Spurningalisti

Almennar spurningar um notkun á skýjaþjónustu

1. Nota grunnskólar sveitarfélagsins skýjaþjónustuveitendur í grunnskólastarfi eða hyggjast þeir gera það á næstunni (fyrir lok 2022)? Tilgreinið einungis skýjaþjónustuaðila sem vinna **persónuupplýsingar nemenda**.

2. Ef grunnskólar sveitarfélagsins nota skýjaþjónustuveitendur, er sveitarfélagið beðið um að veita eftirfarandi upplýsingar fyrir hvern skýjaþjónustuveitanda:

   Almennar upplýsingar um skýjaþjónustuveitandann og samning við hann

   a) Hvert er nafn skýjaþjónustuveitandans?
   b) Við hvaða lögaðila var samið um veitingu skýjaþjónustunnar og hvaða skýjaþjónustu var samið um?
   c) Hver er gildistími samningsins og allar dagsetningar endurnýjunar eða fyrirhugaðra breytinga á þjónustunni?
   d) Hvaða útfærsla af skýjaþjónustu er notuð (almennt ský, einkaský, blandað ský eða samfélagsský) og hvernig er þjónustulíkanið (SaaS, PaaS, IaaS eða DSaaS)?
   e) Hvaða lög gilda um samninginn?
   f) Var framkvæmt mat á áhrifum á persónuvernd fyrir vinnslu persónuupplýsinga hjá þessum skýjaþjónustuveitanda?

   Tegundir persónuupplýsinga sem unnar eru

   g) Hvaða flokka persónuupplýsinga er unnið með í skýinu? Er um að ræða viðkvæmar persónuupplýsinga, t.d. heilsufarsupplýsingar, eða persónuupplýsingar sem varða hrein einkamálefni einstaklinga, s.s. upplýsingar um félagslega stöðu?[1] Tilgreinið nánar.
   h) Persónuupplýsingar hverra eru unnar í skýinu (persónuupplýsingar nemenda, persónuupplýsingar foreldra, persónuupplýsingar kennara eða annarra)?
   i) Í hvaða tilgangi er þjónustan notuð (fyrir skrifstofu, samskipti, þjónustu við nemendur, foreldra eða kennara, þróun, netþjóna) og er sá tilgangur þáttur í grunnhlutverki grunnskóla?
   j) Vinnur skýjaþjónustuveitandinn fjarmælingar- eða greiningargögn? Tilgreinið flokka persónuupplýsinga sem um ræðir í því sambandi, t.d. IP-tölur. (Frekari spurningar um fjarmælingar- og greiningargögn er að finna hér fyrir neðan.)

[1] Sjá leiðbeiningar EDPB um mat á áhrifum á persónuvernd um mat á því hvort vinnsla er "líkleg til að leiða til mikillar áhættu" samkvæmt reglugerð 2016/679 (bls. 9).

Skilgreining hlutverka

k) Hvert er hlutverk sveitarfélagsins/grunnskólans og skýjaþjónustuveitandans samkvæmt samningi þeirra á milli, þ.e. telst viðkomandi vera ábyrgðaraðili, vinnsluaðili eða sameiginlegur ábyrgðaraðili?

l) Ef sveitarfélagið/grunnskólinn er ábyrgðaraðili en skýjaþjónustuveitandinn vinnsluaðili, liggur fyrir vinnslusamningur í samræmi við 3. mgr. 28. gr. reglugerðar (ESB) 2016/679? Athugið að spurt er um samningsskilmála vinnslusamninga í spurningu 13 og því þarf ekki að fjalla um þá hér.

m) Ef sveitarfélagið/grunnskólinn og skýjaþjónustuveitandinn eru sameiginlegir ábyrgðaraðilar, notar skýjaþjónustuveitandinn persónuupplýsingar, þ.m.t. fjarmælingar- og greiningargögn, í eigin tilgangi? Ef svo er, skal svara eftirfarandi spurningum:
    - Í hvaða tilgangi notar skýjaþjónustuveitandinn upplýsingarnar?
    - Hefur sveitarfélagið/grunnskólinn tekið tillit til þeirra upplýsinga sem skýjaþjónustuveitandinn notar í eigin tilgangi við mat á áhrifum persónuvernd?
    - Hver er vinnsluheimild fyrir vinnslu persónuupplýsinga á vegum skýjaþjónustuveitandans?

n) Notar skýjaþjónustuveitandinn undirvinnsluaðila? Ef svo er, tilgreinið nánar.

Öflun skýjaþjónustuveitanda

3. Lýsið ferlinu sem sveitarfélagið/grunnskólinn fylgdi (eða myndi fylgja), þ.m.t. mati á áhrifum á persónuvernd, við að greina hvaða skýjalausn hentaði þörfum sveitarfélagsins/grunnskólans og við að velja tiltekinn skýjaþjónustuveitanda. Tilgreinið einkum hvaða ófrávíkjanlegu skilyrði, ef einhver, voru sett varðandi persónuvernd til þess að mögulegur skýjaþjónustuveitandi kæmi til greina og hvort þau skilyrði hafi verið forsendur fyrir vali og samningi um notkun skýjaþjónustu.

4. Framkvæmir sveitarfélagið/grunnskólinn mat á áhrifum á persónuvernd eða biður um slíkt mat frá skýjaþjónustuveitanda áður en skýjaþjónusta er valin?
    - Ef svo er, hvenær í ferlinu, skv. spurningu 3, er matið framkvæmt og hvaða áhrif hefur niðurstaða þess við val á skýjaþjónustu? Hér er einkum spurt um hvaða áhrif greindar áhættur hafa, t.d. varðandi öryggi forrita og notendaskila, auðkenni og aðgangsstýringar, dulkóðun og lyklastjórnun, raunlægt öryggi, öryggi sýndarvéla og nethögunar, aðskilnað í rekstri og aðskilnað í samnýttum geirum, atvikastjórnun o.s.frv.
    - Ef sveitarfélagið/grunnskólinn hefur ekki framkvæmt mat á áhrifum á persónuvernd samkvæmt framangreindu er þess óskað að skýrt verði hvers vegna ekki var talið að vinnslan hefði í för með sér mikla áhættu fyrir réttindi og frelsi einstaklinga.

5. Byggir sveitarfélagið/grunnskólinn á íslenskum eða alþjóðleglegum stöðlum eða viðurkenndum starfsvenjum við mat á skýjaþjónustuveitendum, t.d. ISO 27001/ISO 27701, annað hvort sem þátt í eigin mati eða af því að sveitarfélagið/grunnskólinn krefst slíkrar vottunar? Ef skýjaþjónustan er vottuð, t.d. samkvæmt ISO-stöðlum, eða fylgir tilteknum hátternisreglum (e. code of conduct), hvaða upplýsingum um vottunina hefur þú aðgang að, t.d. vottunarskýrslu, og hversu oft?

6. Þegar sveitarfélagið/grunnskólinn semur um notkun skýjaþjónustu fyrir vinnslu persónuupplýsinga, hefur sveitarfélagið/grunnskólinn athugað hvar upplýsingarnar eru unnar, hvert þeim er miðlað, hvar þær eru vistaðar og hvaðan þær eru aðgengilegar?
    - Ef skýjaþjónustuveitandinn notar undirvinnsluaðila, hefur sveitarfélagið/grunnskólinn athugað hvert persónuupplýsingum, sem eru unnar af undirvinnsluaðilum, er miðlað, hvar þær eru vistaðar og hvaðan þær eru aðgengilegar?

7. Hefur sveitarfélagið/grunnskólinn upplifað áskoranir sem lúta að reglum, t.d. á grundvelli persónuverndarlöggjafarinnar, um notkun skýjaþjónustu? Ef það er raunin, tilgreinið þessar áskoranir og hvernig brugðist hefur verið við þeim.

8. Hefur sveitarfélagið/grunnskólinn samráð við persónuverndarfulltrúa sveitarfélagsins (óháð hugsanlegu samráði við persónuverndarfulltrúa skýjaþjónustuveitandans) þegar ákveðið skal hvaða skýjaþjónustuveitanda skuli samið við? Útskýrið hvers vegna (ekki).

9. Hefur sveitarfélagið/grunnskólinn einhvern tímann samið við skýjaþjónustuveitanda þrátt fyrir neikvæða umsögn eða ráðgjöf persónuverndarfulltrúa um annað?

Samningurinn við skýjaþjónustuveitandann

Svarið eftirfarandi spurningum með því að vísa til allra skýjaþjónustuveitenda sem taldir eru upp í svari við spurningu 1.

10. Ef sveitarfélagið/grunnskólinn og skýjaþjónustuveitandinn eru sameiginlegir ábyrgðaraðilar, var þá farið að ákvæðum 26. gr. reglugerðar (ESB) 2016/679? Útskýrið almennt með tilliti til þess hvernig tryggt hefur verið að skýjaþjónustuveitandinn uppfylli skyldur sínar samkvæmt reglugerðinni. Hafi verið gert samkomulag í samræmi við framangreint ákvæði óskar Persónuvernd þess að fá afrit þess afhent.

11. Ef skýjaþjónustuveitandinn er vinnsluaðili, var þá farið að ákvæðum 28. gr. reglugerðar (ESB) 2016/679? Útskýrið almennt með tilliti til þess hvernig tryggt hefur verið að skýjaþjónustuveitandinn uppfylli skyldur sínar samkvæmt reglugerðarinni. Þá óskar Persónuvernd þess að fá afrit vinnslusamnings afhent.

12. Er kveðið á um tilkynningar um öryggisbresti í samkomulagi/samningi við skýjaþjónustuveitandann?

13. Hefur sveitarfélagið/grunnskólinn samið við skýjaþjónustuveitandann í samvinnu við önnur sveitarfélög/grunnskóla eða aðra aðila? Ef svo er, hvaða áhrif hafði samvinnan á samningsskilmála?

14. Hefur sveitarfélaginu/grunnskólanum gengið vel að semja um ákvæði sem lúta að því að draga úr áhættu við vinnslu persónuupplýsinga?

- Lýsið niðurstöðu þar að lútandi, ef við á.
- Ef svarið er nei, skal útskýra ástæðurnar sem liggja því til grundvallar, þ.m.t. hugsanlegar hindranir sem upp komu í ferlinu.

15. Hefur sveitarfélagið/grunnskólinn gert þjónustusamning um skýjaþjónustuna? Ef svo er, er þar kveðið á um endurheimt þjónustu ef upp kemur bilun?

16. Hefur sveitarfélagið/grunnskólinn samið um eða gert skipulagslegar og/eða tæknilegar ráðstafanir til að takmarka vinnslu persónuupplýsinga af hálfu skýjaþjónustuveitandans, einkum í eigin þágu? Lýsið þeim ráðstöfunum, ef við á, og útskýrið ástæðurnar að baki þeim. (Frekari spurningar um miðlun persónuupplýsinga til þriðju landa er að finna hér fyrir neðan.)

17. Hefur sveitarfélagið/grunnskólinn gert einhverjar ráðstafanir til að tryggja að hægt sé að rifta samningi eða segja honum upp, t.d. ef ákveðið er að nota aðra skýjaþjónustu? Lýsið þeim ráðstöfunum, ef við á.

Upplýsingar um samninginn: Miðlun persónuupplýsinga til þriðju landa

Svarið eftirfarandi spurningum með því að vísa til allra skýjaþjónustuveitenda sem taldir eru upp í svari við spurningu 1.

18. Miðlar skýjaþjónustuveitandi og/eða undirvinnsluaðilar hans persónuupplýsingum til þriðju landa, þ.m.t. fjarmælingar- og greiningargögnum? Ef svarið er já, skal svara eftirfarandi spurningum.

19. Hefur sveitarfélagið/grunnskólinn gert eða samið um tæknilegar og/eða skipulagslegar ráðstafanir til að tryggja öryggi persónuupplýsinga við miðlun þeirra til þriðju landa í samræmi við ákvæði reglugerðar (ESB) 2016/679? Hefur sveitarfélagið/grunnskólinn mælt fyrir um að persónuupplýsingar skuli aðeins unnar á tilteknu svæði eða í tilteknum löndum? Ef svo er, lýsið þessum ráðstöfunum.

20. Ef sveitarfélagið/grunnskólinn miðlar persónuupplýsingum, þ.m.t. greiningar- eða fjarmælingargögnum, til þriðju landa, lýsið hvaða ráðstafanir hafa verið gerðar samkvæmt V. kafla reglugerðar (ESB) 2016/679. Er hinum skráðu veitt fræðsla um miðlunina í samræmi við f-lið 1. mgr. 13. gr., eða, ef við á, samkvæmt f-lið 1. mgr. 14. gr. reglugerðarinnar.

21. Ef sveitarfélagið/grunnskólinn hefur notast við staðlaða samningsskilmála (e. SSC), tilgreinið hvaða stöðluðu samningsskilmálar voru notaðir. Þá óskar Persónuvernd þess að fá afrit skilmálanna afhent.

22. Ef sveitarfélagið/grunnskólinn hefur notað staðlaða samningsskilmála við miðlun eða byggt á bindandi fyrirtækjareglum (e. BCR), hefur sveitarfélagið/grunnskólinn þá metið aðstæður í því landi sem um ræðir, meðal annars gildandi löggjöf sem lýtur að persónuvernd, og tekið afstöðu til

skilmálanna með hliðsjón af þeim aðstæðum, sbr. Schrems II dóm Evrópudómstólsins? Ef svo er, óskar Persónuvernd þess að fá afhent afrit af því mati.

23. Ef sveitarfélagið/grunnskólinn hefur komist að þeirri niðurstöðu að flutningsaðilinn geti í raun ábyrgst að hann uppfylli bindandi fyrirtækjareglur og/eða staðlaða samningsskilmála, lýsið þá í smáatriðum ástæðum fyrir þessari niðurstöðu og leggið fram gögn þar að lútandi, ef þau eru fyrir hendi.

24. Ef sveitarfélagið/grunnskólinn hefur komist að þeirri niðurstöðu að ráðstafanir vegna miðlunar skv. V. kafla reglugerðar (ESB) 2016/679 séu ófullnægjandi, þ. á m. staðlaðir samningsskilmálar eða bindandi fyrirtækjareglur, hefur þá verið íhugað að grípa til viðbótarráðstafana og ef svo er, hvaða ráðstafana? Hefur sveitarfélagið/grunnskólinn gengið úr skugga um hvort framkvæmanlegt sé að grípa til þessara viðbótarráðstafana og að ekkert í löggjöf þriðju landa komi í veg fyrir að þeim sé beitt til að tryggja að ekki sé grafið undan persónuvernd einstaklinga? Lýsið niðurstöðum þessa mats.

25. Hefur sveitarfélagið/grunnskólinn leitað ráðlegginga hjá persónuverndarfulltrúa sveitarfélagsins varðandi lagalegar kröfur um alþjóðlega miðlun persónuupplýsinga? Ef svo er, hverjar voru ráðleggingar persónuverndarfulltrúans?

26. Hefur sveitarfélaginu/grunnskólanum verið tilkynnt um beiðni stjórnvalda þriðju landa til skýjaþjónustuveitandans um aðgang að persónuupplýsingum? Ef svarið er já, hvert var innihald tilkynningarinnar?

Nánari upplýsingar um samninginn: Söfnun og vinnsla greiningar- eða fjarmælingargagna hjá skýjaþjónustuveitandanum

Svarið eftirfarandi spurningum með því að vísa til hvers skýjaþjónustuveitanda og undirvinnsluaðila hans, sem taldir eru upp í spurningum 1 og 2.

27. Ef skýjaþjónustuveitandinn safnar og vinnur greiningar- eða fjarmælingargögn vegna skýjaþjónustu, á hvern hátt fer sú söfnun og vinnsla fram?
    a. Er þessum gögnum safnað á tæki notanda eða á netþjónum skýjaþjónustuveitandans?
    b. Eru gögnin færð undir gerviauðkenni eða gerð ópersónugreinanleg?
        i. Ef gögnin eru færð undir gerviauðkenni,
            1. hvar á færslan sér stað? Á tæki notanda eða á netþjónum skýjaþjónustuveitanda?
            2. hvernig er færslan framkvæmd (tækni, auðkenni o.s.frv.)?
        ii. Ef gögnin eru gerð ópersónugreinanleg,
            1. hvar eru gögnin gerð ópersónugreinanleg? Á tæki notandans, eða á netþjónum skýjaþjónustuveitandans?
            2. hvernig eru gögnin gerð ópersónugreinanleg (tækni, hópunarstig (e. level of aggregation), eftir því sem við á)?

c. Er þessi gagnasöfnun sjálfgefin eða ekki? Ef svo er, hvaða stýringar býður skýjaþjónustuveitandinn upp á til að takmarka söfnun og vinnslu?
d. Hvaða öryggisráðstöfunum beitir sveitarfélagið/grunnskólinn til að vernda þessi gögn við miðlun, í minni og sem vistuð?

28. Safnar skýjaþjónustuveitandinn og vinnur greiningar- eða fjarmælingargögn eða aðrar upplýsingar vegna notkunar skýjaþjónustunnar, sem sveitarfélagið/grunnskólinn og/eða skýjaþjónustuveitandinn telja ekki vera persónuupplýsingar?

Hlítni

29. Vaktar sveitarfélagið/grunnskólinn viðeigandi tæknilegar og skipulagslegar ráðstafanir, þ.m.t. öryggisráðstafanir skýjaþjónustuveitandans, til að ganga úr skugga um að þær séu í samræmi við vinnslusamning/samkomulag og/eða alþjóðlega staðla? Lýsið ferlinu sem notað er við slíkt eftirlit.

30. Felur eftirlit, skv. spurningu 29, í sér reglulegt mat á áhrifum á persónuvernd, þ.m.t. reglulegt áhættumat upplýsingaöryggis varðandi framkvæmd skýjavinnslu? Ef svarið er já, hvernig fer eftirlitið fram, hvaða þættir samningsins/samkomulagsins eru vaktaðir og hversu oft?

31. Sinnir sveitarfélagið/grunnskólinn eftirliti með því hvernig skýjaþjónustuveitandinn uppfyllir almennt kröfur reglugerðar (ESB) 2016/679, umfram það sem sérstaklega hefur verið samið um, t.d. varðandi viðeigandi verndarráðstafanir vegna alþjóðlegrar miðlunar og þróun í réttarframkvæmd? Lýsið aðgerðum hvað þetta varðar.

Skilgreiningar

Almennt ský: (e. public cloud) Tölvuský sem þjónar fjölda aðila (fyrirtækjum, stofnunum eða öðrum aðilum) og er opið öllum sem vilja nýta auðlindir þess.

Blandað ský: (e. hybrid cloud) Samtengd tölvuský sem geta deilt auðlindum en eru í eigu aðskilinna eigenda.

DSaaS: (Data Storage as a Service) Skýjaþjónustuveitandi veitir notendum aðgang að geymslu gagna. Dæmi: OneDrive.

Einkaský: (e. private cloud) Tölvuský sem er ætlað til notkunar fyrir einn aðila (fyrirtæki, stofnun eða aðra aðila). Skýið getur verið hýst og rekið af sérhæfðum þjónustuaðila (skýjaþjónustuveitanda) eða af fyrirtækinu sjálfu.

Fjarmælingargögn: (e. telemetry data) Gögn sem verða til við notkun þjónustunnar, þ. á m. í öryggisskyni.

IaaS: (Infrastructure as a Service) Skýjaþjónustuveitandi veitir notendum aðgang að sýndarvélum. IaaS getur komið í stað netþjóna á starfsstöð. Dæmi: Elastic Compute Cloud (Amazon), Simple Storage Service, Green Qloud.

PaaS: (Platform as a Service) Skýjaþjónustuveitandi veitir notendum tiltekin stýrikerfi. Dæmi: Azure (Microsoft), Google App Engine, Facebook.

SaaS: (Software as a Service) Skýjaþjónustuveitandi veitir notendum möguleikann á að nota tiltekinn hugbúnað eftir þörfum. Dæmi: Office 365, Gmail, Google Drive, Google Docs, G-Suite, Hangouts.

Samfélagsský: (e. community cloud) Tölvuský sem eru sett upp fyrir tilstuðlan hóps aðila (fyrirtækja, stofnana eða annarra aðila) sem hafa svipaðra hagsmuna að gæta.

Skýjaþjónusta: (e. cloud service) Þjónusta sem felur í sér aðgang að vélbúnaði, stýrikerfum og hugbúnaði eftir þörfum notandans.