



Reglur um meðferð upplýsinga um viðskiptavini

1. Markmið

Traust og áreiðanleg meðferð upplýsinga er grundvallarregla í starfsemi Arion banka og leggur bankinn metnað sinn í að tryggja trúnað við viðskiptavini sína og öryggi við meðferð persónuupplýsinga.

Reglur þessar gilda um meðferð Arion banka á upplýsingum um viðskiptavini sína og eru þær settar samkvæmt 19. gr. b. [laga nr. 161/2002 um fjármálafyrirtæki](#).

Markmið regnanna er að stuðla að öruggri og réttmætri meðferð upplýsinga um viðskiptavini, í samræmi við grundvallarsjónarmið um persónuvernd og friðhelgi einkalífs.

Reglur bankans taka mið af ákvæðum laga og reglna sem kunna að mæla fyrir um þagnarskyldu og meðferð og öryggi persónuupplýsinga. Um meðferð persónuupplýsinga gilda ákvæði [laga um persónuvernd og vinnslu persónuupplýsinga nr. 90/2018](#) og reglur byggðar á þeim.

2. Gildissvið

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

3. Vistun upplýsinga um viðskiptavini

Arion banki vistar allar upplýsingar sem viðskiptavinir veita bankanum við upphaf viðskipta og á meðan á viðskiptasambandi stendur. Upplýsingar sem bankinn kann að fá frá þriðja aðila, t.d. Þjóðskrá Íslands, Creditinfo eða Fasteignamati ríkisins, eru einnig vistaðar. Vistun gagnanna skal gerð í samræmi við skjalavistunaráætlun bankans og lög og reglur og er hún eftir atvikum á rafrænu formi eða pappírformi.

Bankinn eyðir upplýsingum um viðskiptamenn þegar ekki er lengur málefnaleg ástæða til að varðveita þær. Málefnaleg ástæða til varðveislu upplýsinga getur m.a. byggst á fyrirmælum í lögum eða að bankinn vinni enn með upplýsingarnar í samræmi við upphaflegan tilgang með söfnun þeirra.

Auk öryggisreglna bankans, þar sem fjallað er ítarlega um upplýsingaöryggi og meðferð upplýsinga, hefur bankinn sett sér verklagsreglur fyrir skjalastjórn og varðveislu og eyðingu gagna.



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 bankans, nema skylt sé að veita upplýsingar lögum samkvæmt. Þagnarskylda helst þótt látið sé af starfi.

Einungis er heimilt að veita utanaðkomandi aðilum upplýsingar um viðskiptavini bankans 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 upplýsingum á grundvelli þess og í hvaða tilgangi upplýsingum 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 1. mgr. 4. gr. reglna þessara, sbr. og 58. gr. [laga nr. 161/2002 um fjármálafyrirtæki](#).

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

Miðlun upplýsinga kann að stafa af frumkvæði Arion banka, m.a. þar sem bankinn telst tilkynningaskyldur aðili samkvæmt [lögum nr. 140/2018 um aðgerðir gegn peningabætti og fjármögnun hryðjuverka](#). Í því felst að Arion banka ber að tilkynna lögreglu ef grunur leikur á að viðskiptavinir noti þjónustu bankans til peningabættis og/eða fjármögnunar hryðjuverka. Jafnframt ber Arion banka samkvæmt [lögum um ábyrgðarmenn nr. 32/2009](#) að tilkynna ábyrgðarmönnum lána um stöðu þeirra, vanefndir eða aðrar breytingar er varða ábyrgðina.

5. Öryggisráðstafanir

Arion banki 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 varða viðskipta- eða 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 varða viðskipti sín við bankann.



Óski viðskiptavinur eftir afritum af gögnum skal hann gera það með skriflegum hætti. Viðskiptavinir eiga ekki rétt á aðgengi persónuupplýsingum starfamanna bankans. Við yfirferð á beiðnum um gögn leggur bankinn til grundvallar lög og reglur um persónuvernd og þagnarskyldu ásamt lögum um fjármálafyrirtæki.

7. Aðgangur starfsfólks að upplýsingum um viðskiptavini

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

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

1. aðgangi að upplýsingum og starfsstöðvum er stýrt, m.a. með úthlutun aðgangs- og lykilorða;
2. tryggja rekjanleika uppflettinga og vinnsluáðgerða; og
3. fræða starfsfólk um ábyrgð sína og skyldur við meðferð upplýsinga um viðskiptavini.

8. Eftirlit

Öryggisstjóri bankans hefur eftirlit með að aðgangur starfsfólks að upplýsingum sé í samræmi við þau verkefni sem viðkomandi starfsmaður eða starfseining innan bankans 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 gagna 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 bankans viðurlögum, í formi áminningar eða brottresturs eftir alvarleika brotsins. Þá geta brot varðað 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 taka gildi við samþykkt þeirra.

Reglur þessar skulu vera aðgengilegar viðskiptavinum og eru birtar á heimasíðu bankans (www.arionbanki.is).

Samþykkt 27. mars 2023