Gefið út af stjórn Íslandsbanka

Stefna um persónu-vernd og vinnslu persónuupplýsinga

Október 2020

Útgáfa	Breytingar	Breytt af	Dags.	Staðfest af	Dags.

Efnisyfirlit

Stefna um persónuvernd og vinnslu persónuupplýsinga

Kópavogur, 28. október 2020

Stjórn Íslandsbanka

Hallgrímur Snorrason
Stjórnarformaður

Anna Þórðardóttir

Árni Stefánsson

Flóki Halldórsson

Frosti Ólafsson

Guðrún Þorgeirsdóttir

Heiðrún Jónsdóttir

1. Inngangur

Íslandsbanki hf. (hér eftir bankinn eða ábyrgðaraðili) leggur ríka áherslu á gæta persónuverndar í starfsemi sinni og ber ábyrgð á að vinnsla persónuupplýsinga sé í samræmi við grundvallarsjónarmið og reglur um persónuvernd og friðhelgi einkalífs og lög um persónuvernd og vinnslu persónuupplýsinga.

1.1. Lagarammi

Stefna þessi er sett með vísan til meginreglunnar um ábyrgðarskyldu og 1. og 2. mgr. 24. gr. almennu persónuverndarreglugerðar Evrópuþingsins og ráðsins nr. 2016/679 sem lögfest var með lögum nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga (hér eftir persónuverndarlög). Þar kemur fram að með hliðsjón af eðli, umfangi, samhengi og tilgangi vinnslunnar og áhættu, mislíklegri og misalvarlegri, fyrir réttindi og frelsi einstaklinga skal ábyrgðaraðili gera viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja og sýna fram á að vinnslan fari fram í samræmi við lögin. Þar sem það samrýmist meðalhófi í tengslum við vinnslustarfsemina skulu ráðstafanir þessar *m.a.* fela í sér að ábyrgðaraðili innleiði viðeigandi persónuverndarstefnur.

1.2. Skilgreiningar

Eftirfarandi skilgreiningar eru úr persónuverndarlögum:

Ábyrgðaraðili: einstaklingur eða lögaðili, opinbert yfirvald, sérstofnun eða annar aðili sem ákvarðar, einn eða í samvinnu við aðra, tilgang og aðferðir við vinnslu persónuupplýsinga. Í stefnu þessari: Íslandsbanki hf.

Persónuupplýsingar: hvers kyns upplýsingar um persónugreindan eða persónugreinanlegan einstakling **(skráðan einstakling/hinn skráði)**; einstaklingur telst persónugreinanlegur ef unnt er að persónugreina hann, beint eða óbeint, svo sem með tilvísun í auðkenni eins og nafn, kennitölu, staðsetningargögn, netauðkenni eða einn eða fleiri þætti sem einkenna hann í líkamlegu, lífeðlisfræðilegu, erfðafræðilegu, andlegu, efnalegu, menningarlegu eða félagslegu tilliti.

Vinnsla: aðgerð eða röð aðgerða þar sem persónuupplýsingar eru unnar, hvort sem vinnslan er sjálfvirk eða ekki, s.s. söfnun, skráning, flokkun, kerfisbinding, varðveisla, aðlögun eða breyting, heimt, skoðun, notkun, miðlun með framsendingu, dreifing eða aðrar aðferðir til að gera upplýsingarnar tiltækar, samtenging eða samkeyrsla, aðgangstakmörkun, eyðing eða eyðilegging.

Vinnsluaðili: einstaklingur eða lögaðili, opinbert yfirvald, sérstofnun eða annar aðili sem vinnur persónuupplýsingar á vegum ábyrgðaraðila.

Öryggisbrestur við vinnslu 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.

1.3. Markmið og gildissvið

Markmið stefnu þessarar er að tryggja að bankinn, stjórn hans og starfsmenn fari að viðeigandi lögum, reglum og innri reglum bankans sem gilda um vinnslu persónuupplýsinga. Stefnunni er ætlað að tilgreina helstu skyldur bankans þegar kemur að vernd og vinnslu persónuupplýsinga og skilgreina ábyrgð og verkaskiptingu innan bankans í því skyni. Stefnunni er jafnframt ætlað að tryggja að umgjörð um persónuvernd sé í samræmi við viðeigandi lög, reglur, tilmæli og leiðbeiningar sem gilda um persónuvernd á hverjum tíma. Stefnunni er jafnframt ætla að tryggja að

ábyrgð og verkaskipting innan bankans í tengslum við málaflokkinn sé skýr og fullnægjandi eftirlit með honum sé viðhaft.

Stefna þessi skal gilda um alla vinnslu persónuupplýsinga skráðra einstaklinga hjá bankanum óháð landfræðilegri staðsetningu slíkra upplýsinga. Stefnan gildir um starfsmenn, stjórn, verktaka og alla þá sem koma að vinnslu persónuupplýsinga fyrir hönd bankans sem ábyrgðaraðila.

1.4. Eignarhald og endurskoðun stefnu

Stefna þessi er samþykkt af stjórn Íslandsbanka. Stefnan skal yfirfarin eigi sjaldnar en á tveggja ára fresti og uppfærð þegar þurfa þykir. Persónuverndarfulltrúi ber ábyrgð á að tryggja að endurskoðun eigi sér stað og að hafa umsjón með innleiðingu hennar innan bankans.

2. Hlutverk og ábyrgð

2.1. Stjórn bankans

Stjórn samþykkir stefnu þessa og ber að tryggja að viðeigandi og fullnægjandi innri reglur, ferlar, kerfi og verklag séu til staðar.

2.2. Áhættustefnunefnd

Áhættustefnunefnd rýnir og staðfestir stefnuskjöl um áhættustýringu, þ. á m. stefnu þessa, hvort sem um er að ræða reglubundna endurskoðun eða tilfallandi breytingar, áður en þær eru lagðar fyrir stjórn til samþykktar.

2.3. Framkvæmdastjórn

Framkvæmdastjórar bera ábyrgð á innleiðingu stefnu þessarar. Í því felst m.a. að tryggja að starfsmenn þeirra þekki stefnu þessa og skyldur sínar samkvæmt henni og starfi í samræmi við hana. Framkvæmdastjórar bera ábyrgð á að starfsmenn þeirra starfi í samræmi við persónuverndarlög sem og viðeigandi ytri og innri reglur, ferla, kerfi og verklag sem bankinn hefur sett sér. Framkvæmdastjórar bera einnig ábyrgð á því að starfsfólk þeirra sæki fræðslu um persónuvernd og öryggisbresti við vinnslu persónuupplýsinga.

2.4. Persónuverndarfulltrúi

Persónuverndarfulltrúi bankans veitir ráðgjöf á sviði persónuverndar og hefur eftirlit með framkvæmd og innleiðingu stefnu þessarar. Tryggt skal að persónuverndarfulltrúi komi tímanlega að öllum málum sem tengjast vernd persónuupplýsinga og að hann hafi nauðsynleg úrræði til að inna af hendi störf sín. Jafnframt skal tryggt að hann fái engin fyrirmæli varðandi framkvæmd verkefna sinna og honum verði hvorki vikið úr starfi né refsað fyrir framkvæmd þeirra.

Persónuverndarfulltrúi skal upplýsa ábyrgðaraðila og starfsmenn um skyldur sínar samkvæmt persónuverndarlögum og veita þeim ráðgjöf þar að lútandi. Hann skal fylgjast með því að farið sé að ákvæðum laganna varðandi vernd persónuupplýsinga, þ.m.t. úthlutun ábyrgðar, vitundarvakning og þjálfun starfsfólks og tilheyrandi úttektir. Hann skal einnig veita ráðgjöf varðandi mat á áhrifum á persónuvernd og fylgjast með framkvæmd þess og vera tengiliður fyrir Persónuvernd varðandi mál sem tengjast vinnslu persónuupplýsinga.

Nánar er kveðið er á um stöðu og hlutverk persónuverndarfulltrúa í 35. gr. persónuverndarlaga, sbr. 37. – 39. gr. almennu persónuverndarreglugerðarinnar og í erindisbréfi sem bankastjóri setur.

2.5. Áhættustýring

Áhættustýring bankans hefur eftirlit með innleiðingu og sinnir eftirliti í samræmi við umgjörð bankans um áhættustýringu og innra eftirlit. Áhættustýring skal koma að mati á áhættu vegna

rekstraráhættuatvika sem teljast öryggisbrestir við vinnslu persónuupplýsinga. Áhættustýring stýrir, vaktar og metur hlítingaráhættu bankans í tengslum við persónuvernd í samstarfi við persónuverndarfulltrúa sbr. stefnu bankans um hlítingaráhættu.

2.6. Innri endurskoðun

Innri endurskoðun metur hvort stefnur, umgjörð og verklag séu með fullnægjandi hætti m.t.t. krafna laga og ytri reglna um persónuvernd og hefur eftirlit með störfum persónuverndarfulltrúa.

2.7. Allir starfsmenn

Allir starfsmenn skulu þekkja og starfa í samræmi við stefnu þessa.

Starfsmenn skulu ávallt:

- gæta trúnaðar við vinnslu persónuupplýsinga og meðhöndla þær á lögmætan og sanngjarnan hátt,
- fylgja því verklagi sem innleitt hefur verið um persónuvernd þ.m.t. að tilkynna án tafar um öryggisbresti sem kunna að verða við vinnslu persónuupplýsinga samkvæmt verklagi þar um,
- vera meðvitaðir um réttindi hinna skráðu,
- leitast við að takmarka það tjón sem bankinn getur orðið fyrir verði brot á lögum og reglum um persónuvernd.

Starfsmenn geta leitað til persónuverndarfulltrúa séu þeir í vafa um hvernig meðferð persónuupplýsinga skal vera háttað. Þeir skulu jafnframt senda persónuverndarfulltrúa ábendingar telji þeir meðferð persónuupplýsinga ekki í samræmi við lög, reglur eða verklag. Þá geta starfsmenn einnig sent inn nafnlausar ábendingar sem tilkynningar um misferli á innri síðu bankans.

3. Umgjörð persónuverndar

3.1. Ábyrgðarskylda

Til að vernda réttindi og frelsi einstaklinga við vinnslu persónuupplýsinga skal tryggt að gerðar verði viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja og sýna fram á að meginreglum og kröfum persónuverndarlaga sé fullnægt („ábyrgðarskylda“). Með viðeigandi tæknilegum og skipulagslegum ráðstöfunum er *m.a.* átt við að gerðar skulu ráðstafanir í kerfum sem geyma persónuupplýsingar og settar skulu innri stefnur og verklag sem stuðla að og tryggja hlítni við persónuverndarlög.

3.2. Meginreglur um vinnslu persónuupplýsinga

Vinnsla persónuupplýsingar skal vera í samræmi við meginreglur persónuverndarlaga sbr. 1. mgr. 5. gr. með þeim undantekningum sem við eiga og að verklag endurspegli þær. Þannig skulu persónuupplýsingar:

- unnar með lögmætum, sanngjörnum og gagnsæjum hætti gagnvart skráðum einstaklingi („lögmæti, sanngirni og gagnsæi“),
- fengnar í tilgreindum, skýrum og lögmætum tilgangi og ekki unnar frekar á þann hátt að ósamrýmanlegt sé þeim tilgangi („takmörkun vegna tilgangs“),
- nægilegar, viðeigandi og takmarkast við það sem nauðsynlegt er miðað við tilganginn með vinnslunni („lágmörkun gagna“),
- áreiðanlegar og, ef nauðsyn krefur, uppfærðar; gera skal allar eðlilegar ráðstafanir til að tryggja að persónuupplýsingum, sem eru óáreiðanlegar, með hliðsjón af tilganginum með vinnslu þeirra, verði eytt eða þær leiðréttar án tafar („áreiðanleiki“),
- varðveittar á því formi að ekki sé unnt að persónugreina skráða einstaklinga lengur en þörf er á miðað við tilganginn með vinnslu upplýsinganna („geymslutakmörkun“),

- unnar með þeim hætti að viðeigandi öryggi persónuupplýsinganna sé tryggt, þ.m.t. vernd gegn óleyfilegri eða ólögmætri vinnslu og gegn glötun, eyðileggingu eða tjóni fyrir slysni, með viðeigandi tæknilegum og skipulagslegum ráðstöfunum („heilleiki og trúnaður“).

3.3. Réttindi hinna skráðu

Leitast skal við að tryggja hinum skráðu eftirfarandi réttindi með þeim takmörkunum sem við geta átt:

- Rétt til upplýsinga um vinnslu, varðveislu og meðferð persónuupplýsinga hjá bankanum.
- Rétt til aðgangs að persónuupplýsingum.
- Rétt til leiðréttingar óáreiðanlegra persónuupplýsinga
- Rétt til eyðingar („rétt til að gleymast“)
- Rétt til takmörkunar á vinnslu
- Rétt til að flytja eigin gögn
- Rétt til að andmæla vinnslu persónuupplýsinga

3.4. Innbyggð og sjálfgefin persónuvernd

Þegar ákveðnar eru aðferðir við vinnslu persónuupplýsinga og þegar vinnslan fer sjálf fram skulu gerðar viðeigandi tæknilegar og skipulagslegar ráðstafanir, sem hannaðar eru til að framfylgja meginreglum um persónuvernd, og fella nauðsynlegar verndarráðstafanir inn í vinnsluna til að uppfylla kröfur persónuverndarlaga og vernda réttindi hinna skráðu samkvæmt þeim. Í þessu felst m.a. að bankinn skal setja sér reglur sem kveða á um ráðstafanir sem stuðla að innbyggðri og sjálfgefinni persónuvernd.

3.5. Skrá um vinnslustarfsemi

Halda skal skrá um vinnslustarfsemi og skal skráin gerð aðgengileg Persónuvernd að beiðni hennar. Skráin skal haldin í sérstöku kerfi sem persónuverndarfulltrúi hefur aðgang að.

3.6. Vinnsluaðilar

Þegar öðrum er falin vinnsla persónuupplýsinga fyrir hönd bankans skal einungis leita til vinnsluaðila sem veita nægilegar tryggingar fyrir því að þeir geri viðeigandi tæknilegar og skipulagslegar ráðstafanir til að vinnslan uppfylli kröfur persónaverndarlaga. Í þessum tilvikum skal ávallt gera skriflegan samning sem skuldbindur vinnsluaðila gagnvart bankanum. Útvistun skal vera í samræmi við útvistunarstefnu bankans.

Í þeim tilvikum þar sem bankinn telst vinnsluaðili þriðja aðila skal einnig gera skriflegan vinnslusamning.

3.7. Mat á áhrifum á persónuvernd

Þegar líklegt er að tiltekin tegund vinnslu geti haft í för með sér mikla áhættu fyrir réttindi og frelsi einstaklinga, einkum þar sem beitt er nýrri tækni og með hliðsjón af eðli, umfangi, samhengi og tilgangi vinnslunnar, skal ábyrgðaraðili láta fara fram mat á áhrifum fyrirhugaðra vinnsluaðgerða á vernd persónuupplýsinga áður en vinnslan hefst. Leita skal ráðgjafar persónuverndarfulltrúa við þetta mat.

3.8. Öryggi

Gerðar skulu viðeigandi tæknilegar og skipulagslegar ráðstafanir til að viðunandi öryggi persónuupplýsinga og að meðferð persónuupplýsinga sé í samræmi við öryggisstefnu bankans. Verði öryggisbrestur við vinnslu persónuupplýsinga hjá bankanum skal fara með slíka bresti í samræmi við persónuverndarlög og verklag bankans þar um.