FJÁRMÁLAEFTIRLIT

Gátlisti vegna innleiðingar skýjalausna hjá eftirlitsskyldum aðilum

Samkvæmt 1. mgr. 8. gr. laga nr. 87/1998 um opinbert eftirlit með fjármálastarfsemi ber eftirlitsskyldum aðilum að haga starfsemi sinni í samræmi við heilbrigða og eðlilega viðskiptahætti. Jafnframt má af 2. mgr. 10. gr. laganna leiða skyldu sömu aðila til þess að halda hag og rekstri sínum heilbrigðum.

Mikilvægt er að eftirlitsskyldir aðilar kynni sér og meti þær áhættur sem fylgja útvistun á upplýsingakerfum og skýjalausnum. Eftirlitsskyldir aðilar verða að huga að öryggi upplýsingakerfa þar sem mikil ábyrgð er lögð á þá aðila sem treyst er fyrir persónuupplýsingum og upplýsingum um fjárhagsmálefni aðila.

Fjármálaeftirlitið hefur sett leiðbeinandi tilmæli um upplýsingakerfi eftirlitsskyldra aðila nr. 1/2019 sem og um útvistun hjá eftirlitsskyldum aðilum nr. 6/2014. Með nefndum tilmælum er stefnt að því að samræmdar kröfur verði gerðar til allra eftirlitsskyldra aðila varðandi rekstur upplýsingakerfa og notkun upplýsingatækni. Sömu kröfur eru gerðar þó svo rekstri kerfanna sé útvistað. Megintilgangur tilmælanna er að lágmarka rekstraráhættu og stuðla að eftirfylgni eftirlitsskyldra aðila við lög og reglur er lúta að rekstri upplýsingakerfa. Jafnframt er að finna í hinum ýmsu sérlögum auknar kröfur um meðhöndlun gagna og varðveislu þeirra.

Fjármálaeftirlitið mælist til þess að eftirlitsskyldir aðilar fylli út eftirfarandi gátlista og skili honum til stofnunarinnar 30 dögum áður en áætlað er að taka skýjalausn í notkun, í þeim tilgangi að meta í samvinnu við Fjármálaeftirlitið, hvort viðkomandi skýjalausn standist þær kröfur sem gerðar eru til upplýsingakerfa eftirlitsskyldra aðila og útvistun þeirra.

Dagsetning / *Date* **Eftirlitsskyldur aðili / *Undertaking***

_____ _____

1. Tegund þjónustu / *Type of service*

1.1 Hvernig skýjaþjónustu mun fyrirtækið notast við? / *What kind of service is the undertaking considering implementing? (Namely IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service) or SaaS (Software-as-a-Service))*

1.2 Um hvernig ský er að ræða? / *Type of cloud?*

1.3 Hvað heitir skýjalausnin? / *What is the name of the cloud solution in question?*

1.4 Hvaða þjónustu er verið að kaupa? / *What kind of solution is being bought from the cloud provider?*

1.5 Hvaða gögn verða geymd í skýjalausninni? / *What data is to be stored in the cloud solution?*

2. Aðgengi / Access

2.1 Hafa kerfisstjórar eftirlitsskylds aðila aðgang að gögnum félagsins í skýinu? / *Do system managers of the undertaking have access to its data in the cloud?*

2.2 Felur skýjalausnin í sér að hýsingaraðili eða kerfisstjórar hans hafi aðgang að eða geti yfirfarið vistuð gögn eftirlitsskylds aðila? / *Does the cloud solution provide the service provider or its system managers with access or ability to review data stored in the cloud?*

2.3 Er aðila/aðilum utan skýjalausnaaðilans veittur aðgangur að upplýsingakerfum sem notuð eru við geymslu og vinnslu gagna? / *Are any parties or subcontractors outside of the cloud service provider granted access to the IT systems used to store and process data?*

☐ Já ☐ Nei

2.3.1 Ef svar við 2.3 er *já*; er til staðar skriflegur samningur sem tryggir fylgni við þær öryggiskröfur sem gerðar eru til eftirlitsskyldra aðila? / *If the answer to 2.3 is yes; is there a written contract in place to ensure compliance with the security requirements required of regulated entities?*

2.3.2 Ef svar við 2.3 er já; hvert er eðli þess aðgengis sem utanaðkomandi aðila er veitt? */ If the answear to 2.3 is yes; what is the nature of the access granted to a third party?*

2.4 Er aðgengi Fjármálaeftirlitsins að gögnum hýstum í skýjalausnum tryggt, í samræmi við 3. kafla leiðbeinandi tilmæla nr. 1/2019 um upplýsingakerfi eftirlitsskyldra aðila? / *Is the access of supervisors ensured, in accordance with chapter 3 in Guidelines no. 1/2019 on the IT systems of regulated entities?*
Að mati Fjármálaeftirlitsins er nauðsynlegt að í þjónustusamningi eða skilmálum um hluteigandi skýjalausn sé ákvæði um aðgang eftirlitsaðila. */ In the view of the Supervisor it is crucial to have a provision in the service agreements or terms of service ensuring Supervisory access.*

2.5 Liggur fyrir hvaða upplýsingum hýsingaraðili safnar um hinn eftirlitsskylda aðila og hvernig þær upplýsingar eru nýttar? / *What information does the cloud solution provider collect about the regulated entity and how is that information used?*

2.6 Veitir hýsingaraðili þriðja aðila, s.s. undirverktökum eða samstarfsaðilum, upplýsingar um gögn eða vinnslu félagsins, m.a. til að nota við markaðssetningu? / *Does the cloud solution provider grant access to any third parties, e.g. subcontractors or other affiliates, information regarding the data stored or processed, including for marketing purposes?*

☐ Já ☐ Nei

2.6.1. Ef svarið við 2.6 er *já*; hvert er eðli og umfang þeirra upplýsinga sem veittar eru? / *If the answear to 2.6 is yes; what is the nature and scope of the information provided?*

2.7. Hvaða aðferðir eru notaðar við auðkenningu og heimildagjöf notenda? / *What methods are used for authentication and authorisation of users?*

3. Áhættumat / *Risk assessment*

3.1 Hefur fyrirtækið framkvæmt áhættumat vegna innleiðingar skýjalausnarinnar? / *Has the undertaking performed a risk assessment with regard to the implementation of the cloud solution?*
Mikilvægt er að eftirlitsskyldir aðilar framkvæmi eigið áhættumat vegna innleiðingar og notkunar skýjalausna, en styðjist ekki aðeins við áhættumat framkvæmt af þjónustu- eða útvistunaraðila. / *It is important that the regulated entity performs their own risk assessment and not only rely on the risk assessment of the service provider.*

3.2 Hafa helstu áhættur við innleiðinguna verið metnar? / *Have the main risks of implementation been assessed?*
Helstu áhættur ættu að koma fram í áhættumati félagsins vegna innleiðingu lausnarinnar. / *Main risks should be identified in the undertakings implementation risk assessment*.

3.2.1. Hvernig er fyrirhugað að beita áhættumildun vegna liðar 3.2? / *How will risk mitigation be applied, with reference to point 3.2?*
Áhættumildun samkvæmt þessum lið ættu að koma fram í áhættumati félagsins. Fullnægjandi svar væri að skila inn áhættumati í viðhengi. / *Risk mitigation according to this paragraph should be included in the undertakings risk assessment.*

4. Öryggi / *Security*

4.1. Uppfyllir lausnin ISO/IEC 27018/:2014 eða aðra sambærilega öryggisstaðla? / *Is the cloud solution ISO/IEC 27018/:2014 certified or holds other equivalent certifications?*
ISO/IEC 27018:2014 — Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors.

4.2 Er tryggt að gögnum sé endanlega eytt úr skýjalausninni þegar samningi um þjónustuna lýkur, þ.m.t. afrit?/ *Is it ensured that data is permanently deleted from the cloud solution when the service agreement ends, including backups?*
Skilmálar skýjaþjónustuaðila taka fram hvort að gögnum er eytt endanlega út, kjósi notandinn að hætta í þjónustu hjá hýsingaraðilanum eða hvort þau eru yfirskrifuð smám saman af næsta notanda. */ Terms of service should include a provision stating if the data put in the cloud solution is permanently deleted if the undertaking choses to discontinue the service or if the data is transcribed gradually by the next user.*

4.3 Eru gögn dulkóðuð áður en þau eru send og vistuð í skýjalausn? / *Is the data encrypted before it's sent or saved in the cloud solution?*

☐ Já ☐ Nei

4.3.1 Ef svar við 4.3 er já; hverjir hafa aðgang að dulkóðunarlyklinum? / *If the answer to 4.3 is yes; who has access to the encryption key?*

4.4. Hvernig er aðskilnaði gagna ótengdra aðila háttað í skýinu, bæði í hýsingu gagnanna og vinnslu þeirra? / *How is the separation of unrelated parties' data in the cloud solution ensured both regarding storage and processing of data?*

4.5. Hvar er landfræðileg staðsetning gagnanna og hvernig er hún staðfest? / *Where is the geographic location of the data and how is it verified?*

4.6. Undir hvaða lögsögu fellur samningur um skýjaþjónustu? / *Under which jurisdiction does the service agreement with the cloud solution provider fall?*

4.7. Er fyrirhugað að hýsa viðkvæmar persónuupplýsingar eða önnur viðkvæm gögn í skýjalausninni? / *Is the intention to put sensitive personal data in the cloud solution or other data that could be considered sensitive?*
Sbr. lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga. */ Cf. Act No. 90/2018 on privacy and personal data processing?*

4.7.1. Er fyrirhuguð hýsing í skýjalausn og meðhöndlun gagna í samræmi við kröfur persónuverndarlaga?/ *Is the intended use of data in the cloud solution in accordance with legal requirements regarding privacy and processing of personal data?*

4.7.2. Hvernig skilgreinir hinn eftirlitsskyldi aðili önnur viðkvæm gögn og hafa verið gerðar sérstakar ráðstafanir vegna hýsingar þeirra? / *How does the undertaking define „other sensitive data", and have there been made any special arrangements in that regard?*

4.8. Er kveðið á um í samningi um skýjalausn að frávik í rekstri hýsingaraðila skulu tilkynnt hinum eftirlitsskylda aðila? / *Does the service agreement with the cloud solution provider state that the undertaking s4.9.hall be notified of any deviations in the operations of the cloud solution?*
Hér er einnig átt við upplýsingaskyldu vegna innbrota eða annarra öryggisfrávika hjá hýsingaraðila. */ This also refers to notification requirements regarding on premise security issues encountered by the cloud solution provider.*

4.9. Hvernig hyggst félagið hafa eftirlit með fylgni hýsingaraðila við þau lög og reglur sem um hina útvistuðu starfsemi gilda? */ How does the undertaking intend to monitor the compliance of the could solution provider with the laws and regulations governing the outsourced activities?*

4.10. Hvernig verða gögn vernduð í samskiptum milli skýjalausnar og notanda? / *How will data be protected in transit between the cloud solution and the user?*

4.11. Er hýsingaraðili samningsbundinn til að tryggja öryggi þeirra gagna sem vistuð eru í skýjalausninni? / *Is the cloud solution provider contractually bound to ensure the security of the data stored in the cloud solution?*

5. Afritun */ Backups*

5.1 Hvernig er afritun á þeim gögnum sem hýst eru í skýjalausnum háttað*? / How is the backup process regarding the data in the cloud solution***?**
Fyrirkomulag og verklag afritunar þarf að mati Fjármálaeftirlitsins að vera með skipulögðum hætti og innihalda reglubundið eftirlit með því að afrit séu samkvæmt skjalfestu verklagi, nothæf og aðgengileg og innihaldi m.a. lýsingu á geymslutíma, staðsetningu afrita og búnaði nauðsynlegum til endurheimtu. / *The backup process needs to be organized and based on written procedures. Furthermore, it needs to be regularly monitored to ensure compliance, that backups are usable and accessible and retrievable.*

5.2 Eru afritin vistuð á öruggum stað í hæfilegri fjarlægð frá frumgögnum? / *Are the backups located in a safe place at a reasonable distance from the original data?*

5.3. Hvernig er aðgangsstýringu að afritum háttað, þ.e. hverjir hafa aðgang? / *How is access to backups controlled and who has access to them?*

5.4. Eru afritin ritvarin með þeim hætti að ekki sé hægt að breyta þeim eða eyða? / *Are the backups stored in manner that prevents editing and/or deleting?*

5.5. Er tryggt að afrit séu læsileg og aðgengileg til loka lögbundins varðveislutíma þar sem það á við? / *Is it ensured that backups are readable and accessible until the end of the statutory retention period?*
Kveðið er á um lögbundinn varðveislutíma viðskiptafyrirmæla í hinum ýmsu lögum er varða rekstur eftirlitsskyldra aðila:
Lög nr. 145/1994 um bókhald
Lög nr. 30/2004 um vátryggingasamninga
Lög nr. 108/2007 um verðbréfaviðskipti
Provisions regarding statutory retention period of data are stipulated in Act No. 145/1994 on Bookkeeping, Act No. 30/2004 on insurance contracts and Act. No. 108/2007 on Securities transactions.

5.6. Hvernig er aðgengi eftirlitsaðila að afritum tryggt? / *How is regulatory access to the data ensured?*

5.7. Hver er afhendingartími og afhendingastaður afritaða gagna? / *What is the delivery time and place of delivery of backups?*

5.8. Hvernig er endurheimting gagna frá afritum háttað? / *How is recovery of data form backups performed?*

6. Viðbúnaðarumgjörð / *Contingency plan*

6.1 Hefur viðbúnaðaráætlun fyrirtækisins verið uppfærð m.t.t. fyrirhugaðrar notkunar á skýjalausn? / *Has the undertaking's contingency plan been updated with respect to the intended usage of cloud solutions?*

6.2. Hefur viðbúnaðaráætluninni verið fylgt eftir með kennslu, æfingum og prófunum á varalausnum sem tryggja að þær virki eins og til er ætlast? / *Has the contingency plan been implemented with instructions, training and testing of backup solutions, to ensure they work as expected?*

6.2.1. Eru prófanir skv. lið 6.2 skjalfestar svo hægt sé að leggja fullnægjandi mat á framkvæmd og árangur?/ *Are the tests referred to in point 6.2 documented so that an adequate assessment of the process and performance can be made?*

6.3. Hefur fyrirtækið gert útgönguáætlun (e. exit strategy) vegna notkunar skýjalausnarinnar? / *Is there an exit strategy in place regarding the usage of cloud solutions?*
Mikilvægt er að eftirlitsskyldir aðilar meti hvaða áhrif þjónusturof hafi á starfsemi félagsins og hvernig þeir hyggist bregðast við. */ It is important that regulated entities assess the impact of a service rupture and plan for how to respond.*

7. Útvistun / *Outsourcing*

7.1 Samræmist útvistunin útvistunarstefnu félagsins og leiðbeinandi tilmælum nr. 6/2014 um útvistun? / *Is the outsourced cloud solution consistent with Guidelines No. 6/2014 on Outsourcing?*

7.2. Uppfyllir samningur við útvistunaraðila ákvæði liðar 26 í leiðbeinandi tilmælum nr. 1/2019 um upplýsingakerfi eftirlitsskyldra aðila um innihald slíkra samninga? / *Does the outsourcing contract meet the obligations stipulated in point 26 of the cited Guidelines on the contents of such contracts?*

7.3. Hefur Fjármálaeftirlitið verið upplýst um útvistunina og aðgengi stofnunarinnar að gögnunum tryggt? / *Has the regulator been informed of the outsourcing and have the access rights of the regulator been ensured?*

7.4. Er til staðar þjónustusamningur eða er aðeins um að ræða einhliða skilmála útvistunaraðilans? / *Is the outsourcing on the basis of a service agreement or on the basis of a standard unilateral terms of service?*

7.4.1. Ef skrifað er undir staðlaða skilmála útvistunaraðila, er tryggt að þeir séu óbreytanlegir á samningstíma? / *When accepting standard unilateral terms of service, are there any provisions ensuring they remain unchanged during contract period?*

7.5. Felur útvistunin í sér keðjuútvistun? / *Does the outsourcing involve chain outsourcing?*

7.6. Hvernig er þagnarskylda sem hvílir á eftirlitsskyldum aðilum tryggð hjá hýsingaraðila? / *How is it ensured that confidentiality requirements made to regulated entities are followed when outsourcing to a cloud solution provider?*

Skjal uppfært 19. ágúst 2019