefur verulega þýðingu fyrir hann.

☐ Réttur skv. 1. mgr. er ekki til staðar ef beitt er viðhlítandi ráðstöfunum til að gæta persónuverndarhagsmuna viðkomandi og um er að ræða ákvörðun sem byggist á fyrirmælum laga eða tengist gerð eða efndum samnings.

■ **28. gr.** *[[Um andmælarétt hins skráða og um bannskrá [Þjóðskrár Íslands].¹⁾]]²⁾*

☐ Hinum skráða er heimilt að andmæla vinnslu upplýsinga um sjálfan sig ef hann hefur til þess lögmætar og knýjandi ástæður vegna sérstakra aðstæðna sinna nema kveðið sé á um annað í öðrum lögum. Eigi andmælin rétt á sér er ábyrgðaraðila óheimil frekari vinnsla umræddra upplýsinga.

☐ [[Þjóðskrá Íslands]¹⁾ skal halda skrá yfir þá sem andmæla því að nöfn þeirra séu notuð í markaðssetningarstarfsemi. [Ráðherra]³⁾ setur, í samráði við Persónuvernd, nánari reglur⁴⁾ um gerð og notkun slíkrar skrár og hvaða upplýsingar skuli koma þar fram.]²⁾ Ábyrgðaraðilar sem starfa í beinni markaðssókn og þeir sem nota skrá með nöfnum, heimilisföngum, netföngum, símanúmerum og þess háttar eða miðla þeim til þriðja aðila í tengslum við slíka starfsemi skulu, áður en slík skrá er notuð í slíkum tilgangi, bera hana saman við skrá [Þjóðskrár Íslands]¹⁾ til að koma í veg fyrir að markpóstur verði sendur eða hringt verði til einstaklinga sem hafa andmælt slíku. Persónuvernd getur heimilað undanþágu frá þessari skyldu í sérstökum tilvikum.

☐ Öll notkun bannskrár skv. 2. mgr. er óheimil í öðrum tilgangi en þar er lýst.

☐ Skylt er að nafn ábyrgðaraðila komi fram á áberandi stað á útsendum markpósti og hvert þeir sem andmæla því að fá slíkan markpóst og marksímtöl geti snúið sér. Viðtakandi markpósts á rétt á að fá vitneskju um hvaðan þær upplýsingar koma sem liggja

úthringingu eða útsendingu til grundvallar. Þetta gildir ekki um markaðssetningu ábyrgðaraðila á eigin vöru og þjónustu sem notar eigin viðskiptamannaskrár, enda beri útsent efni með sér hvaðan það kemur. [Ef markpóstur er sendur með rafrænum hætti er skylt að fram komi á ótvíræðan hátt um leið og hann er mótttekinn að um slíkan póst sé að ræða.]⁹⁾

□ Ábyrgðaraðili er heimilt að afhenda félaga-, starfsmanna- eða viðskiptamannaskrár til nota í tengslum við markaðssetningarstarfsemi. Þetta á þó aðeins við ef:

1. ekki telst vera um afhendingu viðkvæmra persónuupplýsinga að ræða,
2. hinum skráðu hefur, áður en afhending fer fram, verið gefinn kostur á að andmæla því, hverjum fyrir sitt leyti, að upplýsingar um viðkomandi birtist á hinna afhentu skrá,
3. slíkt fer ekki gegn reglum eða samþykktum viðkomandi félags,
4. ábyrgðaraðili kannar hvort einhver hinna skráðu hefur komið andmælum á framfæri við [Þjóðskrár Íslands],¹⁾ sbr. 2. mgr., og eyðir upplýsingum um viðkomandi áður en hann lætur skrána af hendi.

□ Ákvæði 5. mgr. gildir ekki ef afhending félaga-, starfsmanna- eða viðskiptamannaskrár til nota við dreifingu markpósts byggist á samþykki hins skráða, sbr. 1. tölul. 1. mgr. 8. gr.

□ Ákvæði 1.–5. mgr. gilda, eftir því sem við á, einnig um markaðs-, neyslu- og skoðanakannanir. Persónuvernd er heimilt að undanþiggja vísindarannsóknir og hliðstæðar rannsóknir slíkum takmörkunum, enda þyki ljóst að slíkt geti skert til muna áreiðanleika niðurstöðu rannsóknarinnar.⁶⁾

¹⁾L. 77/2010, 5. gr. ²⁾L. 50/2006, 23. gr. ³⁾L. 162/2010, 164. gr. ⁴⁾Rgl. 36/2005. ⁵⁾L. 30/2002, 23. gr. ⁶⁾L. 90/2001, 8. gr.

V. kafli. Flutningur persónuupplýsinga úr landi.

■ **29. gr.** *Flutningur persónuupplýsinga til ríkis sem veitir fullnægjandi persónuupplýsingavernd.*

□ Heimill er flutningur persónuupplýsinga til annars ríkis ef lög þess veita persónuupplýsingum fullnægjandi vernd.

□ Ríki sem framfylgir tilskipun Evrópusambandsins 95/46/ESB um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálst flæði slíkra upplýsinga telst fullnægja skilyrðum 1. mgr. [Sama á við um lönd eða staði sem Persónuvernd auglýsir¹⁾ í Stjórnartíðindum að virtum ákvörðunum framkvæmdastjórnar Evrópubandalagsins.]²⁾

□ Við mat á því hvort ríki sem ekki framfylgir tilskipun 95/46/ESB fullnægi skilyrðum 1. mgr. skal m.a. líta til reglna viðkomandi ríkis um meðferð persónuupplýsinga, reglna um góða viðskiptahætti og þeirra öryggisráðstafana sem viðhafðar eru hjá viðtakanda. Þá skal taka mið af því hvort viðkomandi ríki hafi fullgilt samning Evrópuráðsins nr. 108 frá 28. janúar 1981, um vernd einstaklinga varðandi vélræna vinnslu persónuupplýsinga.

¹⁾Rgl. 1100/2008, sbr. rgl. 424/2010. Augl. 228/2010, sbr. augl. 108/2012, augl. 419/2013 og augl. 1316/2013. ²⁾L. 90/2001, 9. gr.

■ **30. gr.** *Flutningur persónuupplýsinga til ríkis sem ekki veitir fullnægjandi persónuupplýsingavernd.*

□ Óheimill er flutningur persónuupplýsinga til ríkis sem ekki veitir fullnægjandi persónuupplýsingavernd nema:

1. hinn skráði hafi samþykkt flutninginn, eða
2. slíkt sé nauðsynlegt til efnda á þjóðréttarskuldbindingum eða vegna aðildar Íslands að alþjóðastofnun, eða
3. heimild standi til slíks flutnings í öðrum lögum, eða

4. afhendingin sé nauðsynleg til að gera eða efna samning milli hins skráða og ábyrgðaraðila, eða

5. flutningurinn sé nauðsynlegur til að gera eða efna samning í þágu hins skráða, eða

6. afhendingin sé nauðsynleg til að verja verulega hagsmuni hins skráða,

[7. ef miðlun er nauðsynleg eða fyrirskipuð samkvæmt lögum vegna þess að brýnir almannahagsmunir krefjast þess eða til að unnt sé að stofna, hafa uppi eða verja réttarkröfur, eða

8. um sé að ræða upplýsingar sem almennur aðgangur er að].¹⁾

□ Persónuvernd getur heimilað flutning upplýsinga til ríkis er greinir í 1. mgr. telji hún sérstök rök mæla með því, jafnvel þótt skilyrðum ákvæðisins sé ekki fullnægt. Í slíku tilviki skal m.a. taka tillit til eðlis upplýsinganna, fyrirhugaðs tilgangs vinnslunnar og hve lengi hún varir. [Persónuvernd getur heimilað miðlun persónuupplýsinga til þriðju landa þótt þau hafi ekki verið talin veita friðhelgi borgaranna nægilega einkalífssvernd. Slíkt er háð því að ábyrgðaraðili hafi, að mati stofnunarinnar, veitt nægilegar tryggingar fyrir slíku. Getur stofnunin t.d. áskilið að ábyrgðaraðili hafi gert við viðtökuaðila skriflegan samning sem hafi að geyma tiltekin stöðluð samningsákvæði í samræmi við ákvörðun sem Persónuvernd hefur auglýst í Stjórnartíðindum, að teknu tilliti til ákvarðana framkvæmdastjórnar Evrópubandalagsins, sbr. 2. mgr. 29. gr. laga þessara. Að öðru leyti getur Persónuvernd sett nánari fyrirmæli²⁾ um flutning persónuupplýsinga úr landi.]¹⁾

¹⁾L. 90/2001, 10. gr. ²⁾Rgl. 712/2008, sbr. rgl. 927/2009, rgl. 423/2010 og rgl. 1174/2014. Rgl. 1100/2008, sbr. rgl. 424/2010.

VI. kafli. Tilkynningarskylda, leyfisskylda o.fl.

■ 31. gr. Tilkynningarskylda.

□ Sérhver ábyrgðaraðili sem beitir rafrænni tækni við vinnslu persónuupplýsinga, sbr. 8. gr. og 1. mgr. 9. gr., skal á þar til gerðu formi tilkynna Persónuvernd um vinnsluna tímanlega áður en hún hefst. Tilkynna skal allar breytingar sem verða frá því sem greinir í upphaflegri tilkynningu.

□ Tilkynningarskyldan á ekki við ef einungis er unnið með upplýsingar sem gerðar hafa verið og eru aðgengilegar almenningi.

□ Persónuvernd getur ákveðið¹⁾ að vissar tegundir vinnslu almennra upplýsinga skuli vera undanþegnar tilkynningarskyldu eða að um þær gildi einfaldari tilkynningarskylda. Persónuvernd getur jafnframt ákveðið¹⁾ að vissar tegundir vinnslu skuli vera leyfisskyldar. Um vinnslu sem undanþegin er tilkynningarskyldu getur Persónuvernd sett fyrirmæli, þar á meðal um þau atriði sem talin eru í 2. mgr. 35. gr. Persónuvernd getur einnig mælt fyrir um ráðstafanir til að draga úr óhagræði sem slík vinnsla persónuupplýsinga kann að hafa í för með sér fyrir hinn skráða.

¹⁾Rgl. 712/2008, sbr. rgl. 927/2009, rgl. 423/2010 og rgl. 1174/2014.

■ 32. gr. Efni tilkynninga.

□ Í tilkynningu til Persónuverndar skv. 31. gr. skal tilgreina eftirfarandi atriði:

1. nafn og heimilisfang ábyrgðaraðila og eftir atvikum fulltrúa hans, sbr. 6. gr.;

2. hver ber daglega ábyrgð á að uppfylla skyldur ábyrgðaraðila;

3. tilgang vinnslunnar;

4. skilgreiningu og aðra lýsingu á þeim tegundum upplýsinga sem notaðar verða við vinnslu;

5. hvert upplýsingarnar eru sóttar;

6. þá heimild sem stendur til söfnunar upplýsinganna;
7. hverjum upplýsingarnar verða afhentar;
8. hvort ráðgert sé að flytja persónuupplýsingarnar úr landi;
9. hvort ráðgert sé að birta upplýsingarnar á netinu;
10. hvaða öryggisráðstafanir verða viðhafðar í vinnslunni;
11. hvort og hvenær persónuupplýsingum eða persónuauðkennum verði eytt;
- [12. hvernig uppfyllt séu fyrirmæli 20. og 21. gr.]¹⁾

☐ Persónuvernd getur sett nánari fyrirmæli²⁾ um form og efni tilkynninga og um framkvæmd tilkynningarskyldunnar að öðru leyti.

☐ Ábyrgðaraðili skal sjá til þess að Persónuvernd hafi á hverjum tíma undir höndum réttar upplýsingar um vinnsluna. Þegar liðin eru þrjú ár frá því að tilkynning var send Persónuvernd skal senda henni nýja tilkynningu með uppfærðum upplýsingum nema henni hafi áður verið tilkynnt um breytta vinnslu. Persónuvernd getur mælt fyrir um ráðstafanir til að tryggja gæði og áreiðanleika tilkynninga og ákveðið mismunandi tilkynningarfrest eftir tegund og eðli vinnslu.³⁾

¹⁾L. 81/2002, 4. gr. ²⁾Rgl. 712/2008, sbr. rgl. 927/2009, rgl. 423/2010 og rgl. 1174/2014. ³⁾Rgl. 1100/2008, sbr. rgl. 424/2010.

■ 33. gr. *Leyfis skyld vinnsla.*

☐ Sé um að ræða vinnslu almennra eða viðkvæmra persónuupplýsinga sem getur falið í sér sérstaka hættu á að farið verði í bága við réttindi og frelsi skráðra aðila getur Persónuvernd ákveðið¹⁾ að vinnslan megi ekki hefjast fyrr en hún hefur verið athuguð af stofnuninni og samþykkt með útgáfu sérstakrar heimildar. Persónuvernd getur ákveðið²⁾ að slík leyfis skylda falli brott þegar settar hafa verið almennar reglur og öryggisstaðlar sem fylgja skuli við slíka vinnslu.

¹⁾Rgl. 712/2008, sbr. rgl. 927/2009, rgl. 423/2010, rgl. 548/2013 og rgl. 1174/2014. ²⁾Rgl. 170/2001, sbr. rgl. 157/2003 og rgl. 853/2010. Rgl. 1100/2008, sbr. rgl. 424/2010.

■ 34. gr. *Forsendur leyfisveitingar o.fl.*

☐ Ábyrgðaraðila má aðeins veita leyfi skv. 33. gr., eða einstakar aðrar heimildir samkvæmt lögum þessum, ef líklegt er að hann geti fullnægt skyldum sínum samkvæmt lögnum eða fyrirmælum Persónuverndar.

☐ Við afgreiðslu mála er tengjast vinnslu viðkvæmra persónuupplýsinga skal Persónuvernd, innan þeirra marka sem greinir í II. kafla laganna, meta hvort vinnslan geti valdið hinum skráða slíku óhagræði að ekki verði úr því bætt með forsvaranlegum hætti með skilyrðum sem sett eru skv. 35. gr. Ef slíkt óhagræði getur orðið skal Persónuvernd meta hvort hagsmunir sem mæla með vinnslunni vegi þyngra en hagsmunir hins skráða.

■ 35. gr. *Skilmálar Persónuverndar um vinnslu persónuupplýsinga.*

☐ Þegar ábyrgðaraðila er veitt leyfi skv. 33. gr. skal Persónuvernd binda það skilyrðum, svo sem um dulkóðun persónuauðkenna og öðrum sem hún metur nauðsynleg hverju sinni, til að draga úr eða koma í veg fyrir hugsanlegt óhagræði hins skráða af vinnslunni. Sama gildir eftir því sem við á þegar Persónuvernd berst tilkynning um vinnslu viðkvæmra persónuupplýsinga sem fellur undir 1. mgr. 9. gr.

☐ Við mat á því hvaða skilyrði skal setja fyrir vinnslu skal Persónuvernd m.a. athuga:

1. hvort tryggt sé að hinn skráði geti nýtt réttindi sín samkvæmt lögnum, þar á meðal til að hætta þátttöku í verkefni, og eftir atvikum fá eytt skráðum persónuupplýsingum, til að fá fræðslu um réttindi sín og beitingu þeirra;

2. hvort persónuupplýsingar verði nægjanlega öruggar, áreiðanlegar og uppfærðar í samræmi við tilgang vinnslunnar skv. 7. gr.;

3. hvort með persónuupplýsingarnar verði farið af þeirri varúð sem reglur um þagnarskyldu og tilgangur vinnslunnar krefst;

4. hvort skipulagt hafi verið hvernig hinum skráða verði veittar upplýsingar og leiðbeiningar, innan þeirra marka sem sanngjarnt er að ætlast til miðað við umfang vinnslunnar og aðrar öryggisráðstafanir sem viðhafðar eru;

5. hvort stofnað hafi verið til öryggisráðstafana sem séu eðlilegar miðað við tilgang vinnslunnar.

☐ Persónuvernd getur ákveðið að ábyrgðaraðili og vinnsluaðili, svo og starfsmenn á vegum þeirra, skuli undirrita yfirlýsingu um að þeir lofi að gæta þagmælsku um viðkvæmar persónuupplýsingar sem þeir fá vitneskju um við vinnslu þeirra. Ábyrgðaraðili eða fulltrúi hans skal votta rétta undirskrift starfsmanns og dagsetningu slíkrar yfirlýsingar og koma til Persónuverndar innan tilskilins frests. Brot á slíkri þagnarskyldu varðar refsingu skv. 136. gr. almennra hegningarlaga. Þagnarskyldan helst þótt látið sé af starfi.

☐ Persónuvernd getur afgreitt erindi er lýtur að vinnslu viðkvæmra persónuupplýsinga með skilyrði um að sérstakur tilsjónarmaður verði skipaður til að hafa eftirlit fyrir hönd Persónuverndar með því að vinnsla sé í samræmi við lög og að ábyrgðaraðili greiði allan kostnað sem af því hlýst.

■ [35. gr. a. Um leyfi fyrir vísindarannsóknum á heilbrigðissviði fer samkvæmt lögum um vísindarannsóknir á heilbrigðissviði.]¹⁾

¹⁾L. 44/2014, 36. gr.

VII. kafli. Eftirlit og viðurlög.

■ 36. gr. *Skipulag Persónuverndar og stjórnssýsla.*

☐ Persónuvernd er sjálfstæð stofnun með sérstaka stjórn og heyrir stjórnarfarslega undir [ráðherra].¹⁾

☐ Persónuvernd er sjálfstæð í störfum sínum og verður ákvörðunum hennar samkvæmt lögum þessum ekki skotið til annarra stjórnvalda.

☐ Ráðherra skipar fimm menn í stjórn Persónuverndar og jafnmarga til vara til fjögurra ára í senn. Formann og varaformann stjórnarinnar skipar ráðherra án tilnefningar og skulu þeir vera lögfræðingar og fullnægja hæfisskilyrðum héraðsdómara. Hæstiréttur tilnefnir einn stjórnarmann og Skýrslutæknifélag Íslands annan og skal hann vera sérfróður á sviði tölvu- og tæknimála. Varamenn skulu fullnægja sömu skilyrðum og aðalmenn.

☐ Ráðherra ákveður laun stjórnarmanna.

☐ Þegar stjórnarmenn eru ekki sammála ræður meiri hluti niðurstöðu máls. Ef atkvæði eru jöfn ræður atkvæði formanns.

☐ Ráðherra skipar forstjóra Persónuverndar til fimm ára í senn að fenginni tillögu stjórnar. Forstjóri situr fundi stjórnar með málfrelsi og tillögurétti.

☐ Forstjóri Persónuverndar annast daglega stjórn og ræður annað starfsfólk Persónuverndar.

☐ Forstjóri ber ábyrgð á fjárreiðum og starfsmannahaldi Persónuverndar. Stjórn Persónuverndar ákveður að öðru leyti skiptingu starfa á milli stjórnar og starfsmanna hennar.²⁾

¹⁾L. 126/2011, 308. gr. ²⁾Rgl. 231/2012.

■ **37. gr. Verkefni Persónuverndar.**

□ Persónuvernd annast eftirlit með framkvæmd laga þessara og reglna settra samkvæmt þeim.

□ Persónuvernd úrskurðar í ágreiningsmálum sem upp kunna að koma um vinnslu persónuupplýsinga [á Íslandi, hvort sem íslensk lög eða lög annars ríkis gilda um vinnsluna].¹⁾ Persónuvernd getur fjallað um einstök mál að eigin frumkvæði eða samkvæmt erindi þess sem telur að ekki hafi verið unnið með persónuupplýsingar um hann í samræmi við lög þessi og reglur sem settar eru samkvæmt þeim eða einstökum fyrirmælum.

□ Verkefni Persónuverndar eru m.a. eftirfarandi:

1. að afgreiða leyfisumsóknir, taka við tilkynningum og mæla, eftir því sem þurfa þykir, fyrir um ráðstafanir að því er varðar tækni, öryggi og skipulag vinnslunnar þannig að hún verði í samræmi við ákvæði laganna,²⁾

2. að hafa eftirlit með því að farið sé að lögum og öðrum reglum um vinnslu persónuupplýsinga og að bætt sé úr annmörkum og mistökum,

3. að fylgjast með almennri þróun á sviði persónuupplýsingaverndar á innlendum og erlendum vettvangi og hafa yfirsýn yfir og kynna helstu álitæfni sem tengjast vinnslu persónuupplýsinga,

4. að skilgreina og afmarka hvar persónuvernd er hætta búin og veita ráð um leiðir til lausnar,

5. að leiðbeina þeim sem ráðgera að vinna með persónuupplýsingar, eða þróa kerfi fyrir slíka vinnslu, um persónuvernd, þar á meðal með því að aðstoða við gerð starfs- og siðareglna fyrir einstaka hópa og starfsstéttir,³⁾

6. að tjá sig, samkvæmt beiðni eða að eigin frumkvæði, um álitæfni varðandi meðferð persónuupplýsinga og veita umsagnir við setningu laga og annarra reglna sem þýðingu hafa fyrir persónuvernd,

7. að birta árlega skýrslu um starfsemi sína.

□ Persónuvernd getur ákveðið að ábyrgðaraðili skuli greiða þann kostnað sem hlýst af eftirliti með því að hann fullnægi skilyrðum laga þessara og reglna sem settar eru samkvæmt þeim eða einstökum fyrirmælum. Persónuvernd getur einnig ákveðið að ábyrgðaraðili greiði kostnað við úttekt á starfsemi við undirbúning útgáfu vinnsluleyfis og annarrar afgreiðslu.

□ [Persónuvernd setur reglur⁴⁾ um rafræna vöktun og vinnslu efnis sem verður til við vöktunina, svo sem hljóð- og myndefnis, þar á meðal um öryggi, varðveislu og notkun þess. Þá getur hún gefið fyrirmæli um rétt þess sem myndaður hefur verið til að skoða myndir sem teknar hafa verið af honum. Persónuvernd setur jafnframt reglur og gefur fyrirmæli um eyðingu efnis sem til verður við framkvæmd rafrænnar vöktunar, ákveður varðveisluaðferð og varðveislutíma og heimilar afhendingu þess í öðrum tilvikum en þeim sem mælt er fyrir um í 2. mgr. 9. gr.]⁵⁾

¹⁾L. 90/2001, 11. gr. ²⁾Rgl. 340/2003. ³⁾Augl. 1001/2001. ⁴⁾Rgl. 837/2006, sbr. rgl. 394/2008, rgl. 475/2011 og rgl. 869/2014. ⁵⁾L. 81/2002, 5. gr.

■ **38. gr. Aðgangur Persónuverndar að upplýsingum o.fl.**

□ Persónuvernd getur krafist ábyrgðaraðila, vinnsluaðila og þá sem starfa á þeirra vegum um allar þær upplýsingar og skriflegar skýringar sem henni eru nauðsynlegar til þess að rækja hlutverk sitt, þar á meðal þær upplýsingar sem hún þarf til að geta metið hvort

tiltekin starfsemi eða vinnsla falli undir ákvæði laganna. Einnig getur Persónuvernd kvatt ábyrgðaraðila, vinnsluaðila og þá sem starfa á þeirra vegum á sinn fund til að veita munnlegar upplýsingar og skýringar varðandi ákveðna vinnslu persónuupplýsinga.

□ Persónuvernd hefur í eftirlitsstörfum sínum án dómsúrskurðar aðgang að húsnæði þar sem vinnsla persónuupplýsinga fer fram eða gögn eru varðveitt, þar á meðal stöðum þar sem varðveittar eru skrár, myndir, sbr. 4. gr., persónuupplýsingar sem lúta rafrænni vinnslu, og tæki til slíkrar vinnslu. Persónuvernd getur framkvæmt hverja þá prófun eða eftirlitsaðgerð sem hún telur nauðsynlega og krafist nauðsynlegrar aðstoðar starfsfólks á slíkum vettvangi til að framkvæma prófun eða eftirlit. Persónuvernd getur óskað liðveislu lögreglu ef einhver leitast við að hindra hana í eftirlitsstörfum sínum.

□ Réttur Persónuverndar til að krefjast upplýsinga eða aðgangs að starfsstöðvum og tækjabúnaði verður ekki takmarkaður með vísun til reglna um þagnarskyldu.

■ **39. gr. Undanþágur frá þagnarskyldu.**

□ Ákvæði um þagnarskyldu standa því ekki í vegi að Persónuvernd veiti persónuverndarstofnunum erlendis upplýsingar þegar slíkt er nauðsynlegt til að hún eða hin erlenda persónuverndarstofnun geti ákveðið eða framkvæmt aðgerðir til að tryggja persónuvernd.

■ **40. gr. Stöðvun vinnslu o.fl.**

□ Persónuvernd getur mælt fyrir um stöðvun vinnslu persónuupplýsinga, þar á meðal söfnunar, skráningar eða miðlunar, mælt fyrir um að persónuupplýsingar verði afmáðar eða skrár eytt, í heild eða að hluta, bannað frekari notkun upplýsinga eða lagt fyrir ábyrgðaraðila að viðhafa ráðstafanir sem tryggja lögmæti vinnslunnar. Við mat á því hvort og þá hvaða úrræðum skuli beitt skal Persónuvernd m.a. taka tillit til þeirra atriða sem greinir í 2. mgr. 35. gr.

□ Komi í ljós að fram fer vinnsla persónuupplýsinga sem brýtur í bága við ákvæði laga þessara eða reglur settar samkvæmt þeim er Persónuvernd heimilt að fela lögreglustjóra að stöðva til bráðabirgða starfsemi viðkomandi og innsigla starfsstöð hans þegar í stað.

□ Sinni aðili ekki fyrirmælum Persónuverndar skv. 1. mgr. getur hún afturkallað leyfi sem hún hefur veitt samkvæmt ákvæðum laga þessara þar til úr hefur verið bætt að hennar mati.

■ **41. gr. Dagsektir.**

□ Ef ekki er farið að fyrirmælum Persónuverndar skv. 10., 25., 26. eða 40. gr. getur hún ákveðið að leggja dagsektir á þann sem fyrirmælin beinast að þar til úr hefur verið bætt að mati Persónuverndar. Sektir geta numið allt að 100.000 kr. fyrir hvern dag sem líður eða byrjar að líða án þess að fyrirmælum Persónuverndar sé fylgt.

□ Ef ákvörðun Persónuverndar um dagsektir er skotið til dómstóla byrja dagsektir ekki að falla á fyrr en dómur er endanlegur. Dagsektir renna í ríkissjóð og má án undangengins dóms gera aðför til fullnustu þeirra.

■ **42. gr. Refsingar.**

□ Brot á ákvæðum laga þessara og reglugerða settra samkvæmt þeim varða fésektum eða fangelsi allt að þremur árum nema þyngri refsing liggi við samkvæmt öðrum lögum. Sama refsing liggur við ef ekki er farið að fyrirmælum Persónuverndar.

□ Nú er brot framið í starfsemi lögaðila og má þá gera lögaðilanum fésekt skv. II. kafla A almennra hegningarlaga.

■ 43. gr. *Bætur.*

□ Hafi ábyrgðaraðili eða vinnsluaðili unnið með persónuupplýsingar í andstöðu við ákvæði laga þessara, reglna eða fyrirmæla Persónuverndar skal ábyrgðaraðili bæta hinum skráða það fjárhagslega tjón sem hann hefur orðið fyrir af þeim völdum. Ábyrgðaraðila verður þó ekki gert að bæta tjón sem hann sannar að hvorki verður rakið til mistaka né vanrækslu af hans hálfu eða vinnsluaðila.

VIII. kafli. Lagatengsl, gildistaka o.fl.

■ 44. gr. *Tengsl við ákvæði annarra laga.*

□ Lögin gilda um vinnslu og meðferð persónuupplýsinga sem fram fer samkvæmt öðrum lögum nema þau lög tilgreini annað sérstaklega.

□ Lög þessi takmarka ekki þann rétt til aðgangs að gögnum sem mælt er fyrir um í upplýsingalögum og stjórnsýslulögum.

■ 45. gr. *Reglugerðir um einstaka flokka starfsemi.*

□ Með reglugerð má mæla fyrir um meðferð persónuupplýsinga í tiltekinni starfsemi og hjá einstökum starfsstéttum.

□ Í reglugerð¹⁾ skal mælt fyrir um heimild til söfnunar og skráningar upplýsinga sem varða fjárhagsmálefni og lánstraust fyrirtækja, svo og annarra lögaðila, í því skyni að miðla til annarra upplýsingum um það efni. Heimild til slíkrar starfsemi skal bundin leyfi Persónuverndar og um hana gilda eftirfarandi ákvæði laganna: 11. gr. um öryggi og gæði upplýsinga, 12. gr. um innra eftirlit, 13. gr. um meðferð vinnsluaðila á upplýsingum, 18. gr. um upplýsingarétt hins skráða, 21. gr. um viðvörðunarskyldu þegar upplýsingum er safnað frá öðrum en hinum skráða, 25. gr. um leiðréttingu og eyðingu rangra og villandi upplýsinga, 26. gr. um eyðingu og bann við notkun upplýsinga sem hvorki eru rangar né villandi, 33. gr. um leyfisskylda vinnslu, 34. gr. um forsendur leyfisveitingar, 35. gr. um skilmála, 38. gr. um aðgang Persónuverndar að upplýsingum o.fl., 40. gr. um stöðvun vinnslu o.fl., 41. gr. um dagsektir, 42. gr. um refsingar og 43. gr. um bætur.

□ Að fenginni umsögn Persónuverndar skal ráðherra í reglugerð²⁾ mæla nánar fyrir um eftirlit Persónuverndar með rafrænni vinnslu persónuupplýsinga hjá lögreglu. Þar skal m.a. mælt fyrir um skyldu lögreglu til að tilkynna Persónuvernd um rafrænt unnar skrár sem hún heldur og efni slíkra tilkynninga. Þá skal mælt fyrir um í hvaða tilvikum og með hvaða hætti hinn skráði á rétt til aðgangs að persónuupplýsingum sem skráðar hafa verið um hann hjá lögreglu, svo og heimild lögreglu til miðlunar upplýsinga í öðrum tilvikum. Loks skal mælt fyrir um öryggi persónuupplýsinga og innra eftirlit lögreglu með því að vinnslu persónuupplýsinga sé hagað í samræmi við lög, svo og um tímalengd á varðveislu skráðra upplýsinga.

□ Þá skal í reglugerð kveða nánar á um starfsemi þeirra sem nota nafnalista, vinna nafnárítanir, þar á meðal við markaðssetningarstarfsemi, og við gerð markaðs- og skoðanakannana.

¹⁾Rg. 246/2001. ²⁾Rg. 322/2001, sbr. 926/2004, 362/2008 og 1137/2008.

■ 46. gr. *Gildistaka.*

□ Lög þessi öðlast gildi 1. janúar 2001. ...

■ **Ákvæði til bráðabirgða.** Þegar er lög þessi hafa verið birt skal ráðherra skipa stjórn og auglýsa embætti forstjóra Persónuverndar laust til umsóknar. Eftir að forstjóri hefur verið

skipaður ræður hann eftir þörfum annað starfsfólk til að annast undirbúning að gildistöku laganna og sinna stjórnsýslu skv. 2. mgr.

☐ Þrátt fyrir 1. mgr. 46. gr. skal Persónuvernd þegar er stjórn hennar hefur verið skipuð taka að sér eftirlit með því að meðferð persónuupplýsinga í Schengen-upplýsingakerfinu á Íslandi sé í samræmi við lög nr. 16/2000, um Schengen-upplýsingakerfið á Íslandi.

☐ Sérhver ábyrgðaraðili sem beitir rafrænni tækni við vinnslu persónuupplýsinga við gildistöku laganna skal á þar til gerðu eyðublaði tilkynna Persónuvernd um vinnsluna í samræmi við ákvæði 31. og 32. gr. innan sex mánaða frá gildistöku þeirra.

☐ Leyfi sem tölvunefnd hefur gefið út skulu halda gildi, enda fari þau ekki í bága við lög þessi.

Fskj. 6

Forsíða | Veftré

Upplýsingar um þig | Hafa samband | Aðgengismál | Information in English



Útlit síðu:

Leita á vefnum

Sláðu inn leitarorð

Leita

Forsíða
Um Persónuvernd
Efst á baugi - Úrskurðir o.fl.
Ný persónuverndarlöggjöf 2018
Lög og reglur
Lög um persónuvernd
Reglur og reglugerðir
Önnur lög
Aðrar reglur og leiðbeiningar
Alþjóðasamningar og Evrópulöggjöf
Spurningar og svör
Tilkynningar
Umsóknir og eyðublið
Útgefið efni
Tenglar

Þú ert hér: **Forsíða** > **Lög og reglur** > **Reglur og reglugerðir**

Reglur nr. 299/2001 um öryggi persónuupplýsinga

I. KAFLI

Markmið og gildissvið

1. gr.
Markmið

Markmið reglna þessara er að tryggja öryggi við vinnslu persónuupplýsinga. Í því felst að tryggja eðlilega leynd upplýsinganna, lögmætan aðgang að þeim, gæði þeirra og auðanleika. Að öðru leyti en kemur fram í reglum þessum má til hlífðsjónar og leiðbeiningar stýðjast við staðalinn [IST ISO/IEC 27001 Upplýsingatækni – Öryggisáætlun – Stjórnkerfi upplýsinga – Kröfur.]¹

¹ Reglur nr. 551/2013, 1. gr.

2. gr.

Gildissvið

Reglur þessar gilda um vinnslu persónuupplýsinga sem lög nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga, taka til. Persónuvernd getur veitt undánþágu frá fyrirmælum reglna þessara ef um er að ræða vinnslu persónuupplýsinga sem ekki telst hafa í för með sér hættu fyrir friðhelgi einkalífs, t.d. þegar lítið er til umfangs vinnslunnar, áhættu af vinnslunni og eðlis þeirra gagna sem veita á.

II. KAFLI
Öryggiskerfi

3. gr.

Ábyrgðaraðila ber að útbúa öryggiskerfi til að tryggja vernd persónuupplýsinga. Undirbúningur öryggiskerfis fer fram í þessum áföngum:

1. Ábyrgðaraðili setur sér skriflega *öryggisstefnu*. Í henni skal m.a. koma fram almenn lýsing á afstöðu æðsta stjórnanda ábyrgðaraðila til öryggismála. Við móttöku öryggisstefnu skal taka mið af því hvaða persónuupplýsingar skuli vernda, hvernig skuli vernda þær og þeirri aðferð sem viðhófið verður við vinnslu þeirra.
2. Ábyrgðaraðili gerir skriflegt *áhættumat*. Áhættumat er mat á hættunni á því að óviðkomandi fái aðgang að persónuupplýsingum, geti breytt upplýsingunum eða skert öryggi þeirra að öðru leyti. Áhættumat tekur einnig til athugunar á umfangi og afleiðingum hættunnar m.t.t. eðlis þeirra persónuupplýsinga sem unnið er með. Markmið áhættumats er að skapa forsendur fyrir vali á öryggisráðstöfunum, sbr. III. kafla reglna þessara. Þá skal tilgreina hvað geti farið úrskeiðis, hvaða áhrif slíkt geti haft á öryggi upplýsinganna og hvaða líkur séu á slíku. Áhættumat skal endurskoðað reglulega.
3. Ábyrgðaraðili velur hvaða *öryggisráðstafanir* skulu viðhafðar í samræmi við III. kafla reglna þessara og setja fram skriflega lýsingu á þeim, í lýsingunni skal m.a. koma fram afstöða ábyrgðaraðilans til þess hvað sé áætlaðanleg áhætta við vinnsluna. Þá skal rakið hvaða öryggisráðstöfunum verði beitt og hvernig þær verði útfærðar, þ.a.m. við hönnun, þróun, rekstur, prófun og viðhald þess kerfis, þ.m.t. hugbúnaðar, sem notað verður við vinnslu upplýsinganna. Þar skal og tekið fram hvernig þrúgdást verði við áföllum í rekstri vinnslukerfisins, hvernig flutningi persónuupplýsinga milli vinnslukerfa verði hagað, þ.a.m. mögulegum flutningi gagna milli ábyrgðar- og vinnsluadila. Öryggisráðstafanir skal endurskoðað reglulega.

Persónuvernd skal hvenær sem hún óskar hafa aðgang að öryggisstefnu ábyrgðaraðila, áhættumati og lýsingu á viðkomandi öryggisráðstöfunum.

III. KAFLI
Öryggisráðstafanir

4. gr.

Almennt

Ábyrgðaraðili skal gera viðeigandi öryggisráðstafanir og ber ábyrgð á því að vinnsla persónuupplýsinga séu í samræmi við lög, reglur og fyrirmæli Persónuverndar um hvernig tryggja skuli öryggi upplýsinga, þ.m.t. þá stöðia sem hún ákveður. Markmið skipulags- og tæknilegra öryggisráðstafana er til að tryggja nægilegt öryggi og vernda persónuupplýsingar gegn ólöglegri eyðileggingu, gegn því að þær glattist eða breytist fyrir slysi, gegn óleyfilegum aðgangi og gegn ölli annarri ólögmætni vinnslu.

Við val öryggisráðstafana skal taka mið af áhættu af vinnslunni og eðli þeirra gagna sem veita á. Skulu þær tryggja nægilegt öryggi með hlífðsjón af nýjustu tækni og kostnaði við framkvæmd þeirra. Sé persónuupplýsingum miðlað um Netið skal taka mið af þeirri auknu áhættu sem sú aðferð hefur í för með sér.

5. gr.

Öryggisráðstafanir varðandi starfsmannamál

Í þeim tilgangi að fyrirbyggja og takmarka tjón af völdum mannlegra mistaka, þjófnaðar, svika og annarrar misnotkunar, skal ábyrgðaraðili gripa til þeirra öryggisráðstafana sem við eiga hverju sinni, t.d.:

1. Kanna feril umsækjenda um störf.
2. Fá skjalfestar þagnaryfirlýsingar starfsmanna.
3. Skilgreina með skýrum hætti hlutverk og skyldur hvers starfsmanns sem hefur aðgang að persónuupplýsingum, þ.a.m. hverjir beri ábyrgð á einstökum skráasöfnum.
4. Gera nauðsynlegar ráðstafanir til þess að starfsmönnum sé með reglubundnum hætti gætt grein fyrir starfsskyldum sínum og þeim afleiðingum sem það getur haft í för með sér að brjóta þær.

6. gr.

Ytra öryggi

Í þeim tilgangi að fyrirbyggja og takmarka tjón af völdum óheimils aðgangs, skal ábyrgðaraðili gripa til þeirra öryggisráðstafana sem við eiga hverju sinni, t.d.:

1. Stýra aðgangi að húsneði með úthlutun lykila, aðgangskorta o.þ.h.
2. Viðhafa öryggisvörðlu, t.d. með öryggisvörðum, viðvönunarkerfum eða rafrænni vöktun.

7. gr.

Skipulagslegar og tæknilegar öryggisráðstafanir

Í þeim tilgangi að fyrirbyggja og takmarka tjón af völdum bilana og óheimils aðgangs að vinnslubúnaði, skal ábyrgðaraðili gripa til þeirra öryggisráðstafana sem við eiga hverju sinni, t.d.:

1. Stýra aðgangi að búnaði með úthlutun aðgangs- og lykilorða.
2. Dulköða eða eyða persónuauðkennum, eða að setja númer í stað persónuauðkenna og varðveita greiningarlykil með tryggum hætti.
3. Tryggja rekjanleika uppflettinga og vinnsluáðgerða.
4. Varðveita persónuupplýsingar á ónettengdri tölvu.
5. Takmarka aðgang að persónuupplýsingum við lesaðgang (uppflettaðgang), svo sem í þeim tilgangi að hindra óheimila eyðingu, afritun eða samkeyrslu.
6. Viðhafa sívirkar veiruvarnir.

IV. KAFLI
Innra eftirlit

8. gr.

Ábyrgðaraðili skal viðhafa innra eftirlit með vinnslu persónuupplýsinga til að ganga úr skugga um að unnið sé í samræmi við gildandi lög og reglur, þ.a.m. þá skilmála sem Persónuvernd hefur sett um viðkomandi vinnslu. Innra eftirlit skal m.a. beinast að:

1. Athugun á því hvort vinnslan sé heimil skv. lögum nr. 77/2000.
2. Hvort fullnægt hafi verið tilkynningar- eða leyfisskyldu þeirri sem kveðið er á um í lögnum.
3. Hvort uppfylltar séu reglur 7. gr. laganna um lögmæti vinnslu, þ.a.m. ákvæði 5. II. um eyðingu persónuupplýsinga sem ekki þarf að varðveita lengur, miðað við upphaflegan tilgang með söfnun þeirra.
4. Hvort virt séu í framkvæmd ákvæði um rétt hins skræða samkvæmt lögnum.
5. Hvort fylgt sé þeim öryggisráðstöfunum sem valdar hafa verið skv. c-lið 1. mgr. 3. gr. og III. kafla reglna þessara.

6. Innra eftirlit skal viðhafið með reglubundnum hætti. Tíðni eftirlitsins og umfang þess skal 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 skal þó eigi fara fram sjaldnar en árlega.

Að jafnaði skal viðhafa innra eftirlit samkvæmt fyrirfram skilgreindu kerfi.

Ábyrgðaraðili skal sja til þess að gerð sé skýrsla um hvern aðgerð sem er liður í innra eftirliti. Í slíkri skýrslu skal lýsa móturstöðu hvers þáttar eftirlitsins. Skýrslur um innra eftirlit skal varðveita tryggilega og hefur Persónuvernd rétt til aðgangs að þeim hvenær sem þess er óskað.

V KAFLI Vinnsluadili 9. gr.

Ábyrgðaraðili er heimilt að semja við tiltekinn aðila um að annast, í heild eða að hluta til, þá vinnslu persónuupplýsinga sem hann ber ábyrgð á. Slíkt er þó háð því skilyrði að ábyrgðaraðili hafi aður sannreynt að umráðsdur vinnsluadili geti viðhafið þær öryggisráðstafanir sem um vinnsluna gilda og framkvæmt innra eftirlit með vinnslunni.

Samningur skv. 1. mgr. skal vera skriflegur og i. að minnsta kosti tveimur eintökum. Þar skal m.a. koma fram að vinnsluadili skuli starfa í samræmi við fyrirmæli ábyrgðaraðila og að ákvæði reglna þessara um skyldur ábyrgðaraðila gildi einnig um þá vinnslu sem vinnsluadili framkvæmir. Ábyrgðaraðili og vinnsluadili skulu hvor varðveita sitt eintak af samningnum.

Hafi vinnsluadili staðfestu í öðru EES ríki en ábyrgðaraðili, skv. 1. mgr. 6. gr. laga nr. 77/2000, þá skal jafnframt geta þess í samningi að lög og reglur þess ríkis þar sem vinnsluadili hefur staðfestu, gildi um öryggisráðstafanir við vinnslu persónuupplýsinga.

Hverjum þeim er starfar í umboði ábyrgðaraðila eða vinnsluadila er aðeins heimilt að vinna með persónuupplýsingar í samræmi við fyrirmæli ábyrgðaraðila, nema lög mæli fyrir á annan vegg.

VI KAFLI Gildistaka o.fl. 10. gr.

Tilkynning til Persónuverndar um öryggisráðstafanir

Í tilkynningu til Persónuverndar skv. 31. gr. laga nr. 77/2000 skal koma fram með hvaða hætti ábyrgðaraðili fullnægir ákvæðum reglna þessara

11. gr. Gildistaka

Reglur þessar, sem settar eru samkvæmt heimild í 11. og 12. gr. laga nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga, bölast þegar gildi.

Persónuvernd, 20. mars 2001,
Páll Hreinsson stjórnarformaður.

1