Áhrif nýrrar persónuverndarlöggjafar á skólastarf

Málþing Persónuverndar og Háskóla Íslands
9. nóvember 2017
Háskólabíói

Vigdís Eva Líndal
skrifstofustjóri upplýsingaöryggis

Persónuvernd

Persónuvernd

Yfirlit

1. Nokkur mikilvæg hugtök
2. Hvað breytist ekki eftir maí 2018?
3. Skólastarf og GDPR - nýjar skyldur
4. Sérstök álitaefni í tengslum við skólastarf

Persónuvernd

Nokkur mikilvæg hugtök

Persónuupplýsingar

Å Hvers kyns upplýsingar um persónugreindan eða persónugreinanlegan einstakling

Å Nafn, kennitala, raðnúmer snjalltækja, staðsetningargögn, IP-tölur, o.fl.

Å Fjöldi breyta getur skipt máli

Å Almennar persónuupplýsingar – viðkvæmar persónuupplýsingar

Vinnsla

Å Sérhver aðgerð eða röð aðgerða þar sem persónuupplýsingar eru unnar, hvort sem vinnsla er sjálfvirk eða ekki.

Å Söfnun, leit, miðlun, skráning, varðveisla, samkeyrsla, eyðing, o.fl.

Persónuvernd

Nokkur mikilvæg hugtök

Ábyrgðaraðili

Å Aðili sem ákvarðar, einn eða í samvinnu við aðra, tilgang og aðferðir við vinnslu persónuupplýsinga

Å Sérhver leikskóli, grunnskóli, framhaldsskóli og háskóli sjálfstæðir ábyrgðaraðilar

Vinnsluaðili

Å Sá sem vinnur persónuupplýsingar á vegum ábyrgðaraðila

Å Upplýsingakerfi frá þriðja aðila, ekki einstakir starfsmenn skóla

ï T.d. Karellen, Mentor og Inna.

Persónuvernd

Hvað breytist ekki eftir maí 2018?

Þarf áfram að fylgja ákveðnum kröfum:

Å Hvaða heimild stendur til vinnslunnar?

—Lagaheimild/skylda - almannahagsmunir

—Samþykki

—Lögmætir hagsmunir

Å Er vinnslan lögmæt, gagnsæ, hófleg, áreiðanleg?

Å Hver er tilgangur vinnslunnar?

Å Veit einstaklingurinn/forráðamaður af vinnslunni?

Å Er búið að tryggja öryggi upplýsingana?

Å Hvar eru upplýsingarnar vistaðar og hvar má vista þær? Innan eða utan EES?

Persónuvernd

Skólastarf og GDPR – nýjar skyldur

Å *Ábyrgðarskylda*

Å Skrá yfir vinnslustarfsemi

Å Sjálfstæðar skyldur lagðar á vinnsluaðila

Å Mat á áhrifum á persónuvernd – DPIA

Å Öryggi við vinnslu – tilkynningar um öryggisbresti

Å Persónuverndarfulltrúi

Å Aukin réttindi einstaklinga – réttindi barna, samþykki, aðgangsréttur, sjálfvirk ákvarðanataka, o.fl.

Å Sektarheimildir

Persónuvernd

Ábyrgðarskylda

2. mgr. 5. gr. og 24. gr. GDPR

Ábyrgðaraðili er ábyrgur fyrir því að farið sé að meginreglum og **þarf að geta sýnt fram á það**

- ✓ Gera tæknilegar og skipulagslegar ráðstafanir
  - ï Mat á áhrifum á persónuvernd
  - ï Sjálfgefin og innbyggð persónuvernd
- ✓ Skjalfesting stefnu og verklagsreglna
  - ï Gerð skráar yfir vinnslustarfsemi
- ✓ Hlutverk persónuverndarfulltrúa

Persónuvernd

Skrá yfir vinnslustarfsemi

30. gr. GDPR

Å Yfirlit yfir alla vinnslu persónuupplýsinga í viðkomandi skóla

ï Efni og form

Å Bæði hjá ábyrgðaraðila og vinnsluaðila

ï Ítarlegri skrá hjá ábyrgðaraðilum

Å Aðgengileg Persónuvernd

Å Undantekning <250 starfsmenn, nema:

ï Vinnsla líkleg til að leiða af sér áhættu fyrir réttindi og frelsi hins skráða

ï Er ekki tilfallandi

ï Tekur til viðkvæmra persónuupplýsinga og upplýsinga um refsiverðan verknað

Persónuvernd

Notkun vinnsluaðila í skólastarfi

28. gr. GDPR

Å **Eingöngu heimilt ef:**

- ï *Nægilegar tryggingar* fyrir öryggi og réttindum einstaklinga
- ï *Vinnslusamningur* hefur verið gerður

Å **Efni vinnslusamnings**

- ï Viðfangsefni og tímalengd vinnslu
- ï Eðli og tilgangur
- ï Tegund persónuupplýsinga
- ï Flokkar skráðra einstaklinga
- ï Réttindi ábyrgðaraðila
- ï Sértæk ákvæði, m.a. um þagnarheit, öryggi, úttektir, fyrirmæli ábyrgðaraðila o.fl.

Å Brjóti vinnsluaðili í bága við ákvæði GDPR, þegar hann ákveður tilgang og aðferðir, telst hann ábyrgðaraðili

Persónuvernd

Sjálfstæðar skyldur vinnsluaðila

Å Tryggja **öryggi** upplýsinga

Å Halda **skrá yfir vinnslustarfsemi**

Å Tilkynna ábyrgðaraðila um **öryggisbrest**

Å Útnefna **persónuverndarfulltrúa**

Å Notkun **undirvinnsluaðila** (t.d. skýjaþjónustu) óheimil nema með samþykki ábyrgðaraðila

Å **Sektarheimildir** ná einnig til vinnsluaðila

Å Ítarlegri fyrirmæli um **efni vinnslusamnings** í 28. gr.

Persónuvernd

Mat á áhrifum á persónuvernd (DPIA)

35.-36. gr. GDPR

Hvenær?

Å Kerfisbundið og umfangsmikið mat á persónulegum þáttum eða eftirlit

Å Umfangsmikil vinnsla viðkvæmra persónuupplýsinga

⇒ Listar yfir vinnslu sem þarf ávallt að fara í mat á áhrifum væntanlegir

Hvað ef vinnsla er áfram mjög áhættusöm þrátt fyrir að öryggisráðstafanir hafi verið gerðar?

Å **Fyrirframsamráð** við Persónuvernd

⇒ Sjá nánar álit 29. gr. hópsins

Persónuvernd

Öryggi við vinnslu – tilkynningar um öryggisbrot

32.-34. gr. GDPR

Å Skólar og þeirra vinnsluaðilar þurfa að gera viðeigandi **tæknilegar og skipulagslegar ráðstafanir** til að tryggja öryggi

- ï Með dulkóðun, notkun gerviauðkenna, tryggja tiltækileika, álagsþol o.s.frv.
- ï Skipulagðir ferlar nauðsynlegir
- ï Innbyggð og sjálfgefin persónuvernd

Å **Skylda til að tilkynna öryggisbrot**

- ï Til Persónuverndar innan 72 klst.
- ï Til hins skráða/foreldra ef mikil áhætta
- ï Vinnsluaðilar þurfa að tilkynna til ábyrgðaraðila

Persónuvernd

Persónuverndarfulltrúi

37.-39. gr. GDPR

Å **Öll stjórnvöld**, þ.m.t. allir skólar
  ï Samnýting möguleg
Å Tiltekin fyrirtæki ef aðalstarfsemi er:
  ï Umfangsmikil, reglubundin og kerfisbundin vöktun á einstaklingum
  ï Umfangsmikil vinnsla viðkvæmra persónupplýsinga
Å Sérþekking á persónuverndarlöggjöf
Å Sjálfstæður og óháður
Å Starfsmaður – verktaki
Å Verkefni
  ï Reglufylgni, fræðsla, ráðgjöf, tengiliður

Persónuvernd

Aukin og ný réttindi einstaklinga

III. kafli GDPR

Å**Sérstök sjónarmið um börn**

- ï Börn eiga að njóta sérstakrar verndar
- ï Öll fræðsla á skýru og einföldu máli

ÅAuknar kröfur til **samþykkis**

Å**Aðgangsréttur**

Å**Andmælaréttur**

ÅRéttur til að **gleymast** *og* ***til leiðréttingar***

Å**Upplýsingaréttur** áður en vinnsla hefst

Å**Sjálfvirk ákvarðanataka**

Persónuvernd

Breytt eftirlit – sektarheimildir

VI. kafli GDPR

ÅÞátttaka persónuverndarstofnana í samevrópsku umhverfi

ï Einn afgreiðslustaður og samræmingarkerfi

Å Stórauknar sektarheimildir

ï Allt að 4% af árlegri heildarveltu eða 20 milljónum evra

ï Allt að 2% af árlegri heildarveltu eða 10 milljónum evra

ï Ná einnig til vinnsluaðila

Persónuvernd

Sérstök álitaefni í tengslum við skólastarf

ÅMyndbirtingar af börnum og notkun samfélagsmiðla

ï Sjá leiðbeiningar Persónuverndar

ÅNotkun á smáforritum (e. apps)

ÅMarkaðssetning í skólastarfi

ÅTölvuskýjalausnir

⇒ Lögmæti, meginreglur, öryggi, skýrt hlutverk vinnsluaðila, vinnslusamningar, mat á áhrifum, fræðsla

Persónuvernd

Frekari upplýsingar

- Vefsíða Persónuverndar um GDPR
- Vefsíða 29. gr. vinnuhópsins
- Vefsíða ICO (UK)
- Vefsíða Datatilsynet (NO)
- Vefsíða Datatilsynet (DK)
- Vefsíða Datainspektionen (SE)
- Vefsíða IC á Mön