PERSÓNU VERND



Akraneskaupstaður
Stillholti 16-18
300 Akranesi

Reykjavík, 1. nóvember 2019

Tilvísun: 2019061186/VIS

**Efni: Ráðgjöf vegna fyrirhugaðrar opnunar bókhalds Akraneskaupstaðar og mats á áhrifum á persónuvernd**

*1. Erindi Akraneskaupstaðar*

Með tölvupósti 5. júní 2019 óskaði Akraneskaupstaður eftir fyrirframsamráði við Persónuvernd vegna fyrirhugaðrar enduropnunar bókhalds kaupstaðarins, en Persónuvernd hafði áður, með ákvörðun í máli nr. 2018/804, dags. 31. janúar 2019, komist að þeirri niðurstöðu að birting viðkvæmra persónuupplýsinga á vefsíðu Akraneskaupstaðar í tengslum við opið bókhald samrýmdist ekki eldri lögum nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga, auk þess sem öryggi við vinnslu persónuupplýsinga var ekki talið samrýmast 11. og 12. gr. laganna. Þá var gerð athugasemd við að vinnslusamningur hefði ekki verið gerður við KMPG ehf. í samræmi við 13. gr. laganna.

Með tölvupóstinum fylgdu drög að mati á áhrifum á persónuvernd vegna hinnar fyrirhuguðu vinnslu. Þar kemur fram að Akraneskaupstaður hyggist opna bókhald kaupstaðarins til að auka aðgengi að fjárhagsupplýsingum og skýra á myndrænan og einfaldan hátt ráðstöfun fjármuna hans. Akraneskaupstaður beri ábyrgð á vinnslunni og sé því ábyrgðaraðili í skilningi laga nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga.

*1.1. Lýsing fyrirhugaðrar vinnslu*

Fram kemur í erindi Akraneskaupstaðar að opnun bókhalds kaupstaðarins feli einkum í sér aðgang að fjárhagsbókhaldi, afritun gagna yfir í vinnslugrunn, afstemmingu og útgáfustýringu gagna, afmáningu persónuauðkenna gagna í vinnslugrunni og útgáfu ópersónugreinanlegra gagna í opnu bókhaldi. Þær persónuupplýsingar sem unnið verði með séu nöfn, kennitölur, heimilisföng, starfsmannaupplýsingar á borð við starfsheiti, laun, viðveru og stéttarfélag, upplýsingar um vörukaup og þjónustu, símanúmer og tölvupóstföng. Flokkar skráðra séu íbúar og viðskiptavinir Akraneskaupstaðar, starfsmenn, birgjar, tengiliðir samstarfsaðila, verktakar og þjónustuaðilar.

Tilgangur vinnslunnar sé að veita íbúum, fjölmiðlum og öðrum, sem láti rekstur sveitarfélaga sig varða, aukinn og einfaldari aðgang að rekstrarupplýsingum í anda opins lýðræðis og gagnsæis hjá hinu opinbera. Vinnslan byggi á heimild í c-lið 1. mgr. 6. gr. og 2. mgr. 9. gr. reglugerðar (ESB) 2016/679. Öll vinnsla muni fara fram á starfsstöð ábyrgðaraðila, Akraneskaupstaðar.

Flæði gagna frá fjárhagskerfi Akraneskaupstaðar yfir í Power BI-skýjaþjónustu Microsoft, sem til stendur að nýta til að gera fjárhagsupplýsingar aðgengilegar á vefnum, er útlistað í mati á áhrifum á persónuvernd. Fram kemur að frumskráning gagna, þar sem finna megi persónugreinanleg gögn, fari

fram í Navision-gagnagrunni Akraneskaupstaðar. Afrit af öllum gögnum sem þaðan verða flutt verði varðveitt og sérhver gagnaflutningur lotumerktur. Fram kemur að gögn, sem afrituð eru á færslustigi, kunni að innihalda persónugreinanlegar upplýsingar. Á þessu stigi verði gögn ekki dregin saman til að unnt sé að tryggja rekjanleika milli fjárhagskerfis og afstemmingarvinnu. Skilgreindur verði SQL-aðgangur með lesheimildir sem nái eingöngu til þeirra taflna og dálka er varði gagnaflutning frá fjárhagskerfi Akraneskaupstaðar yfir í afstemmningar og útgáfustýringu. Þá verði persónuauðkenni afmáð í gagnaflutningi, en skilgreining persónuauðkenna liggi hins vegar ekki fyrir á þessu stigi. Að þessu loknu verði öll þau gögn, sem birta á og sem heimilt er að birta opinberlega, afrituð í gagnagrunninn „Opið bókhald". Gögn verði dregin saman í gagnaflutningi og allar persónugreinanlegar upplýsingar afmáðar eftir settum reglum. Öll gögn, sem til stendur að birta opinberlega, verði því næst afrituð yfir í „Power BI Desktop". Þar verði framkvæmd aðgerðin „Publish to Web" sem feli í sér birtingu gagnanna á vefnum.

### *1.2. Mat á áhrifum á persónuvernd*

Í drögum að mati á áhrifum á persónuvernd kemur fram að í upphafi hafi áhætta á því að frumgögn verði aðgengileg öðrum verið talin mikil. Þörf hafi verið á úrbótum og litið hafi verið til þeirra mistaka sem gerð voru þegar bókhald Akraneskaupstaðar var opnað í apríl 2018. Gripið verði til eftirfarandi ráðstafana af því tilefni:

- Sérfræðingur fenginn til að undirbúa birtingu og vinnslusamningur gerður við hann.
- Dregið verði verulega úr magni persónuupplýsinga sem dregnar verði úr bókhaldskerfi Akraneskaupstaðar. Einungis þær upplýsingar sem þörf er á verði nýttar í gagnagrunn fyrir birtingu bókhaldsins til að fyrirbyggja að þar birtist persónugreinanlegar upplýsingar. Farið verði markvisst yfir hvaða upplýsingar sé nauðsynlegt að vinna með til að settu markmiði verði náð.
- Öryggisgirðingar verði settar upp og upplýsingar færðar milli ferla til að takmarka magn þeirra upplýsinga sem liggja muni til grundvallar birtum gögnum.
- Afritun gagna úr bókhaldskerfi kaupstaðarins og yfir í vinnslugrunn verði dulkóðuð (256 bit AES).

Þá verði aðgangi að gögnum stýrt á þann veg að það verði ekki umfram það sem raunverulega þarf hverju sinni og settar innbyggðar reglur um hópa sem ekki skuli koma til birtingar á vef Akraneskaupstaðar. Loks verði trúnaðaryfirlýsingar undirritaðar.

Fram kemur að í ljósi framangreindra ráðstafana verði litlar sem engar líkur taldar á því að hægt verði að persónugreina þær upplýsingar sem liggja munu til grundvallar birtingunni.

## *2. Um ákvörðun Persónuverndar í máli nr. 2018/804*

Líkt og að framan greinir var bókhald Akraneskaupstaðar opnað í apríl 2018. Samdægurs kom í ljós að unnt var að nálgast persónugreinanlegar upplýsingar í hinu opnu bókhaldi. Í kjölfar fréttaumfjöllunar um málið hóf Persónuvernd frumkvæðisathugun á því hvort birting upplýsinganna hefði verið í samræmi við þágildandi lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga.

Í svarbréfi Akraneskaupstaðar við bréfi Persónuverndar um upphaf fyrrnefndrar frumkvæðisathugunar kemur fram að rekja megi það, að unnt hafi verið að skoða undirliggjandi gögn í hinu opna bókhaldi sem voru persónugreinanleg, til þess að skýringarreitur í bókhaldi kaupstaðarins hafi ekki verið fjarlægður áður en gögnin voru afrituð í skýjaþjónustu í Power BI-umhverfi Microsoft. Í umræddum skýringarreitum hafi mátt finna nöfn skjólstæðinga sem skýringu á greiðslu. Öryggisbresturinn hafi því átt sér stað við útgáfu mælaborðsins og birtingu gagnanna á vefnum, þ.e. við aðgerðina „Publish to Web". Birtingarmynd öryggisbrestsins hafi verið sú að hægt hafi verið að „hægrismella" á myndræna framsetningu bókhaldsgagna og velja „See records". Þannig hafi hluti þeirra gagna sem lágu til grundvallar í skýjaþjónustu Power BI orðið aðgengilegur almenningi þrátt fyrir að hafa ekki verið sýnilegur í mælaborði opins bókhalds.

Niðurstaða Persónuverndar var sú að birtingin hefði verið andstæð ákvæðum laga nr. 77/2000. Þá var öryggi við vinnslu persónuupplýsinganna ekki talið í samræmi við ákvæði 11. og 12. gr. sömu laga auk þess sem ekki hefði verið gerður vinnslusamningur við KPMG ehf. líkt og skylt hefði verið, en félagið var sölu- og þjónustuaðili lausnarinnar Opið bókhald. Lagði Persónuvernd fyrir Akraneskaupstað að gera viðeigandi tæknilegar og skipulagslegar ráðstafanir sem tækju mið af eðli, umfangi, tilgangi og áhættu fyrir réttindi og frelsi skráðra einstaklinga, sbr. 23. gr. laga nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga. Þá var lagt fyrir Akraneskaupstað að gera vinnslusamning við KPMG ehf. Með bréfi til Persónuverndar, dags. 29. mars 2019, gerði Akraneskaupstaður grein fyrir því að kaupstaðurinn myndi ekki eiga samstarf við KMPG ehf. þegar bókhald bæjarins yrði opnað á ný. Af þeirri ástæðu hafi gerð vinnslusamnings við KPMG ehf. ekki farið fram. Með bréfi, dags. 12. apríl 2019, var Akraneskaupstað tilkynnt um að Persónuvernd teldi ekki þörf á frekari viðbrögðum stofnunarinnar vegna málsins.

## *3. Lagaumhverfi og sjónarmið*

### *3.1. Heimild til vinnslu og meginreglur laga nr. 90/2018*

Öll vinnsla persónuupplýsinga verður að falla undir eitthvert af heimildarákvæðum 9. gr. laga nr. 90/2018. Má þar nefna að vinna má með persónuupplýsingar sé það nauðsynlegt til að fullnægja lagaskyldu sem hvílir á ábyrgðaraðila. Ræðst það af aðstæðum hverju sinni hvort tiltekin vinnsla persónuupplýsinga teljist nauðsynleg og er ábyrgðaraðila falið visst mat í þeim efnum. Í erindi Akraneskaupstaðar kemur fram að sú vinnsla persónuupplýsinga, sem opnun bókhalds kaupstaðarins felur í sér, styðjist við c-lið 1. mgr. 6. gr. og 2. mgr. 9. gr. reglugerðar (ESB) 2016/679.

Auk heimildar samkvæmt framangreindu verður vinnsla persónuupplýsinga að fullnægja öllum grunnkröfum 1. mgr. 8. gr. laga nr. 90/2018, sbr. 5. gr. reglugerðar (ESB) 2016/679. Er þar meðal annars kveðið á um að persónuupplýsingar skuli unnar með sanngjörnum, málefnalegum og lögmætum hætti og að öll meðferð þeirra sé í samræmi við vandaða vinnsluhætti persónuupplýsinga. Þá skulu persónuupplýsingar unnar með þeim hætti að viðeigandi öryggi þeirra sé tryggt. Ábyrgðaraðili, sem í því tilfelli sem hér um er ræðir Akraneskaupstaður, ber ábyrgð á því að vinnsla persónuupplýsinga uppfylli ávallt ákvæði 1. mgr. 8. gr., sbr. 2. mgr. sömu greinar, og skal geta sýnt fram á það.

### *3.2. Fyrirframsamráð við Persónuvernd samkvæmt 30. gr. laga nr. 90/2018*

Í 1. mgr. 29. gr. laga nr. 90/2018 er kveðið á um að ábyrgðaraðili skuli láta fara fram mat á áhrifum fyrirhugaðra vinnsluaðgerða á vernd persónuupplýsinga áður en vinnslan fer fram, ef líklegt er að vinnslan geti haft í för með sér mikla áhættu fyrir réttindi og frelsi einstaklinga. Ef slíkt mat gefur til kynna að vinnsla myndi hafa mikla áhættu í för með sér, nema ábyrgðaraðili grípi til ráðstafana til að draga úr henni, skal ábyrgðaraðili hafa samráð við Persónuvernd áður en vinnslan hefst, sbr. 1. mgr. 30. gr. laga nr. 90/2018. Telji Persónuvernd að fyrirhuguð vinnsla mundi brjóta í bága við reglugerð (ESB) 2016/679, einkum ef ábyrgðaraðili hefur ekki greint eða dregið úr áhættunni með fullnægjandi hætti, skal stofnunin veita ábyrgðaraðila og, eftir atvikum, vinnsluaðila skriflega ráðgjöf og getur notað til þess allar valdheimildir sínar sem um getur í 41.-43. gr. laga nr. 90/2018.

## *4. Niðurstaða*

Af erindi Akraneskaupstaðar, ásamt drögum að mati á áhrifum á persónuvernd vegna fyrirhugaðrar opnunar bókhalds kaupstaðarins, má ráða að ýmsar úrbætur hafi verið gerðar á því verklagi sem viðhaft var við opnun bókhaldsins í apríl 2018. Fram kemur í erindinu að gætt verði að því að þau skilyrði, sem tilgreind voru í ákvörðun Persónuverndar í máli nr. 2018/804 og sem lýst er hér að framan, verði uppfyllt. Þannig er þess meðal annars getið að dregið verði úr magni persónuupplýsinga sem dregnar verða úr bókhaldskerfi, persónuauðkenni afmáð í gagnaflutningi og afritun gagna dulkóðuð.

Að mati Persónuverndar er, að svo stöddu, ekki ástæða til að ætla að sú vinnsla persónuupplýsinga sem felast mun í opnun bókhalds Akraneskaupstaðar eins og henni er lýst í erindi kaupstaðarins, muni brjóta í bága við ákvæði laga nr. 90/2018 eða reglugerðar (ESB) 2016/679. Persónuvernd telur þó rétt að árétta tiltekin atriði:

1. Skilgreina þarf persónuauðkenni og hvernig þau skuli afmáð áður en vinnsla hefst.
2. Tryggja þarf að fullnægjandi prófanir, þ.m.t. á virkni þeirrar hugbúnaðarlausnar sem notast er við, fari fram áður en að opnun bókhalds Akraneskaupstaðar kemur. Þá skulu slíkar prófanir einnig framkvæmdar með reglulegu millibili eftir að vinnsla hefst.
3. Ábyrgðaraðili skal einungis leita til vinnsluaðila sem veita nægilegar tryggingar fyrir því að þeir geri viðeigandi tæknilegar og skipulagslegar ráðstafanir til að vinnsla uppfylli kröfur reglugerðar (ESB) 2016/679 og að réttindi skráðra einstaklinga séu tryggð, sbr. 1. mgr. 25. gr. laga nr. 90/2018. Þá skal áréttað að á vinnsluaðila hvílir nú sjálfstæð skylda til að tryggja viðunandi öryggi persónuupplýsinga, sbr. 1. mgr. 27. gr. laga nr. 90/2018.
4. Ganga þarf frá vinnslusamningi við vinnsluaðila áður en vinnsla hefst, hafi ekki þegar verið gengið frá slíkum samningi.

Verði gætt að framangreindum atriðum og þeim ráðstöfunum, sem lýst er í erindi Akraneskaupstaðar og mati á áhrifum á persónuvernd, gerir Persónuvernd ekki athugasemd við að vinnsla persónuupplýsinga, sem felst í opnun bókhalds kaupstaðarins, hefjist. Byggist sú afstaða stofnunarinnar á því að þær forsendur sem lýst er í framangreindum gögnum standist. Loks áréttar Persónuvernd að ábyrgðaraðili ber ávallt ábyrgð á því að vinnsla persónuupplýsinga uppfylli ákvæði 1. mgr. 8. gr. laga nr. 90/2018, sbr. 2. mgr. sömu greinar.

F.h. Persónuverndar,

Helga Sigríður Þórhallsdóttir

Vigdís Sigurðardóttir