

Reglur Stefnis hf. um meðferð upplýsinga um viðskiptavini

1. Markmið

Traust og áreiðanleg meðferð upplýsinga er grundvallarregla í starfsemi Stefnis hf. (hér eftir „Stefnir“ eða „félagið“) og leggur Stefnir metnað sinn í að tryggja trúnað við viðskiptavinum sína og öryggi við meðferð persónuupplýsinga.

Reglur þessar gilda um meðferð Stefnis á upplýsingum um viðskiptavinum sína og viðskiptavinum Arion banka hf. (hér eftir „útvistunaraðila“) í tilviki útvistunar á eignarstýringu til félagsins (hér eftir sameiginlega „viðskiptavinir“). Meðferð upplýsinga um viðskiptavinum skal vera í samræmi við góða viðskiptahætti, grundvallarsjónarmið um persónuvernd og friðhelgi einkalífs og þagnarskyldu, sem koma fram m.a. í lögum nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga, lögum nr. 161/2002 um fjármálafyrirtæki, lögum nr. 45/2020 um rekstraraðila sérhæfðra sjóða og lögum nr. 116/2021 um verðbréfasjóði.

Nánar er fjallað um vinnslu félagsins á persónuupplýsingum viðskiptavina í persónuverndaryfirlýsingu félagsins.

2. Gildissvið

Reglurnar gilda fyrir allt starfsfólk, stjórnarmenn, endurskoðendur og hverja aðra sem taka að sér verk í þágu Stefnis (hér eftir sameiginlega nefndir „starfsmenn“). Reglurnar ná til allra upplýsinga í vörslu félagsins er varða viðskipta- eða einkamálefni viðskiptavina, á hvaða formi sem slíkar upplýsingar kunna að vera.

3. Vistun upplýsinga um viðskiptavinum

Stefnir vistar allar upplýsingar sem viðskiptavinir veita Stefni við upphaf viðskipta og á meðan á viðskiptasambandi stendur. Vistun gagna er gerð í samræmi við lög og reglur og er hún eftir atvikum á rafrænu formi eða pappírformi.

Upplýsingum um viðskiptamenn er eytt þegar ekki er lengur málefnaleg ástæða til að varðveita þær. Málefnaleg ástæða til varðveistu upplýsinga getur m.a. byggst á fyrirmælum í lögum eða að félagið vinni enn með upplýsingarnar í samræmi við upphaflegan tilgang með söfnun þeirra.

Auk þess hefur Stefnir sett sér reglur um varðveislutíma og eyðingu persónuupplýsinga - ábyrgð og hlutverk ábyrgðaraðila í vinnslu.

4. Þagnarskylda og miðlun upplýsinga

Starfsfólk er bundið þagnarskyldu um allt það sem þeir fá vitneskju um við framkvæmd starfa sinna og varðar viðskipta- eða einkamálefni viðskiptavina, nema skylt sé að veita upplýsingar lögum samkvæmt. Þagnarskylda helst þótt látið sé af starfi.

Einungis er heimilt að veita utanaðkomandi aðilum upplýsingar um viðskiptavinum ef fyrir liggur skýr lagaheimild eða með skriflegu samþykki viðkomandi viðskiptavinar. Í skriflegu samþykki viðskiptavinar skal koma fram til hvaða upplýsinga það tekur, til hvaða aðila er heimilt að miðla upplýsingunum á grundvelli þess og í hvaða tilgangi upplýsingunum er miðlað.

Ef upplýsingum er miðlað til þriðja aðila á grundvelli framangreindrar heimildar, skal sá sem veitir upplýsingarnar áminna viðtakanda um að hann sé bundinn þagnarskyldu með sama hætti og mælt er fyrir um í reglum þessum og lögum.

Opinberir eftirlitsaðilar, s.s. Fjármálaeftirlitið, Samkeppniseftirlitið, lögregla og skattayfirvöld hafa heimild að lögum til að óska eftir upplýsingum um viðskiptamenn og kann félaginu að vera skylt samkvæmt lögum að verða við slíkum beiðnum. Við miðlum upplýsinga til þriðja aðila skal starfsfólk fylgja innri verkferlum og reglum Stefnis eftir því sem við á.

Miðlun upplýsinga kann að stafa af frumkvæði Stefnis, m.a. þar sem Stefnir telst tilkynningarskyldur aðili skv. lögum nr. 140/2018 um aðgerðir gegn peningabætti og fjármögnun hryðjuverka. Í því felst að Stefni ber að tilkynna lögreglu ef grunur leikur á að viðskiptavinir noti þjónustu félagsins til peningabættis og/eða fjármögnunar hryðjuverka.

5. Öryggisráðstafanir

Stefnir ber ábyrgð á því að vinnsla persónuupplýsinga sé í samræmi við lög og reglur og gerir viðeigandi öryggisráðstafanir til að tryggja að svo sé.

Allar upplýsingar er verða viðskipta- og einkamálefni viðskiptavina skulu meðhöndlaðar af fyllstu varúð svo að tryggt sé að þær glatist ekki eða komist í hendur óviðkomandi aðila. Sérstök aðgæsla skal viðhöfð við varðveislu þeirra, ljósritun, sendingu, tölvuskráningu og eyðingu.

Rafræn vistun gagna skal vera á öruggum miðli þar sem öryggisráðstafanir eru í samræmi við kröfur hverju sinni. Við val öryggisráðstafana skal taka mið af áhættu af vinnslunni og eðli þeirra gagna sem á að verja.

6. Upplýsingaréttur viðskiptavina

Viðskiptavinir geta óskað eftir afriti af gögnum er verða viðskipti sín við útivistunaraðila eða Stefni.

Óski viðskiptavins eftir afritum af gögnum skal hann gera það með skriflegum hætti. Þrátt fyrir rétt viðskiptavina til að fá afrit af gögnum grein þessari mun Stefnir ekki afhenda upplýsingar um viðskiptamenn sem koma fram í vinnugögnum starfsmanna, s.s. tölvupóstum, minnisblöðum eða ónákvæmum gögnum. Við yfirferð á beiðnum um gögn leggur bankinn til grundvallar lög og reglur um persónuvernd og þagnarskyldu ásamt lögum um fjármálafyrirtæki.

7. Aðgengi starfsfólks að upplýsingum um viðskiptavini

Heimildir starfsfólks Stefnis til aðgangs og nýtingar upplýsinga um viðskiptavini ná eingöngu til þess sem nauðsynlegt er starfa þeirra vegna. Þannig er starfsfólki óheimilt að fletta upp upplýsingum um viðskiptavini úr kerfum útivistunaraðila nema það sé nauðsynlegt starfa þeirra vegna.

Markmiðum þessarar greinar er m.a. náð fram með því að:

- Aðgangi að upplýsingum og starfsstöðvum er stýrt, m.a. með úthlutun aðgangs- og lykilorða;
- Tryggja rekjanleika uppflettinga og vinnsluáðgerða; og
- Fræða starfsfólk um ábyrgð sína og skyldur við meðferð upplýsinga um viðskiptavini.

8. Eftirlit

Öryggisstjóri hefur eftirlit með að aðgangur starfsfólks að upplýsingum sé í samræmi við þau verkefni sem viðkomandi starfsmaður eða starfseining innan Stefnis er að sinna. Eftirlit þetta skal viðhaft með reglubundnum hætti. Tíðni eftirlitsins og umfang þess skal ákveðið með hliðsjón af þeirri áhættu sem er samfara vinnslunni, eðli þeirra ganga sem unnið er með, þeirri tækni sem notuð er til að tryggja öryggi upplýsinganna og kostnaði af eftirlitinu.

9. Viðurlög

Brot á reglum þessum geta varðað starfsfólk Stefnis viðurlögum, í formi áminningar eða brottreksturs eftir alvarleika brotsins. Þá geta brot varðar viðurlögum t.d. samkvæmt lögum nr. 161/2002 um fjármálafyrirtæki og lögum nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga.

10. Gildistaka og birting

Reglur þessar öðlast gildi að fenginni undirritun framkvæmdastjóra.

Reglur þessar skulu vera aðgengilegar viðskiptavinum og eru birtar á heimasíðu félagsins.

Samþykkt af framkvæmdastjóra Stefnis hf. þann 4. apríl 2025

Jón Finnbogason