APP ARION BANKA

PERSÓNUVERNDARSTEFNA

ÚTG. 1.0, 11. JÚNÍ 2017

UM PERSÓNUVERNDARSTEFNUNA

Hér er fjallað um þá vinnslu persónuupplýsinga sem notkun á símaforriti Arion banka, Netbanka Appinu, hefur í för með sér. Nánar tiltekið er fjallað um:

- hver beri ábyrgð á vinnslunni og í hvaða tilgangi hún fari fram,
- hvers konar persónuupplýsingar sé unnið með,
- hve lengi megi ætla að upplýsingarnar verði geymdar,
- hvert upplýsingunum kunni að verða miðlað og
- með hvaða hætti sé gætt að öryggi þeirra.

Þá er að lokum fjallað um þær kröfur sem stefnu þessari er ætlað að uppfylla.

Notanda er ávallt valfrjálst að veita persónuupplýsingar í Appinu. Kjósi notandi að veita ekki umbeðnar upplýsingar hefur það jafnan þær afleiðingar að ekki er hægt að veita honum þá þjónustu sem viðkomandi virkni í Appinu lýtur að.

ÁBYRGÐARAÐILI, TILGANGUR OG HEIMILD FYRIR VINNSLU PERSÓNUUPPLÝSINGA

Ábyrgðaraðili vinnslunnar er Arion banki hf., Borgartúni 19, 105 Reykjavík. Innan bankans er það upplýsingatæknisvið sem ber ábyrgð á Appinu og þeirri vinnslu persónuupplýsinga sem tengist því.

Til þess að hægt sé að veita notendum þá þjónustu sem talin er upp í lýsingu á Appinu er nauðsynlegt að vinna með ýmiss konar persónuupplýsingar, einkum um notendurna sjálfa. Megintilgangur vinnslunnar er því að gefa notendum kost á þeirri þjónustu sem Appinu er ætlað að veita. Annar tilgangur með vinnslunni er að tryggja öryggi fjármuna og persónuupplýsinga þeirra sem nota Appið. Loks er þeirri vinnslu persónuupplýsinga sem fram fer í tengslum við Appið ætlað að uppfylla þær kröfur sem gerðar eru til bankans á hverjum tíma, einkum í lögum og af þeim sem hafa eftirlit með starfsemi bankans, einkum Fjármálaeftirlitið en einnig til dæmis Persónuvernd.

Um notkun Appsins gilda samningsskilmálar um App Arion banka eins og þeir eru á hverjum tíma, en þá má nálgast á vefsíðunni https://www.arionbanki.is/einstaklingar/rafraen-vidskipti/appid/skilmalar . Heimild til vinnslu persónuupplýsinga í tengslum við Appið er þríþætt. Nánar tiltekið er vinnslan nauðsynleg vegna

- framkvæmdar samnings notanda og bankans um notkun Appsins,
- þeirra lagaskyldna sem hvíla á bankanum, einkum samkvæmt lögum um fjármálafyrirtæki og lögum um opinbert eftirlit með fjármálastarfsemi og
- vegna lögmætra hagsmuna bankans, einkum við að gæta öryggis upplýsingakerfa sinna og þeirra gagna sem þar er unnið með.

ÞÆR TEGUNDIR PERSÓNUUPPLÝSINGA SEM UNNIÐ ER MEÐ

Almennar lýðupplýsingar

Til þess að auðkenna notendur í Appinu, millifæra fé til annarra notenda og nota margar af öðrum aðgerðum forritsins er nauðsynlegt að vinna með upplýsingar um nöfn, kennitölur, heimilisföng, netföng og vistföng (IP-tölur) notenda og þeirra sem þeir eiga í samskiptum við. Þær eru einkum slegnar inn af notanda sjálfum eða kallaðar fram á ný eftir að hann hefur vistað þær en einnig er þeim í sumum tilvikum flett upp í þjóðskrá, í þeim tilgangi að tryggja örugga persónugreiningu. Þá er einnig unnið með upplýsingar með því að fletta upp í símaskrá notanda, hafi hann sérstaklega heimilað fyrirfram slíkar uppflettingar, í þeim tilvikum sem notandi hefur stillt Appið þannig að um leið og hann byrjar að slá inn nafn viðtakanda tilkynningar um greiðslu þá geri Appið tillögu að því hver viðtakandinn sé. Slíkar símaskráruppýsingar eru hins vegar ekki unnar frekar í Appinu og hvorki vistaðar í því né sendar út fyrir símann.

Fjármálaupplýsingar

Margar af þeim aðgerðum sem hægt er að framkvæma í Appinu snúa að bankaupplýsingum um notandann og þá sem hann hefur samskipti við, einkum um banka- og greiðslukortareikninga hans, stöðu á þeim og færslur, þar á meðal um fjárhæðir og tímasetningar aðgerða. Þær upplýsingar eru fengnar úr skrám bankans sjálfs og úr skrám sam haldnar eru sameiginlega um reikninga hjá fjármálafyrirtækjum, t.d. í kerfum Reiknistofu bankanna hf., auk upplýsinga sem notandinn slær inn í Appið.

Öryggisupplýsingar

Í tengslum við Appið er unnið með ýmiss konar persónuupplýsingar beinlínis til að tryggja örugga auðkenningu notenda og til að takmarka óheimilan aðgang. Einkum eru það uppýsingar um notendanafn, leyniorð og merki reiknings, upplýsingar um þann síma sem Appið er sett upp á, stýrikerfi hans og tengingar símans við Arion banka, auk upplýsinga um það sem notandi hefur framkvæmt í Appinu með aðstoð rafrænna skilríkja sinna. Þá er í sama tilgangi unnið með upplýsingar um hvenær og hve lengi Appið er notað til að tengjast Arion banka og hvers konar aðgerðir eru framkvæmdar þar.

GEYMSLUTÍMI PERSÓNUUPPLÝSINGA

Einungis er unnið með persónuupplýsingar í tengslum við Appið að því marki sem það er nauðsynlegt miðað við framangreindan tilgang með vinnslunni. Því eru upplýsingar um tengingar notenda við Arion banka með Appinu og þær aðgerðir sem þeir framkvæma þar að jafnaði einungis vistaðar um nokkurra mánaða skeið. Hins vegar eru upplýsingar um fjárhagslegar aðgerðir, svo sem millifærslur, geymdar lengur eða að jafnaði þann tíma sem notandi er í viðskiptum um viðkomandi þjónustu. Frá því er hins vegar vikið þegar ákvæði laga og reglna kveða á um lengri geymslutíma. Þannig mæla til dæmis bókhaldslög fyrir um að bókhaldsgögn skuli varðveitt í sjö ár.

HVERT PERSÓNUUPPLÝSINGUM ER MIÐLAÐ

Þeim persónuupplýsingum sem vinnslan tekur til er miðlað til þeirra sem þurfa á þeim að halda til að hægt sé að veita þá þjónustu sem notandinn óskar eftir. Þannig er upplýsingum um millifærslur, þar á meðal upplýsingar um fjárhæð og sendanda, miðlað til viðskiptabanka móttakanda og upplýsingar um innborganir á GSM frelsi er miðlað til fjarskiptafyrirtækis notanda. Þá er upplýsingum um aðgerðir notanda, til dæmis hreyfingar á bankareikningum, miðlað til þeirra sem úrskurðir dómstóla eða ákvæði réttarreglna bjóða bankanum að miðla þeim til, einkum til eftirlitsstofnana og löggæsluyfirvalda.

UM ÖRYGGI VINNSLUNNAR

Á Arion banka hvílir rík skylda til að gæta að öryggi þeirra persónuupplýsinga sem bankinn vinnur með. Þeirri skyldu gegnir bankinn með því:

- að setja sér öryggisstefnu,
- að meta þá hættu sem steðjar að viðkomandi vinnslu, til dæmis hættu á að óviðkomandi fái aðgang að upplýsingunum eða þær skemmist eða verði eytt að ósekju og
- að beita öryggisráðstöfunum til að stemma stigu við þá hættu. Þær öryggisráðstafanir eru margs konar og lúta einkum að aðgangsstýringu, raunlægu öryggi, mannauðsöryggi, rekstraröryggi og samskiptaöryggi.

Þá viðhefur bankinn innra eftirlit með ofangreindu og endurskoðar áhættumat sitt og viðbrögð reglulega.

KRÖFUR SEM STEFNUNNI ER ÆTLAÐ AÐ UPPFYLLA

Þessari persónuverndarstefnu er annars vegar ætlað að uppfylla þær kröfur sem gerðar eru að íslenskum lögum til vinnslu persónuupplýsinga og hins vegar þær kröfur sem gerðar eru í skilmálum fyrir dreifingu símaforrita í hugbúnaðardreifingarþjónustum.

Helstu réttarreglur sem stefnunni er ætlað að uppfylla eru ákvæði í lögum um persónuvernd og meðferð persónuupplýsinga, sem nú eru nr. 77/2000, um:

- að vinnsla skuli fara fram í yfirlýstum, skýrum og málefnalegum tilgangi (7. gr.),
- að veita vitneskju um þá vinnslu persónuupplýsinga sem fram fer á hans vegum (16. og 18. gr.) og
- að upplýsa hinn skráða um nánar tiltekin atriði varðandi vinnsluna (20. og 21. gr.).

Þá er stefnunni ætlað að uppfylla ákvæði reglugerðar ESB nr. 2016/679 (almennu persónuverndarreglugerðarinnar), sem fyrirhugað er að taki gildi hér á landi í maí 2018, sbr. einkum ákvæði hennar um:

- gegnsæi upplýsinga og tilkynninga (12. gr.),
- upplýsingar og aðgang að persónuupplýsingum (13.-15. gr.),

Loks skal áréttað að samkvæmt II. kafla reglugerðarinnar er notanda heimilt að óska eftir aðgangi að persónuupplýsingum sínum, láta leiðrétta þær, eyða þeim eða takmarka vinnslu þeirra, auk þess að hafa rétt til að andmæla vinnslu, kvarta yfir henni til Persónuverndar og til að flytja eigin gögn.