Fjármála- og
efnahagsráðuneytið

LEIÐBEININGAR TIL RÍKISSTOFNANA UM NOTKUN Á TÖLVUSKÝJALAUSNUM

Útgefið í nóvember 2016

Innihald

Inngangur

Undanfarið hefur orðið mikil þróun á þeirri tækni sem hefur verið nefnd skýjaþjónusta (e. Cloud Computing). Með skýjaþjónustu er átt við þjónustu þar sem notandinn getur sjálfur afgreitt sig á netinu, eftir þörfum hverju sinni, hvað varðar notkun á tölvukerfum, tölvuumhverfum eða tölvuinnviðum. Tækifæri til hagræðingar og til að auka sveigjanleika í rekstri hafa verið helstu drifkraftar í útbreiðslu á þessari högun upplýsingatækni, en meðal hindrana eru ýmis atriði er lúta að lögsögu, öryggi og stjórn gagna. Umræða um notkun opinberra aðila á skýjalausnum beinist einkum að áleitnum álitaefnum á sviði upplýsingaöryggis, þ. á m. um aðgengileika, varðveislu og leynd upplýsinga. Jafnframt þarf að huga að öðrum álitaefnum s.s. um um stjórn upplýsinga í skýinu og flutning þeirra úr landi.

Fjármála- og efnahagsráðuneytið, í samstarfi við Persónuvernd og Rekstrarfélag Stjórnarráðsins, hefur tekið saman gátlista um hverju stofnanir þurfi að huga að áður en tekin er ákvörðun um notkun tölvuskýja. Gátlistinn er lifandi skjal sem mun taka breytingum eftir því sem tækniframfarir, lög og reglur gefa tilefni til.
Hið opinbera hefur ekki mótað sér sérstaka stefnu um tölvuský en slík stefna getur haft áhrif á það hvaða upplýsingar kemur til álita að vista i tölvuskýjum.

Vakin er athygli á því að gátlistinn er einungis til leiðbeiningar fyrir ríkisstofnanir. Hann hefur ekki að geyma tæmandi talningu á öllum atriðum sem huga þarf að við innleiðingu tölvuskýjalausna.

Hagkvæmur rekstur

Tækifæri til hagræðingar og til að auka sveigjanleika í rekstri hafa verið helstu drifkraftar í útbreiðslu á skýjalausnum. Væntingar um lækkun rekstrarkostnaðar hafa verið algengasta ástæða þess að fyrirtæki og stofnanir taka upp skýjalausnir enda er almenna reglan sú að einungis er greitt fyrir mælda notkun. Engu að síður getur heildarkostnaður vegna tölvuskýja orðið hærri yfir lengri tíma og því ber að skoða rekstrarmálin vel áður en ákvörðun um notkun tölvuskýja er tekin. Líkt og með kaup á almennum vörum og þjónustu ber stofnunum að framfylgja lögum um opinber innkaup þegar samningar um skýjaþjónustu eru gerðir.

Upplýsingaöryggi

Forstöðumenn ríkisstofnana eru ábyrgir fyrir varðveislu og verndun upplýsinga sem varða starfsemi stofnananna. Útvistun tölvukerfa stofnana breytir ekki þeirra ábyrgð. Stofnanir þurfa að setja sér upplýsingaöryggisstefnu sem lágmarkar rekstraráhættu og hámarkar öryggi upplýsinga og verðmæta í eigu og umsjón þeirra. Tryggja þarf að þær kröfur sem upplýsingaöryggisstefna setur á samfellu í rekstri og verndun gagna sé mætt af þjónustuveitendum. Enn fremur þarf að huga að þeim lagaákvæðum sem gilda um meðferð gagna og að tryggt sé að útvistun uppfylli þær lagaskyldur sem settar eru.

Verndun persónuupplýsinga

Ákvörðun um notkun tölvuskýjalausna hjá ríkistofnunum byggist á því að gengið hafi verið úr skugga um að þjónustuveitandi geti framfylgt kröfum sem ríkisstofnun og persónuverndarlög gera. Ríkisstofnun ber að tryggja að hún geti áfram sinnt skyldum sínum, þ.m.t. farið með stjórn upplýsinganna, tryggt öryggi þeirra að undangengnu áhættumati sem leiðir í ljós hvort ávinningur af innleiðingu þjónustunnar sé það mikill að hann réttlæti flutning í skýið. Mikilvægt er að meta hvort flutningur persónuupplýsinga úr landi, ef tölvuský er vistað erlendis, er heimill sem og hvaða tegundir upplýsinga er ásættanlegt að flytja í skýið og þá hvers konar ský. Lykilatriði er að ríkisstofnanir viti hvar, hvernig og hverjir vinna persónuupplýsingar sem þær bera ábyrgð á.

Skref í innleiðingu skýjalausna

Ákvörðun ríkisstofnunar um að taka í notkun skýjalausn ber að vera vel ígrunduð og unnin með faglegum hætti. Við val á skýjalausnum skulu liggja fyrir skilgreindar þarfir stofnunar til slíkra lausna sem og kröfur hennar til fyrirkomulags og virkni skýjaþjónustunnar. Mikilvægt er að samningar um kaup á skýjaþjónustum séu rétt unnir og staðfesti kröfur stofnunar til þjónustunnar sem og ábyrgð þjónustuveitanda. Einnig er nauðsynlegt að tryggja að samningar um kaup á skýjaþjónustu og flutning upplýsinga úr landi samrýmist ákvæðum innlendra laga og reglna. Innleiðingaferli sem hér um ræðir má skipta í eftirfarandi skref:

Skref 1. Þarfagreining

Í upphafi þarf að skilgreina vel þau markmið sem innleiðingunni er ætlað að ná og meta hvort ætlaður ávinningur skýjaþjónustu nái þeim markmiðum betur en aðrir valkostir. Rétt er að skilgreina vel þarfir og kröfur áður en tiltekin lausn verður fyrir valinu. Við ákvörðunina þarf að skoða gaumgæfilega hvaða tegundir upplýsinga er fyrirhugað að færa í skýjaþjónustu og kanna hvaða kröfur lög og reglugerðir setja um verndun, öryggi og staðsetningu upplýsinga. Sérstaklega þarf að skilgreina kröfur um útfærslur, öryggi, afhendingu þjónustu og meðferð gagna.

Skref 2. Áhættumat

Mikilvægt skref í innleiðingu skýjalausnar er áhættumat og á það sérstaklega við ef um er að ræða upplýsingar sem falla undir lög um persónuvernd eða önnur viðkvæm gögn t.d. trúnaðargögn. Í áhættumati eru áhættuþættir greindir og skoðaðir með hliðsjón af trúnaðarstigi, lögum og reglum sem við eiga. Markmið áhættumats er að leiða í ljós hvort forsendur séu til staðar fyrir flutning gagna í tölvuský og þá hvernig tölvuský. Niðurstöður áhættumats skulu bornar upp á móti metnum ávinningi með innleiðingu skýjalausnar. Forsenda fyrir innleiðingunni er að ávinningurinn sé meiri en áhættan.

Skref 3. Kröfulýsing

Í kröfulýsingu eru settar fram kröfur um fyrirkomulag og virkni þjónustunnar í samræmi við lagaákvæði og kröfur um verklag. Kröfurnar lúta að atriðum á borð við rekstrarsamfellu, innra og ytra öryggi, þjónustuferla, meðhöndlun frávika, vottanir, flytjanleika gagna (þ.e. flutning milli þjónustuaðila) og afritun, varðveislu og eyðingu gagna.

Skref 4. Samningagerð

Kaup á skýjaþjónustu skulu staðfest með þjónustu- og vinnslusamningi. Slíkum samningi er ætlað að tryggja það að þjónustuveitandi veiti þjónustuna með þeim hætti sem óskað er eftir, hvað varðar innihald hennar, verndun persónuupplýsinga og öryggi gagna. Í samningnum er lýsing á þjónustunni, takmörkunum hennar og skiptingu ábyrgðar. Tryggja þarf að samningsskilmálar séu ásættanlegir og þeir brjóti ekki gagnvart gildandi lögum. Mikilvægt er að þjónustu- og eftir atvikum vinnslusamningurinn tryggi eignarhald upplýsinga og aðgengi að gögnum.

Gátlisti vegna fyrirhugaðrar innleiðingar á skýjaþjónustu

Ákvörðun um notkun tölvuskýjalausna hjá ríkisstofnunum er háð sérstöku mati hverju sinni. Ómögulegt er að setja fram tæmandi gátlista sem á jafnt við um allar ríkisstofnanir. Eftir sem áður eru settar fram leiðbeiningar í eftirfarandi gátlista um atriði sem huga ber að í þessu sambandi. Í gátlistanum er jöfnum höndum vísað til þess aðila sem veitir tölvuskýjaþjónustu sem þjónustuaðila og vinnsluaðila.
Athygli er vakin á því að ákvörðun um notkun tölvuskýjalausna og eftir atvikum flutning persónuupplýsinga úr landi er ávallt á ábyrgð þeirrar ríkisstofnunar sem tekur slíka ákvörðun.

Ábyrgð

Ábyrgðaraðili er sá aðili, í þessu tilviki sú ríkisstofnun, sem ákveður tilgang vinnslu, þann búnað sem notaður er, aðferð við vinnsluna og aðra ráðstöfun upplýsinga (sbr. l. nr. 77/2000.) Ábyrgðaraðilar (stofnanir) geta útvistað þjónustum en ekki ábyrgð sem viðkomandi ber. Ábyrgðaraðila ber að tryggja að þjónustu- og vinnsluaðili uppfylli kröfur sem ábyrgðaraðili gerir um útfærslu, öryggi, afhendingu þjónustu og meðferð gagna.

Þjónustu- og vinnsluaðili

Ábyrgðaraðili getur samið við þjónustu- og vinnsluaðila um að hann vinni, þ.m.t. hýsi, persónuupplýsingar fyrir ábyrgðaraðila í heild eða að hluta. Þjónustu- og vinnsluaðili skal einungis vinna með persónuupplýsingar í samræmi við skýr fyrirmæli ábyrgðaraðila sem fram koma í sérstökum vinnslusamningi milli aðila (sbr. 13. gr. l. nr. 77/2000). Ábyrgðaraðila ber að sannreyna að þjónustu- og vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit áður en honum er falin vinnsla, eða eftir atvikum hýsing, persónuupplýsinga. Ábyrgðaraðili skal tryggja að þjónustu- og vinnsluaðili hafi skjalaðar verklagsreglur, öryggisferla og viðbragðsáætlanir varðandi eigin starfsmenn.

Áhættumat

Ábyrgðaraðili skal framkvæma skriflegt áhættumat, á þeirri tölvuskýjaþjónustu sem hefur orðið fyrir valinu, áður en ákvörðun er tekin um útvistun þjónustu í tölvuský, í þeim tilgangi að meta hvaða áhætta fylgir því að innleiða þjónustuna. Áhættumat er mat á hættunni á því að óviðkomandi fái aðgang að upplýsingum, 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 gagna sem veittri skýjaþjónustu er ætlað að ná til. Markmið áhættumats er að skapa forsendur fyrir vali á öryggisráðstöfunum. Þá skal tilgreina hvað geti farið úrskeiðis, hvaða áhrif slíkt geti haft á öryggi upplýsinganna og hvaða líkur séu á slíku sbr. reglur nr. 299/2001 um öryggi persónuupplýsinga.
Við gerð áhættumats skal horft til persónuverndarsjónarmiða sbr. lög og reglur um persónuvernd sem og til krafna vegna varðveislu gagna skv. stjórnsýslu- og upplýsingalögum. Skoða skal m.a. sérstaklega eftirfarandi atriði:

1. Meta skal hvaða tegund skýs felur í sér minnsta áhættu fyrir ríkisstofnun
2. Meta skal hættu á óviðkomandi aðgengi að persónuupplýsingum.
3. Meta skal hvort um skerðingu verði að ræða gagnvart öryggi persónuupplýsinga.
4. Vottanir þjónustuaðila gagnvart viðurkenndum stöðlum um upplýsingaöryggi, t.d. ISO 27001
5. Meta skal áhættu gagnvart samfelldum rekstri þjónusta, s.s. vegna netaðgengis og rekstraröryggis innri kerfa þjónustuaðila.
6. Tryggja skal að þjónustu- og vinnsluaðili afhendi ekki þriðja aðila, s.s. undir-vinnsluaðila, gögn ábyrgðaraðila til frekari vinnslu eða varðveislu án samþykkis ríkisstofnunar.
7. Ábyrgðaraðili skal meta áhættu þess við útvistun þjónustu í tölvuský, að meðhöndlun trúnaðarskjala uppfylli ákvæði laga og reglna.
8. Ábyrgðaraðili skal meta kostnað við útvistun þjónustu í tölvuský, bæði hvað varðar breytinguna við útvistunina sjálfa sem og kostnað vegna þjónustunnar.
9. Önnur atriði sem eru mikilvæg með tilliti til eðlis upplýsinga og starfsemi aðila hverju sinni.

Ávinningur af innleiðingu þjónustunnar skal vera nægilega mikill til að réttlæta áhættuna sem fylgir notkun tölvuskýjalausna. Þá er ekki sjálfgefið að útvistun viðkvæmra persónuupplýsinga sé heimil, s.s. upplýsinga um heilsufar, lyfja-, áfengis eða vímuefnanotkun, félagsleg vandamál o.s.frv.

Ábyrgðaraðili skal reglubundið endurtaka áhættumat meðan á útvistun þjónustu stendur.

Þjónustu- og vinnslusamningur

Ábyrgðaraðili skal gera skriflegan þjónustu- og vinnslusamning við þjónustuaðila, sbr. 13. gr. l. nr. 77/2000, sem tilgreinir að þjónustu- og vinnsluaðili megi einungis starfa í samræmi við fyrirmæli ábyrgðaraðila m.a. varðandi stjórn upplýsinga, flutningi úr landi, fyrirmæli um öryggi, uppsagnarákvæði og úrlausn ágreiningsmála. Ábyrgðaraðili skal forðast að gera samning sem hefur langan bindandi gildistíma. Ábyrgðaraðili skal tryggja að öll sömu ákvæði gildi um undirverktaka á vegum þjónustuaðila og gilda um þjónustuaðilann sjálfan.
Mögulegt er að útbúa tvo aðskilda samninga vegna veitingar tölvuskýjaþjónustu, þ.e. annars vegar þjónustusamning sem þjónustuveitandi útbýr og hins vegar vinnslusamning sem viðkomandi stofnun útbýr. Ef um tvo aðskilda samninga er að ræða þá gangi ákvæði vinnslusamnings framar ákvæðum þjónustusamnings. Í þjónustu- og vinnslusamningi ber m.a. að huga að eftirfarandi atriðum:

Almenn atriði

- Uppsagnarákvæði og úrlausn ágreiningsmála.
- Kostnaður vegna útvistunar og notkunar þjónustu.
- Lýsing á þjónustu og takmarkanir á henni.
- Almennar skyldur og ábyrgðir þjónustuaðila gagnvart veitingu þjónustu.
- Gildistími þjónustu og viðbrögð við uppsögn, t.d. hvað varðar endurheimt og eyðingu gagna.
- Greiðslur og greiðsluskilmálar.
- Óviðráðanleg atvik (force majeure).
- Trúnaður og þagnarskylda.
- Ágreiningsmál og úrlausn þeirra.

Atriði er lúta að verndun persónuupplýsinga

- Fyrirmæli ábyrgðaraðila um að þjónustu-/vinnsluaðila sé einungis heimilt að starfa í samræmi við fyrirmæli ábyrgðaraðila.
- Skyldur og ábyrgð þjónustuaðila um þá vinnslu persónuupplýsinga sem hann framkvæmir, þ.m.t. um öryggisráðstafanir sem ábyrgðaraðili gerir kröfu um samkvæmt niðurstöðum áhættumats og að þjónustu- og vinnsluaðili vinni ekki með gögn í öðrum tilgangi en um hefur verið samið.
- Ákvæði um samþykki ábyrgðaraðila fyrir hvers kyns breytingum á þjónustunni s.s. ef flytja á persónuupplýsingar milli landa og/eða þjónustuaðila.
- Réttur ábyrgðaraðila til stjórnunar upplýsinga er þjónusta nær til.

Fyrirkomulag þjónustu

- Aðgengi ábyrgðaraðila að þjónustu þjónustusala.
- Breytingarstjórnun gagnvart innihaldi og fyrirkomulagi þjónustu.
- Upplýsingagjöf vegna frávika og atvika í rekstri þjónustu og viðbragða við þeim.
- Heimildir ábyrgðaraðila til þess að vakta, rýna og fylgjast með þjónustu þjónustusala.
- Eftirlit þjónustuaðila með notkun ábyrgðaraðila á þjónustu.
- Ábyrgð undirverktaka og upplýsingaskylda þjónustu- og vinnsluaðila gagnvart ábyrgðaraðila.
- Framsal þjónustu.
- Áhættumat aðila og viðbrögð við þeim.
- Höfundarréttur gagna sem eru í þjónustu þjónustuaðila.

Flutningur úr landi

Flutningur persónuupplýsinga í gagnaver eða tölvuský sem vistuð eru innan EES svæðisins er almennt heimill. Sömuleiðis flutningur til þeirra ríkja sem nefnd eru í auglýsingu nr. 228/2010, um flutning persónuupplýsinga til annarra landa. Flutningur til annarra ríkja utan ESB og EES er *óheimill* nema samkvæmt einhverri heimild í 30. gr. l.

nr. 77/2000, s.s. samþykki einstaklinga eða leyfis Persónuverndar. Hið opinbera hefur ekki mótað sér sérstaka stefnu um tölvuský en slík stefna getur haft áhrif á það hvaða upplýsingar kemur til álita að vista i tölvuskýjum.

Sé þjónustu- og vinnsluaðili aðili að s.k. Privacy-Shield samkomulagi milli framkvæmdastjórnar Evrópu og bandarískra yfirvalda er flutningur til hans heimill á grundvelli samkomulagsins.
Flutningur ópersónulegra upplýsinga og annarra gagna úr landi er almennt heimill nema sérstaklega sé kveðið á um annað í lögum.
Vakin er athygli á því að niðurstaða áhættumats getur engu að síður valdið því að flutningur gagna úr landi feli í sér óásættanlega áhættu.

Trúnaðarflokkun

Ábyrgðaraðili skal greina þær tegundir upplýsinga sem fyrirhugað er að vista í tölvuskýi, þ.e. hvort um persónuupplýsingar er að ræða og ef svo er, hvort um almennar eða viðkvæmar persónuupplýsingar sé að ræða og framkvæma trúnaðarflokkun á gögnum í þeim tilgangi að meta hvort hýsing í tölvuskýi sé möguleg og tryggja að fyrirkomulag þjónustu uppfylli lagaleg ákvæði og sé ásættanleg af hans hálfu.

Sérstaklega er kveðið á um meðferð trúnaðarmerktra gagna í reglugerð nr. 959/2012, um vernd trúnaðarupplýsinga, öryggisvottanir og öryggisviðurkenningar á sviði öryggis- og varnarmála. Slík gögn má ekki flytja úr landi nema á grundvelli sérstakrar heimildar.

Eignarhald og stjórn upplýsinga

Ábyrgðaraðili skal tryggja að eignarhald, stjórn upplýsinga og aðgengi að gögnum sé varið í vinnslusamningi og á hans hendi svo að þjónustusali eða þriðji aðili geti ekki takmarkað aðgengi með neinum hætti eða unnið upplýsingar frekar hvort sem er vegna ágreinings eða af öðrum ástæðum. Ábyrgðaraðili fer með stjórn upplýsinga samkvæmt vinnslusamningi. Í því felst m.a. að tryggja aðgengi og leynd þegar það á við og að upplýsingar séu ekki unnar í öðrum tilgangi af þjónustuaðila en um var samið, eða gögn flutt milli netþjóna, vinnsluaðila eða ríkja án heimildar ábyrgðaraðila. Ábyrgðaraðili skal geta fullnægt upplýsingaskyldu sinni gagnvart einstaklingum sbr. 20. og 21. gr. laga nr. 77/2000.

Gagnaheilindi

Ábyrgðaraðili skal tryggja að þjónustu- og vinnsluaðili geri viðeigandi ráðstafanir til að tryggja heilindi gagna til samræmis við vægi vinnslu og trúnaðarflokkun gagna s.s. með dulkóðun og samtölugreiningu.

Raunlægt öryggi

Ábyrgðaraðili skal tryggja að þjónustu- og vinnsluaðili viðhafi ásættanlegar, skipulagslegar og tæknilegar öryggisráðstafanir varðandi raunlægt aðgengi að hýsingaraðstöðu (húsnæði).

Innra öryggi

Ábyrgðaraðili skal tryggja að eigin innviðir styðji við örugga notkun á þjónustu- og vinnsluaðila og öryggisferla s.s. varðandi vírusvarnir á útstöðvum, meðhöndlun lykilorða og verklag notenda. Ábyrgðaraðili skal tryggja að notendur séu upplýstir um hvaða gögn sé heimilt að vinna með í umhverfi þjónustuaðila og hvaða takmarkanir gildi.

Eftirlit

Ábyrgðaraðili skal tryggja að honum og eftirlits- og úttektaraðilum á hans vegum sé ávallt heimill aðgangur að hýsingaraðstöðu (húsnæði) þjónustuaðila, að afla gagna og framkvæma úttekt á þjónustu þjónustu- og vinnsluaðila.

Þjónustuviðmið

Ábyrgðaraðili skal tryggja að í samningnum séu skilgreind þjónustuviðmið í samræmi við kröfur ábyrgðaraðila (e. Service Level Agreement, SLA) og skilgreind viðbrögð ef þeim er ekki mætt.

Meðferð gagna / Varðveisla og eyðing

Ábyrgðaraðili skal tryggja að gögn séu ekki varðveitt lengur en heimilt er og að öllum gögnum hjá þjónustu- og vinnsluaðila sé eytt eftir að viðskiptasambandi lýkur.

Gagnaflutningur

Ábyrgðaraðili skal tryggja að í vinnslusamningi við þjónustu- og vinnsluaðila sé kveðið á um örugga meðferð við móttöku og afhendingu gagna hvenær sem er á samningstíma. Ábyrgðaraðili skal tryggja að gögn verði afhent með öruggum hætti og á því formi að mögulegt sé að færa þjónustu milli þjónustuaðila og afhenda til varðveislu hjá Þjóðskjalasafni.

Trúnaður

Ábyrgðaraðili skal útbúa og varðveita trúnaðaryfirlýsingar sem starfsmenn þjónustu- og vinnsluaðila undirrita, og eftir atvikum þriðju aðilar á vegum hans, ef unnið er með viðkvæmar upplýsingar eða önnur gögn sem eru skilgreind sem trúnaðargögn af hálfu ábyrgðaraðila.

Samfella í rekstri

Ábyrgðaraðili skal tryggja að þjónustu- og vinnsluaðili hafi skjalaða viðbragðsáætlun til að bregðast við áföllum og tryggja samfellu í rekstri ábyrgðaraðila. Ábyrgðaraðili skal einnig viðhalda eigin viðbragðsáætlun sem tekur m.a. til afrita af gögnum og verklag fyrir viðlagaáætlun (e. Disaster Recovery).

Þjónustuferlar

Ábyrgðaraðili skal tryggja að þjónustu- og vinnsluaðili hafi skilgreint ferli til að taka við, skjala og vinna úr þjónustubeiðnum og rekstrarfrávikum. Ábyrgðaraðili skal tryggja að samskiptaleiðir og upplýsingagjöf frá þjónustuaðila sé vel skilgreindar og skilvirkar.

Vottanir

Ábyrgðaraðili skal leitast við að þjónustu- og vinnsluaðili starfi eftir vottuðum stjórnunarstöðlum sem eru viðeigandi fyrir þá þjónustu sem um ræðir, sem dæmi ISO 27001:2013, ISO 27017:2015, ISO 27018:2014.

Frávik

Ábyrgðaraðili skal tryggja að þjónustu- og vinnsluaðili upplýsi um öll öryggis- og rekstrarfrávik sem koma upp.

Afritun

Ábyrgðaraðili skal tryggja að afrit af gögnum sé til á öruggum og aðgengilegum stað annarsstaðar en hjá þjónustuaðila frumgagna.

Uppsögn og lok samnings

Við uppsögn og lok samnings ber ríkisstofnunum að tryggja að þjónustu- og vinnsluaðli eyði öllum gögnum og öllum afritum þeirra sem honum var falið að vinna fyrir stofnunina.