Data Protection Notice

1. About the Data Protection Notice

Arion Bank hf. (hereafter "**Arion**" or "**the Bank**") cares about data protection. The protection of personal data is important to the Bank and there is a special emphasis on ensuring that personal data is processed legally, fairly and transparently.

The Data Protection Notice contains explanations of which personal data the Bank collects on *customers,* when and why, on what grounds and how long this data is expected to be kept, where the data might be shared and how the security of the data is safeguarded. The same applies to the processing by the Bank of personal data on *contacts of customers who are legal entities, job applicants* and *other persons* who may visit or contact the Bank for other purposes. The Data Protection Notice also contains information on the rights of persons with respect to the processing of data by the Bank.

This Data Protection Notice applies to all processing undertaken by Arion Bank as a controller as defined by the Data Protection and Processing of Personal Data Act No. 90/2018 ("**Data Protection Act**"). The Bank may also act as a processor, or as a joint controller with other controllers. The Bank works closely with its subsidiaries and partner companies and the role of the Bank may vary depending on the services it provides to these subsidiaries and partner companies, i.e. Vörður, Stefnir and Frjálsi Pension Fund. For information on the processing of personal data by these companies please refer to the data protection notices of Vörður, Stefnir, Frjálsi and other administered pension funds.

Any queries concerning the Bank's processing of personal data or this Data Protection Notice can be sent to personuvernd@arionbanki.is.

2. Personal data processed by the Bank

2.1 Personal data on customers

The table below gives an overview of the personal data which the Bank processes on customers, for what purpose it is being processed and on the basis of which authority. If other data than that specified in the table is being processed, or for another purpose, the Bank will seek to inform the customer of this.

Processing connected to products and services	
How does the Bank process personal data and for what purpose?	The Bank processes personal data when the customer commences a business relationship with the Bank. The Bank does this in order to provide the customer with the services they have requested. The Bank receives this data directly from the customer, from the Bank's systems, from third parties, as applicable, or from public data.
What is the legal basis for processing data?	The processing of personal data is necessary for the Bank to be able to provide the services requested by the customer and it is therefore necessary in order to fulfil agreements with the customer. The Bank is also obliged by law to process certain personal data concerning the customer, e.g. in compliance with the Anti-Money Laundering and Terrorist Financing Act and the Securities Transactions Act.
What personal data does the Bank process?	The Bank processes different types of personal data depending on the type of products and services. The personal data processed can be categorized as follows: • Identification information, i.e. name, ID number, customer number, electronic ID and copy of personal identification documents • Contact information, i.e. address, phone number and e-mail address • Information on family status, i.e. co-habitation, marital status and information spouse and children • Financial information concerning the product or service requested by the customer or which the customer ha from the Bank, e.g. information on business history, solvency, turnover, account balance etc. • Information on assets, e.g. real estate and vehicles • Information concerning insurance. In connection with the sale and servicing of insurance, the Bank processes insurance data, including real estate registration number, car registration number, claims history, information on beneficiaries and the insured etc.
Automated decisions	In certain circumstances the Bank relies on automated decisions in connection with the Bank's products and services. Automated decisions are when a decision is taken on an application and/or a customer's rights, i.e. a decision is taken on a credit appraisal or a loan, without a person being involved. Automated decisions use personal data which is based on a profile created when data is processed automatically to assess a person's circumstances. Automated decisions can only be made with the customer's consent or when such decisions are considered necessary in order to enter into or fulfil an agreement with the customer. Customers are always entitled to human involvement if automated decisions are used in processing.

Who is responsible for processing?	Arion Bank is the controller of personal data on the customer by the Bank in connection with the Bank's products and services. In cases concerning products and/or services of subsidiaries and partner companies which the Bank services, the Bank is a joint controller with the relevant subsidiary and/or partner company. With respect to service and sales of insurance, the Bank acts as joint controller with Vörður.

Communications	
How does the Bank process personal data and for what purpose?	The Bank services its customers through different channels; digitally via the Arion app, online banking Arion chatbots, at branches and the Bank's call centre. The Bank processes personal data in order to be able to provide the services requested by customers, answer queries and to provide appropriate advice. In order to improve its services the Bank might ask customers to participate in service and communications surveys.
What is the legal basis for processing data?	The Bank processes personal data in order to be able to provide the services requested by customers, answer queries and to provide appropriate advice. Processing data is necessary to fulfil agreements. Processing linked to the Bank's service and communications surveys is made on the basis of the Bank's legitimate interests and the same applies to processing data relating to the use of the Bank's digital media.
What personal data does the Bank process?	The Bank processes identification and communications data on the customer, the contents of messages the customer sends to the Bank and in some circumstances financial data in connection with the advice requested by the customer at any given time. In connection with the use of the Arion app, online banking and Arion chatbot, the Bank also processes the customer's IP numbers, action logs, log in routes, type of browser, type and operating system of device used by the customer. Such processing is carried out for the purpose of following up on advice and recommendations. In connection with service and communications surveys the Bank also processes communications data on the customer and the results of the surveys.
Who is responsible for processing?	The Bank is the controller of personal data on the customer. In cases where the Bank is communicating with the customer in connection with products and/or services of subsidiaries or partner companies, the Bank acts as a joint controller with the relevant subsidiary and/or partner company.

Marketing of products and services	
How does the Bank process personal data and for what purpose?	The Bank reserves the right to send the customer marketing material in order to introduce to the customer products and services of Bank and subsidiaries and partner companies of the Bank. Such marketing material can be sent by e-mail, via the Arion app or online banking.

What is the legal basis for processing data?	The Bank has legitimate interests in processing personal data for the purpose of marketing products and services. The customer has the right to object to the Bank's processing of their personal data which is carried out on the grounds of legitimate interests, see Section 7.3 of this Notice. In cases where the Bank wishes to use the customer's personal data and perform a more in-depth analysis of the customer's personal data for the purpose of marketing products and service, the Bank may ask for special consent for this processing. If the customer gives the Bank consent to process personal data for marketing purposes, the customer is always entitled to withdraw this consent, see section 7.5 of this Notice.
What personal data does the Bank process?	The Bank uses the customer's contact details to send them marketing material. In connection with the general marketing of products and services, the Bank process identification information on the customer, e.g. age and/or information on family circumstances. In order to be able to send the customer personalized marketing material, the Bank might also process personal data based on the customer's business history, product use and their dealings with the Bank. The Bank might also process data on the customer's interests in order to invite them to events which the customer might be interested in and/or to offer them personalized services.
Who is responsible for processing?	The Bank is the controller of personal data on the customer in connection with the marketing of its products and services. In cases where the Bank is communicating with the customer in connection with products and/or services of subsidiaries or partner companies, the Bank acts as a joint controller with the relevant subsidiary and/or partner company.

Product development and managing IT systems	
How does the Bank process personal data and for what purpose?	In order to develop and improve products and services and analyze the need for new products and services, the Bank uses customers' personal data. The Bank also processes personal data in certain instances when testing and developing the Bank's systems. Development and testing is essential in order to safeguard the quality and security of the Bank's systems. The Bank tries to make customers' personal data unidentifiable and processes it for the aforementioned purposes.
What is the legal basis for processing data?	Processing is carried out on the grounds of the Bank's legitimate interests.
What personal data does the Bank process?	The personal data the Bank processes in connection with product development and managing IT systems might encompass all the data the Bank processes on the customer in connection with providing products and services and the customer's dealings with the Bank.
Who is responsible for processing?	The Bank is responsible for processing personal data on the customer in connection with product development and managing IT systems. In cases where the Bank processes data connected to products and services of subsidiaries and partner companies, the Bank acts as

	a joint controller, or in some circumstances as processor, on behalf of the relevant subsidiary or partner company.

Internal controls and risk management	
How does the Bank process personal data and for what purpose?	The Bank processes personal data when assessing risk, whether this concerns the Bank's internal operations or business decisions concerning the business relationship with the customer. Data is processed when a business relationship commences and for its duration.
What is the legal basis for processing data?	The Bank has a legal obligation to process data in accordance with the Financial Undertakings Act. Processing related to the Bank's internal controls is carried out on the grounds of legitimate interests.
What personal data does the Bank process?	The personal data the Bank processes in connection with internal controls and risk management might encompass all the data the Bank processes on the customer in connection with providing products and services, the customer's dealings with the Bank and processing connected to anti-money laundering and terrorist financing measures.
Who is responsible for processing?	Arion Bank is the controller of personal data linked to internal controls and risk management.

Anti-money laundering measures and terrorist financing	
How does the Bank process personal data and for what purpose?	The Bank is obliged to know their customers and to perform a risk assessment. When commencing a business relationship all customers have to undergo due diligence. In some cases customers have to undergo enhanced due diligence. The Bank is obliged to monitor business relationships. For more information on the Bank's efforts to prevent money laundering and terrorist financing see **here**.
What is the legal basis for processing data?	The Bank is obliged under the Anti-Money Laundering and Terrorist Financing Act to process data in order to prevent money laundering and terrorist financing. Processing is therefore carried out on the basis of legal obligations.
What personal data does the Bank process?	The personal data processed by the Bank in connection with anti-money laundering and terrorist financing measures can be categorized as follows: • Identification information • Contact information • Information on family status • Financial information • Information about political connections
Who is responsible for processing?	The Bank is the controller of personal data connected to anti-money laundering and terrorist financing measures.

2.2. Personal data of contacts and representatives

In cases where the Bank's customers are legal entities, the Bank processes the contact information of the representatives of the legal entities, e.g. the signature authorities and position of the person in question. One of the reasons for doing this is to be in contact with the customer and to ensure that the person in question is authorized to bind the legal entity. The Bank also processes data on the owners of the relevant legal entity, board of directors, executive committee, authorized signatories, controllers and, as relevant, other contacts. Furthermore, the Bank may process data on the interests of the customers' contacts for marketing purposes, e.g. in connection with invitations to events.

This processing is based on the legitimate interests of the Bank and in some circumstances legal obligations.

In order to be able to communicate with suppliers of partner companies and regulators, the Bank also processes contact information of contacts and their representatives.

2.3 Personal data of job applicants

The Bank processes copies of job applications and the data contained therein, such as name, ID number, address, phone number, e-mail address, education, qualifications and work experience. The Bank might also process data on job references and information which is in the public domain, e.g. on social media.

If the Bank offers an applicant a job, it usually asks for proof of a clean criminal record and information on the applicant's financial status in addition to other information, e.g. which confirm the applicant's education and experience.

Job applications are kept for six months.

Personal data on applicants is processed by the Bank on the basis that the person in question has asked to enter into an agreement with the Bank, and in some circumstances, on the grounds of the Bank's legitimate interests.

2.4 Processing of personal data of minors

The Bank processes personal data on children when this is necessary in order to perform a requested transaction or service, e.g. to open a bank account, issue a debit card, provide access to online banking or the Arion app. The Bank then enters into a special agreement or obtains the consent of the parent/guardian to the processing before a child under 13 is offered the service.

The Bank must send any marketing material concerning products and services intended for children to their parents/guardians. Parents/guardians can decline marketing material, cf. Section 7.3 of this Notice.

2.5 Electronic surveillance

The Bank carries out electronic surveillance by recording telephone calls and using CCTV cameras. CCTV surveillance is carried out at the Bank's branches and near ATMs. Surveillance is carried out to ensure security and to minimize the risk of fraud. The data created by electronic surveillance is kept in accordance with the current laws and regulations.

Processing connected to electronic surveillance is based on the Bank's legitimate interests and, in some circumstances, on legal obligations under the Securities Transactions Act.

2.6 Other processing

In cases where other people than customers, or contacts and representatives of customers and other partners and regulators, contact the Bank, it may be necessary for the Bank to process the personal data of the person in question. This applies for example if the Bank receives a sponsorship request from a customer and/or any kind of feedback concerning the Bank or its subsidiaries.

3. Where does the Bank get personal data from?

In most cases the Bank gets the personal data it processes from the persons themselves. The Bank also receives personal data from third parties in certain circumstances. For example, the Bank gets data from Creditinfo, Registers Iceland, the Directorate of Inland Revenue, the Director of Customs, the Icelandic Property Registry, the Icelandic Vehicle Registry, the Register of Limited Companies and other official registries and the Legal Gazette.

In cases where the Bank provides services to subsidiaries and partner companies, the Bank gets personal data on their customers in order to be able to service these customers and data is processed on the basis of an agreement. In these cases the Bank acts as joint controller and in exceptional cases as a processor.

4. Where is personal data shared?

The Bank may be required to share data on persons it works with to third parties in the circumstances listed below.

4.1 Third parties

Third party refers to independent legal entities, other than the Bank, or persons who are not employees of the Bank.

The sharing of personal data on persons with third parties is done for different reasons and can be categorized according to the basis on which the data is shared:

- On the basis of an agreement

The Bank may be required to share personal data of a customer to a third party in order to meet certain obligations pursuant to an agreement. An example of this is sharing data with the Icelandic Banks' Data Centre and card companies with respect to the execution of transactions and the custodians of financial instruments with respect to investment services.

- Because of a legal obligation

On the basis of legislation, regulations and court and government rulings and government orders, the Bank may be obliged to share information, particularly on customers, with third parties or competent authorities. On the basis of clear legal authority, authorities such as the Financial Supervisory Authority, the Central Bank of Iceland, the District Prosecutor, the Directorate of Inland Revenue and the Customs Authority can request information from the Bank on customers

and others. The Bank is obliged to agree to such requests and, in some circumstances, provide the authorities with access to the Bank's places of work and IT networks for this purpose. For example, the Bank may be obliged to share information on income, debts, information on customers to the Directorate of Internal Revenue with respect to tax returns and withholding tax and information to the inspector of taxes and the district prosecutor with respect to the investigation of individual cases.

- On the grounds of legitimate interests

Some of the Bank's service providers act as independent controllers, e.g. lawyers and accountants. In cases where it is necessary to share a person's personal data with such parties in connection with a provided service, including in connection with protecting interests and pursuing court cases, this represents the sharing of personal data with a third party.

With respect to data which has been collected through electronic surveillance, the Bank may be permitted to share such data with the police or an insurance company, e.g. in the case of a damage to property where the Bank has to make a claim.

In connection with potential mergers and/or acquisitions and sales, the Bank can also share limited data on the customer to potential investors and consultants, e.g. for the purpose of conducting due diligence.

4.2 Processors

The Bank uses third parties in connection with various services to the Bank, e.g. information technology. In connection with these services the Bank may be required to share or provide service providers with access to the personal data processed by the Bank and in such cases the service providers act as processors. In such cases the Bank ensures that the organizations in question have taken adequate security measures to protect personal data and the Bank makes the appropriate processing agreements with them. Processors only process personal data for this purpose and to the extent decided by the Bank.

4.3 Subsidiaries and partner companies

The Bank may share personal data with subsidiaries and partner companies in order to execute an agreement with customers, to fulfil legal requirements, e.g. requirements stipulated by anti-money laundering legislation, or on the grounds of legitimate interests. Data may be shared between the Bank and subsidiaries and/or partner companies for marketing purposes, either by consent or on the grounds of legitimate interests. The role of the Bank depends on the type of processing in each case, e.g. whether it acts as a controller, joint controller or processor.

The Bank is bound by an obligation of confidentiality to its customers under the Financial Undertakings Act and the Bank will always abide by these obligations when sharing data within the Group.

4.4 Sharing personal data outside the EEA

In certain circumstances personal data may be shared abroad and outside the European Economic Area (**EEA**), for example in fulfilment of contractual obligations to a customer or to meet certain legal requirements made of the Bank. However, the Bank does not share information outside the

EEA unless this is done on the basis of the appropriate authority in the Data Protection Act and provided that appropriate measures have been taken.

5. Security of personal data processed by the Bank

The Bank is obliged to safeguard the security of the personal data which it processes and the Bank has a certified information security management system in accordance with ÍST ISO/IEC27001. The security measures taken by the Bank are organizational and technical and primarily involve access management, physical security, personnel security, operating security and communications security. The Bank has internal controls to monitor the above and reviews its risk assessment and responses on a regular basis.

6. Storage time of personal data

Personal data is stored for the duration of the business relationship between the customer and the Bank or as long as is necessary with respect to the purpose of processing, terms of agreements, the Bank's rules and provided there are legitimate reasons to store it. The Bank may be required to store data for legal reasons. Accordingly, accounting data is stored for seven years, data concerning money laundering and due diligence is stored for five years after an individual transaction or after the business relationship ends and copies of trade orders are stored for five years.

Data collected through electronic surveillance is generally kept for 30 days and data on job applicants is kept for six months.

7. Rights of persons under the Data Protection Act

The Data Protection Act ensures various rights for the persons the Bank is processing personal data on. However, these rights are not absolute, and legal obligations or the higher-ranking interests of the Bank or third parties may prevent the Bank from being able to comply with a person's request to exercise these rights on the basis of the Data Protection Act. The Bank seeks to respond to all requests from persons to exercise their rights under the Data Protection Act within 30 days and if the Bank cannot for any reason comply with such request, either partially or fully, the Bank will seek to explain its decision.

7.1 Access to own personal data – personal data reports

Persons are entitled to know whether the Bank is processing personal data about them and to receive information on processing, e.g. purpose, where data is being shared, origin, whether automated decisions are being made and information on their rights. Persons are also entitled to obtain a copy of the personal data the Bank is processing on the person in question.

A *personal data report* can be obtained in Arion online banking, where the customer can request a copy of the personal data on them being processed by the Bank. The personal data report aims to provide the customer with an overview of the personal data which the Bank is processing. However, it cannot be excluded that the Bank is processing more extensive personal data on the customer than that contained in the report. Customers can always request further information on the processing of personal data on them by the Bank in accordance with the right to access and copies of data.

7.2 Correcting and destroying personal data

If a person believes that the personal data being processed by the Bank is inaccurate or incorrect, that person is entitled to have it corrected.

In certain cases a person is entitled to demand that the Bank destroy personal data on them if they believe the data is no longer necessary for the purpose for which it was collected. The same applies if the person withdraws their consent for the processing of personal data and if there is no other legal basis for the processing or if the processing of the data is illegal.

7.3 Right to object and restrictions on processing

A person is entitled to object to the processing of personal data on the grounds of legitimate interests, e.g. processing of personal data for use in direct marketing.

A person is entitled to ask the Bank to restrict the processing of personal data about them, if they believe the data is incorrect, if the processing of the data is illegal or the Bank no longer needs the data but the person needs the data to establish, maintain or protect legal claims.

7.4 Right to data portability

In specific cases where processing is done on the basis of an agreement or consent, a person who has provided the Bank with personal data on themselves electronically may be entitled to get a copy of such data in an organized, standardized and computerized format. A person can also request that the Bank send data about them directly to a third party.

7.5 Withdrawing consent

In cases where processing is based on consent, a person who gave the Bank their consent can withdraw it at any time. Withdrawing consent has no impact on the legitimacy of processing carried out on the basis of consent up until the time that consent is withdrawn.

7.6 Complaints to the Data Protection Authority

The Data Protection Authority monitors the implementation of the Data Protection Act and the processing of personal data and makes rulings on disputes concerning data protection. Further information on the Data Protection Authority can be found on its website, personuvernd.is. If a person is not satisfied with the processing of their personal data by the Bank they can make a complaint to the Data Protection Authority at Rauðarárstígur 10, 105 Reykjavík, e-mail postur@personuvernd.is.

8. Contact details of the Bank and Data Protection Officer

If a data subject wishes to exercise their rights on the basis of the Data Protection Act, cf. section 7 of this Data Protection Notice, or if the person has questions on the Bank's processing of personal data, they are encouraged to contact the Bank. The Bank can be contacted by e-mail at arionbanki@arionbanki.is or by calling 444 7000.

The Bank has also appointed a special Data Protection Officer in accordance with the Data Protection Act. The role of this person includes monitoring compliance with the Data Protection Act, acting as the Bank's contact with the Data Protection Agency and answering queries from people

the Bank is processing data on. The Data Protection Officer can be contacted by e-mail at personuvernd@arionbanki.is.

The Bank has its headquarters at Borgartún 19, 105 Reykjavík and its ID number is 581008-0150.

9. How does the Bank update or change the Data Protection Notice?

The Bank reserves the right to change this Data Protection Notice and add to it at any time in order to best reflect the processing undertaken at the Bank at any given time. Such changes come into effect without prior notice when published on the Bank's website, unless otherwise specified.