Útvistunarstefna

NTÍ ber ábyrgð á að reksturinn uppfylli þær kröfur sem til hans eru gerðar, lögum samkvæmt eins og fram kemur í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun hjá eftirlitsskyldum aðilum[1]. Útvistun skal hagað þannig að hún samræmist þeim lögum, reglugerðum, reglum og öðrum viðmiðum sem um starfsemi viðkomandi eftirlitsskylds aðila gilda, þ. á m. ákvæðum um eðlilega og heilbrigða viðskiptahætti á viðkomandi markaði, með traust, trúverðugleika og öryggi að leiðarljósi[2]. Ekki er heimilt að útvista verkefnum sem lúta að grundvallar stjórnunarþáttum í rekstri NTÍ, s.s. mörkun áhættustefnu, áhættuvilja og áhættuþolmarka, stefnumörkun, reglusetningu m.t.t. áhættusniðs og áhættustýringar, eftirlitshlutverki stjórnar og endanlegri ábyrgð gagnvart viðskiptavinum og eftirlitsaðilum[3].

Útvistun þjónustuaðila til þriðja aðila skal ekki heimil nema með samþykki NTÍ. Þriðja aðila er aldrei heimilt að útvista hýsingu á gögnum NTÍ[4]. Um útvistun til erlendra aðila skal farið skv. kröfum í lið 11.3 í leiðbeinandi tilmælum FME nr. 2/2014 um upplýsingakerfi eftirlitsskyldra aðila.

1 Áhættumat

Áður en verkefni er útvistað skal NTÍ meta áhættu tengda útvistuninni[5]. Skoða skal sérstaklega eftirfarandi:

- Hvort og þá hvaða áhrif útvistunin hefur á starfsemi NTÍ, þ.m.t. áhrif á persónuvernd[6].
- Til hvaða aðgerða ætti að grípa ef óvissa skapast um starfsemi útvistunaraðila sem getur haft neikvæð áhrif á getu útvistunaraðila til að sinna hinu útvistaða verkefni[7].
- Tryggja að útvistunin komi ekki í veg fyrir góða stjórnarhætti NTÍ skv. leiðbeiningum og tilmælum um stjórnarhætti.[8]
- Að útvistunin skaði ekki orðspor NTÍ.[9]
- Að útvistunin feli ekki í sér óþarfa áhættu fyrir rekstur NTÍ.[10]
- Að möguleikar NTÍ til þess að fylgjast með og stýra útvistuðum verkefnum eða þjónustu séu hvorki skertir né torveldaðir.[11]
- Að möguleikar til innra eftirlits, þ. á m. með tilliti til hlutverks stjórnar og endurskoðunarnefndar, séu hvorki skertir né torveldaðir[12].
- Að möguleikar Fjármálaeftirlitsins til eftirlitsstarfa séu hvorki skertir né torveldaðir[13].

[1] Skv. grein 4.1 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[2] Skv. grein 3.1 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[3] Skv. greinum 5.1 - 5.3 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[4] Skv. grein 9.2 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[5] Skv. lið 1 í grein 8.3 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[6] Skv. 23. gr. laga nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga
[7] Skv. lið 3 í grein 8.3 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[8] Skv. lið 1 í grein 3.4 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[9] Skv. lið 2 í grein 3.4 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[10] Skv. lið 3 í grein 3.4 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[11] Skv. lið 4 í grein 3.4 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[12] Skv. lið 5 í grein 3.4 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[13] Skv. lið 6 í grein 3.4 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila

- Að útvistunin hafi ekki takmarkandi áhrif á samfellda og fullnægjandi þjónustu við viðskiptavini[14].
- Að útvistunin leiði ekki til þess að gæði verkefna eða þjónustu verði lakari en ef ekki hefði komið til útvistunar[15].
- Að ákvörðun um útvistun mikilvægra verkefna byggi á viðskiptalegum forsendum en ekki á hagsmunatengslum[16].

2 Samningar

Öryggi upplýsinga skal gætt í samningum við þriðja aðila, s.s. samstarfsaðila, birgja, þjónustuaðila og aðkeyptra sérfræðinga. Ákvæði skal vera í samningi um að öll viðskiptafyrirmæli skuli vera skrifleg og vistuð. Með viðskiptafyrirmælum er átt við samskipti sem fela í sér bindandi ákvarðanir milli aðila, s.s. fyrirmæli um framkvæmd ákveðinna viðskipta, staðfestingu á samningum o.s.frv[17].

Samningar þurfa að ná til eftirfarandi þátta að lágmarki[18]:

- Ítarleg lýsing á hinu útvistaða verkefni[19].
- Kröfur NTÍ sem gerðar eru til samningsaðila og undirverktaka. Gæta skal þess að setja kröfur fram með þeim hætti að unnt sé að hafa virkt eftirlit með hinu útvistaða verkefni[20].
- Reglur um aðgangsstýringar til að vernda gögn NTÍ[21].
- Kröfur NTÍ sem gerðar eru til verndar persónugreinanlegum upplýsingum[22].
- Vinnslusamningur ef útvistunin felur í sér vinnslu persónuupplýsinga[23].
- Réttur til að stunda eftirlit með þeirri starfsemi þjónustuaðilans sem samningurinn tekur til[24].
- Réttur eftirlitsaðila að gögnum á vinnustöð hýsingaraðila[25].
- Ákvæði um eignarhald þeirra gagna og afurða sem varða útvistunarsamninginn[26].
- Viðeigandi kafla upplýsingaöryggisstefnunnar, eða stefnan í heild ef útvistunin er tengd upplýsingatækni.

[14] Skv. lið 7 í grein 3.4 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[15] Skv. grein 5.4 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[16] Skv. grein 6.1 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila.
[17] Skv. leiðbeinandi tilmælum FME nr. 1/2019 vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila
[18] Skv. lið 1 í grein 8.4 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila.
[19] Skv. lið 1 í grein 9.1 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila og lið 26 í leiðbeinandi tilmælum FME nr. 1/2019 vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila.
[20] Skv. lið 2 í grein 9.1 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila.
[21] Skv. lið 33 í leiðbeinandi tilmælum FME nr. 1/2019 vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila
[22] Skv. lögum nr. 90/2018 um Persónuvernd og vinnslu persónuupplýsinga
[23] Skv. lögum nr. 90/2018 um Persónuvernd og vinnslu persónuupplýsinga
[24] Skv. lið 26 í leiðbeinandi tilmælum FME nr. 1/2019 vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila
[25] Skv. liðum 4 og 5 í grein 9.1 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila.
[26] Skv. lið 3 í grein 9.1 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila.

- Verkferli við samningslok[27].
- Hvernig upplýsingagjöf um útvistuð verkefni skuli komið á framfæri við NTÍ[28].
- Viðbrögð við vanefndum. Í hvaða tilfellum er heimilt að segja upp samningi og hvernig það skal gert[29].
- Ákvæði um heimilt og óheimilt framsal.
- Aðgerðir er varða umhverfisöryggi.
- Trúnaðarsamningur við þjónustuaðila þar sem við á[30].
- Ákvæði um að þjónustuaðila sé skylt að tilkynna NTÍ um allar verulegar breytingar í rekstri sínum, sem geta haft áhrif á getu hans til að sinna útvistaða verkefninu[31].
- Tilnefning ábyrgðaraðila hjá þjónustuaðila sem hefur næga þekkingu og reynslu til að sinna verkefninu[32].
- Tilnefna skal starfsheiti ábyrgðaraðila innan NTÍ, sem ber ábyrgð á kröfum sem gerðar eru til stofnunarinnar af hálfu FME og þjónustuaðila. Ábyrgðaraðilinn ber einnig ábyrgð á að fylgjast með breytingum á skipulagi og eignarhaldi útvistunaraðila, hafi það áhrif á getu útvistunaraðilans til að uppfylla efni samningsins[33].
- Ákvæði um úrlausn ágreinings milli samningsaðila[34].

Telji starfsmenn NTÍ sig ekki hafa nægilega þekkingu (tæknilega eða lagalega) til að gera samning um útvistun skal leita til utanaðkomandi ráðgjafa annars en samningsaðila[35].

3 Meðhöndlun atvika, frávika og öryggisbrota

Þjónustuaðili skal halda utan um atvik, frávik og öryggisbrot er snúa að samningsefni er uppgötvast af hálfu þjónustuaðila. Allar skráningar skulu fara fram í kerfum þjónustuaðila[36].

Frávik í upplýsingakerfum

Ef alvarlegt frávik felur í sér rof á varðveislu, leynd, réttleika og/eða tiltækileika upplýsingakerfa og gagna (t.d. innbrot í upplýsingakerfi, gagnaleki, gagnatap, óvænt rekstrarstöðvun upplýsingakerfa (í

[27] Skv. lið 26 í leiðbeinandi tilmælum FME nr. 1/2019 vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila
[28] Skv. lið 3 í grein 8.4 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila.
[29] Skv. lið 4 í grein 8.3, lið 5 í grein 8.4 og lið 7 í grein 9.1 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila.
[30] Skv. lið 9 í grein 9.1 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila.
[31] Skv. lið 6 í grein 9.1 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila.
[32] Skv. grein 6.3 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila.
[33] Skv. grein 6.3 og lið 4 í grein 8.4 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila.
[34] Skv. lið 8 í grein 9.1 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[35] Skv. grein 3.2 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[36] Skv. lið 26 í leiðbeinandi tilmælum FME nr. 1/2019 vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila

heild eða að hluta) sem hefur áhrif á starfsemina) skal þjónustuaðili tilkynna framkvæmdastjóra NTÍ sem fyrst, eða innan 12 klst.

Framkvæmdastjóri ber ábyrgð á því að tilkynningum sé komið áfram til FME innan 24 tíma eftir að frávik uppgötvast. Tilkynningin skal gerð á þar til gert eyðublað í skýrsluskilakerfi FME[37].

Öryggisbrot vegna persónuverndar

Ef öryggisbrestur á meðferð persónuupplýsinga (brestur á öryggi sem leiðir til óviljandi eða ólögmætrar eyðingar persónuupplýsinga, sem eru sendar, varðveittar eða unnar á annan hátt, eða að þær glatist, breytist, verði birtar eða aðgangur veittur að þeim í leyfisleysi,) uppgötvast skal þjónustuaðili tilkynna framkvæmdastjóra NTÍ það sem fyrst, eða innan 24 klst.

Framkvæmdastjóri ber ábyrgð á því að tilkynningum sé komið áfram til Persónuverndar innan 72 tíma eftir að öryggisbrestur uppgötvast. Um efni tilkynningar til Persónuverndar gilda fyrirmæli 33. gr. reglugerðar Evrópusambandsins um Persónuvernd og vinnslu persónuupplýsinga[38].

4 Eftirlit með útvistun

Áður en útvistunarsamningur er undirritaður skal ákveða hvernig eftirliti með útvistuðu verkefni skal háttað[39]. Skal slíkt eftirlit fært inn í úttektaráætlun.

Gæðafulltrúi NTÍ skal kalla eftir skýrslu um atvik, frávik og öryggisbrot hjá þjónustuaðilum sem vinna persónugreinanlegar upplýsingar fyrir NTÍ á sex mánaða fresti til staðfestingar á því að þau hafi verið tilkynnt um leið og þau eiga sér stað.

5 Útvistun mikilvægra verkefna

Tilkynna skal FME um útvistun mikilvægra verkefna auk breytinga sem verða á þeirri útvistun eins fljótt og kostur er[40]. Til mikilvægra verkefna teljast[41]:

- Lykilstarfsvið NTÍ, þ.e. framkvæmd áhættustýringar, innri endurskoðun, regluvarsla og starfsemi tryggingastærðfræðings.
- Önnur verkefni sem eru þess eðlis að veikleikar eða mistök við rækslu þeirra gætu haft alvarlegar afleiðingar fyrir möguleika NTÍ til þess að uppfylla skyldur sínar skv. lögum, reglugerðum eða öðru regluverki og/eða hafa áhrif á möguleika NTÍ til að halda áfram starfsemi.
- Verkefni sem hafa veruleg áhrif á virkni eða framkvæmd áhættustýringar NTÍ.

[37] Skv. liðum 46-49 í leiðbeinandi tilmælum FME nr. 1/2019 vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila
[38] Skv. 27. gr. laga nr. 90/2018 um Persónuvernd og vinnslu persónuupplýsinga
[39] Skv. lið 2 í grein 8.3 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[40] Skv. grein 6.2 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila
[41] Skv. grein 2.3 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila.

Gæta skal þess að útvistunaraðili sem tekur að sér mikilvæg verkefni og þeir starfsmenn útvistunaraðila sem verkefnum sinna, starfi af heilindum, hafi næga sérþekkingu, menntun og reynslu til þess að geta sinnt verkefnunum á fullnægjandi hátt[42].

[42] Skv. grein 7.1 í leiðbeinandi tilmælum FME nr. 6/2014 um útvistun eftirlitsskyldra aðila.