Data Protection Statement of Arion Bank

1. About the Data Protection Notice

One of the Bank's cornerstones is that we say what we mean. The protection of our customers' data is important to the Bank and there is a special emphasis on ensuring that personal data is processed in a legal, fair and transparent way.

The Data Protection Notice contains descriptions of which personal data the Bank collects and why the Bank does so, how long this data is expected to be kept, where the data might be shared and how the security of the data is safeguarded. It also contains information on the rights of customers in respect of the personal data processed by the Bank.

Arion Bank handles and processes personal data on customers in accordance with the Data Protection Act No. 90/2018. The Data Protection Notice is written in concise, clear and simple language.

2. Information on the data controller

The data controller is Arion Bank hf., Borgartún 19, 105 Reykjavík, ID-No. 581008-0150. Arion Bank is a universal bank which provides a comprehensive range of financial services, including savings, loans, asset management, corporate finance and capital markets. Arion Bank operates branches, service points and ATMs throughout Iceland. Arion Bank has an operating licence as a retail bank under the Financial Undertakings Act No. 161/2002 and is supervised by the Financial Supervisory Authority (FME) in accordance with the Official Supervision of Financial Operations Act No. 87/1998 (see website of the Financial Supervisory Authority, www.fme.is). Arion Bank is listed in the Register of Companies, the Register of Limited Companies, the Icelandic Business Information Centre and the FME's register of financial institutions. More information on the activities of Arion Bank can be found on the Bank's website: www.arionbanki.is.

3. Personal data about the customer collected by the Bank

The Bank collects personal data from the customer in order to be able to offer them products and services. Generally this refers to general personal data such as name, ID number, address, phone number, IP number, residence and information on products and services which the customer has already acquired from the Bank or previously used. In some cases the Bank collects sensitive personal data about a customer, such as information on ethnicity or health. The Bank also collects personal data on the customer when the customer contacts the Bank to obtain services, such as by calling the Call Centre, sending an e-mail, webchat, visiting a branch, the Bank's website, using Arion Online Banking or the Arion App. The Bank is also provided with personal data from third parties when necessary and a third party is authorized to provide data to the Bank, e.g. Registers Iceland or Creditinfo. The collection of personal data on a customer is discussed in more detail in section 4.

3.1. Categories of personal data

The Bank places personal data in different categories in order to gain an overview of the different types of data processed by the Bank. Below is a description of the main categories of personal data:

Identification information: Any kind of identification document which identifies the customer, e.g. copy of a passport, driving licence or electronic ID.

Basic information: Name, ID number, address, telephone number, e-mail address and other basic information, e.g. information on legal guardian in case of an individual, information on related legal entities and role of individual at legal entity, e.g. power of attorney or trustee.

Family status: Marital status, spouse, children and related persons.

Financial information: Business history, turnover, transactions and balance on accounts, account numbers, payment card details, interest rates, self-service limits, income, financial obligations, defaults, credit ratings, credit assessments etc.

Information on agreements: Information on agreements which the customer has entered into with the Bank and information on products and services provided to the customer so that the agreements can be executed. This refers to information on loan repayments, use of ATMs, applications for products and services, interest rates, service fees, investment objectives, which is information obtained, for example, in connection with private banking, instructions on securities transactions, signed documents etc.

Information on the origin of assets and capital: This refers to information on business partners, business activities and how funds have been raised.

Information on due diligence: Information which enables the Bank to perform due diligence on the basis of the Act on Measures against Money Laundering and Terrorist Financing No. 140/2018 and to ensure compliance with international sanctions, which includes ascertaining whether the purpose and nature of a business relationship are in compliance with the law and whether the customer is a politically exposed person.

Information created when responding to statutory queries from the authorities: This refers to information sent to the Directorate of Internal Revenue concerning tax returns or withholding tax and information sent to the Director of Tax Investigations or the District Prosecutor concerning the investigation of cases. This may include information on income, debt, receivables etc.

Information on communication between parties: Information which the Bank receives from customers, e.g. by letter or e-mail, from conversations with customers, either at branches, via the Call Centre, on social media or webchat.

Technical information: Information on the devices used by the customer to connect to the Bank via Online Banking or the Arion App. Data derived from this includes IP number, version of operating system and performed actions.

Information on behaviour and use: Information on how the customer uses products and services from the Bank, how often they use them, types of service, the customer's settings, results of surveys and the customer's interests and tastes. This enables the Bank to improve its services and to monitory security.
Public information: Information from Registers Iceland, Icelandic Property Registry, Icelandic Vehicle Registry, Register of Limited Companies and other official registries. It also includes information which can be accessed through a financial information agency such as Creditinfo, and publicly available information online.
Video recordings and audio recordings of phone calls: CCTV footage of places of work and ATMs. Audio recordings of phone calls.
Sensitive personal information: Information on ethnic background, political views, membership of trade unions, health information, fingerprints and distinguishing facial features.
Consent: Consent to things such as cookie policy.
Information concerning insurance: Information on family size, legal guardian, beneficiary, insured party, heirs, claim history, car registration number, property registration number etc. Arion Bank sells insurance policies from Vörður and acquires this information for this purpose.
Applicant information: Name, ID number, address, phone number, e-mail address, education and qualifications, experience, ethnicity, disability.

3.2 Personal data provided to the Bank by an individual

At the beginning of the business relationship the Bank collects basic information, identification information and information on due diligence. Next the individual provides financial information and other information required so that the requested product or service can be provided, e.g. information on payments, i.e. amount, type and recipient. An individual applying for a loan from the Bank must also provide the Bank with the required financial information so that it can assess the customer's creditworthiness and ability to repay the loan, e.g. statement of earnings, assets and debts. The Bank collects information on an individual's behaviour and use of services and information provided by an individual when they participate in market research and/or surveys.

The Bank records and keeps all communications between an individual and the Bank in accordance with the law, this policy and the Bank's rules. When an individual exercises their right to move their personal data from another data controller to the Bank, e.g. Meniga which sends personal data to the Bank, that individual is providing the Bank with personal data about themselves.

If an individual does not wish to provide the Bank with personal data which the Bank has to obtain or if an individual objects to the processing of such data, it may have an impact on whether or how the Bank provides the service in question.

3.3. Personal data created at the Bank

Personal data on a customer is created at the Bank when the Bank provides contractual services or performs its statutory monitoring duties. This refers to information such as what product or services the customer has acquired from the Bank, which branch and ATM the customer uses, when they logged into Online Banking and the Arion App, when they visited the Bank's website, the IP number and identification information, how the customer has contacted the Bank, what advice they have received, payment history, transactions on their accounts, information on employers and salaries, information on buying and selling securities, what services the customer has been offered, requests from the customer and information which provides any indication of fraud or abnormal transactions.

3.4. Audio recording and electronic surveillance

The Bank keeps audio recordings of phone calls in accordance with the Bank's internal rules on electronic surveillance. Phone calls form part of the Bank's security system and have a legal basis in data protection legislation. The Bank's internal rules specify which landline phones and mobile phones are recorded and how long the recordings should be kept for. Recordings are kept for five years in the case of instructions on securities transactions, otherwise it is 90 days. At the end of this period, the recording of the phone call is automatically destroyed. Electronic surveillance is conducted using CCTV cameras at places of work and in the vicinity of the Bank's ATMs. The purpose of processing this information is to guarantee security and minimize the risk of fraud.

3.5. Personal data provided to the Bank by a third party

The Bank receives personal data from third parties. The Bank obtains information from authorized persons nominated by the customer. In order to counter fraud, eradicate money laundering and terrorist financing, data is obtained from known and authorized data providers which are engaged to carry out due diligence reviews. Third parties which provide the Bank with information about people include Registers Iceland, Icelandic Property Registry, Register of Limited Companies, Creditinfo, the Directorate of Inland Revenue and the Director of Customs. Third parties provide the Bank with the information it needs and which they are authorized to provide. It varies whether the parties are authorized independently or whether the customer has given their consent. The Bank then collects information on behalf of the customer, such as tax returns when processing loan applications. The Bank gets information on the customer in order to ensure that the information about the customer is reliable and accurately reflects the customer's financial position. The Bank also acquires personal data which has been published, provided that it is generally authorized to process this information, e.g. information from the Legal Gazette [Lögbirtingablaðið].

4. Why is the personal data being processed and on what basis?

The Bank always requires authorization to process personal data in its possession about the customer. This section discusses the objective of processing data and the authorization to do so.

4.1. In order to execute an agreement

The Bank may be required to process personal data on a customer in order to provide services based on an agreement between the customer and the Bank. The authorization for such processing is, for example, contained in the terms of agreements such as loan terms, payment card terms and general terms of business. The Bank therefore processes personal data on the customer after a business relationship has been established in order to fulfil the agreement. If the customer requires further services, the Bank needs to process personal data on the customer again.

Below are examples of processing carried out on this basis:

- Applications for debit or credit cards
- Setting up access to Online Banking
- Performing a credit assessment or credit rating
- Opening deposit account

4.2 To meet legal obligations

The Bank is obliged to collect, keep and share personal data on the basis of legislation, regulations, court orders, administrative rulings, guidelines on the financial market and other government instructions. Authorities such as the Financial Supervisory Authority, Central Bank of Iceland, District Prosecutor or Directorate of Internal Revenue and customs authorities can request information on the customer from the Bank if there is clear legal authority to do so. 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. Below are examples of processing carried out on this basis:

- Performing credit ratings and credit assessments, assessing the Bank's capital ratio and assessing insurance risk
- Due diligence reviews of individuals on the basis of the Act on Measures against Money Laundering and Terrorist Financing
- Analysis and investigation of cases concerning money laundering, terrorist financing, fraud and other illegal activities
- Mandatory internal controls
- Storage of specific personal data on the basis of the Annual Accounts Act, the Accounting Act and the Securities Transactions Act

The Bank is also legally obliged to store specific personally identifiable data, i.e. in compliance with the provisions of the Act on Measures against Money Laundering and Terrorist Financing, the Accounting Act and due to disclosure to the regulators and other public authorities.

4.3. In respect of legitimate interests

It is in the legitimate interests of the Bank to process personal data on a customer in order to develop the Bank's products and services so it can best meet the needs and expectations of customers and be competitive. This kind of processing does not take place if a person's basic rights and freedom with respect to data protection are considered more important than the interests related to processing the data. The Bank processes various types of personal data and analyzes customers based on factors including business history and use of products. It is in the Bank's legitimate interests to categorize customers (loyalty categorization) in order to be able to offer them various personalized services and to price products and services as precisely as possible. It is also in the Bank's legitimate interests to process personal data for the purposes of direct marketing so that personalized products and services can be introduced to them. The Bank uses various methods to introduce these products and services, e.g. via messages in Online Banking, the Arion App, social media and the Bank's website and also by e-mail to the address provided by the customer. Customers can choose not to receive such messages by changing the settings in their Online Banking account, contacting the Bank by e-mail at arionbanki@arionbanki.is or by calling the Call Centre on 444 7000.

Below are examples of processing carried out on this basis:

- Improving the range of products and services. Personal data is placed into categories, e.g. credit rating, savings and deposits, in order to identify opportunities to improve the Bank's products and services and to offer existing customers personalized products and services. When a customer uses the service Fjármál heimilanna (Household Finances) the Bank analyzes how the customer uses the Bank's products and services and those of other financial institutions from the information provided by the customer. This allows the Bank to further improve the available range of products and service.
- Sending customers messages on various benefits, products and services which may appeal to them.
- Providing customers with personalized financial and insurance advice.
- Analyzing and investigating cases involving online and information security to prevent fraud.
- Processing information on legal entities, owners, the boards of the directors of legal entities, executive management, authorized representatives and their contact persons so that the Bank can make informed decisions on loans, collateral and guarantees.

4.4 Processing based on consent

The Bank processes personal data on customers in certain circumstances on the basis of the customer's consent, e.g. with cookies on the Bank's websites, as described in more detail in the rules and terms on cookies. The Bank also acquires the consent of the customer, if the personal data is expected to be used for another purpose than originally intended. For example, this may refer to offering the customer the services of another company, e.g. an insurance company. In such cases the Bank provides the customer with further information on the processing of personal data to which the consent applies. The customer can withdraw their consent at any time by notifying the Bank. This can be done by changing the settings in Online Banking, contacting the Bank by e-mail at arionbanki@arionbanki.is or by calling the Call Centre on 444 7000. Processing personal data will only cease once the notification of withdrawal of consent has been received by the Bank.

4.5. Processing of personal data on minors

The Bank processes personal data on a child 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. Under the Data Protection Act the Bank must get the consent of the parent or guardian for the processing of personal data on a child under 13 years of age, before the child is offered digital services.

The Bank must send any marketing material concerning products and services intended for children to their parents or guardians. Parents or guardians can decline marketing material by contacting the Bank at arionbanki@arionbanki.is or by calling 444 7000.

5. Automated decision-making and profiling

In certain cases the Bank makes automated decisions on providing services on the basis of a person's profile created from the information the Bank has on that customer. Automated decisions are made using software which automatically processes personal data on a customer and creates a profile. An automated decision is then taken without any involvement from employees. This type of decision is used for Consumer Loans in the Arion App. Profiles are based on information including a person's credit rating and information from the tax register. An algorithm is then used to calculate and decide whether a Consumer Loan can be granted. Automated decisions are only made with a person's consent, if an automated decision is necessary to make or execute an agreement between a person and the Bank or if permitted by law. Other automated decisions which have no direct impact on individuals, e.g. marketing by the Bank based on legitimate interests, may be made without consent. The customer may at any time make objections to an automated decision if it affects the person's interests and ask the Bank to examine and reassess the conclusion reached by sending an e-mail to arionbanki@arionbanki.is or calling 444 7000.

The list below gives some examples of automated decisions:

- Examples of profiling are the calculation of a credit assessment, a credit rating for a customer and loyalty categorization.
- Examples of automated decision-making are granting an overdraft based on the customer's credit assessment.

6. Where is personal data shared?

6.1. General information on sharing personal data

Arion Bank does not share personal data on a customer unless required to do so by law or to fulfil contractual obligations. The customer can, however, authorize the Bank to share personal data with the third party with the customer's consent. Examples of parties which may be authorized by law to request that personal data be shared are regulatory authorities, such as the Financial Supervisory Authority, Central Bank of Iceland, the District Prosecutor, the Director of Internal Revenue, the customs authorities and the law enforcement authorities. The Bank is also obliged to share personal data if a court rules that it must do so.

Personal data is in some cases sent to parties fulfilling statutory tasks or to processors which process personal data on behalf of Arion Bank pursuant to an agreement. These parties include financial information agencies such as Creditinfo, IT companies, such as the Icelandic Banks' Data Centre, debt collection agencies, card companies and custodians of financial instruments as described in the terms of investment services.
Examples of sharing information:

- When there is an obligation to help recover funds which have been transferred into the account of a customer by mistake.
- When it is necessary to trace the origins of funds due to the suspicion of fraud or financial crimes.
- When acquiring services from a third party which provides the Bank with services, e.g. hosting networks.
- Due to serious defaults.
- Due to the collection of overdue payments.
- When the customer agrees to share the information with a processor.
- Due to the handling of a case by arbitration committees or the courts.
- When the law stipulates that information be shared.

When a service is acquired from a third party, whether in IT or debt collection, the Bank seeks to do business with parties who have taken appropriate security measures when processing personal data and who comply with the legislation and rules on data protection.

Service providers which are receiving data concerning the business dealings and/or private concerns of customers are bound by the same obligation of confidentiality as applicable to employees of Arion Bank. The handling of information and the requirements made by Arion Bank of processors are specified in the processing agreement which the Bank makes with service providers.

6.2. Transferring data abroad

In certain circumstances data may be transferred abroad and outside the European Economic Area (EEA), for example in fulfilment of contractual obligations to a customer or legal requirements. If personal data is transferred outside the EEA it must be ensured that the data is protected in the same way as before.

7. How long do we keep data?

Personal data is kept while the business relationship between the customer and the Bank still exists or for as long as necessary given the purpose of the processing, the terms of agreements, the rules of the Bank or as long as there are objective grounds to keep such data.

Objective grounds exist if the data is still being processed according to the original purpose for its collection or in connection with the Bank's commercial interests, e.g. to set out or protect the Bank's legal claims, and such grounds could justify the keeping of such data after the business relationship ends. The Bank will try not to keep data in a personally identifiable format any longer than necessary. Consequently, different types of data may be kept for different lengths of time.

The storage times of data may be stipulated in legislation such as the Account Act No. 145/1994 and the Securities Transactions Act No. 108/2007. The Bank is required to keep information and data in accordance with this legislation and other acts of law applicable to the activities and which stipulate a storage period for information. Copies of personal identification documents, public data and other information collected about individuals on the basis of Act No. 140/2018 on Money Laundering and Terrorist Financing are kept for at least five years after individual transactions or business relationships end.

8. Rights of the customer

The Data Protection Act guarantees customers various rights, which will be discussed in this section, but these rights may be subject to certain restrictions. Examples of this include if it is not possible to comply with a request to erase data on the basis of provisions in the law on the storage time of such data. If the Bank is unable to comply with such a request for any reason the customer is informed of this.

8.1 Access to own personal data – personal data reports

The customer is entitled to know whether the Bank is processing personal data about them. The customer is entitled to access to the data and to get information on the purpose of processing, the categories of recipients, the origin of data, whether automated decisions are being made, and information on the customer's rights (including the right to submit a complaint to the Data Protection Authority). The customer can request information on recorded personal data about them in Arion Online Banking.

8.2 Rectifying inaccurate personal data

If the customer believes that any of the information kept by the Bank about them is inaccurate they are entitled to have it rectified.

8.3 Erasing data

The customer is entitled to demand that the Bank erase personal data on the customer if they believe the data is no longer necessary to the purpose for which it was collected. The same applies if the customer 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.

8.4. Right to object and restrict processing

The customer is entitled to object to the processing of personal data about themselves and the use of this data in direct marketing at any time, including in profiling.

The customer is entitled to ask the Bank to restrict the processing of personal data about them, if there is any doubt that the data is correct, if the processing of the data is illegal or the Bank no longer needs the data but the customer needs the data to establish, maintain or protect legal claims.

The customer is entitled to decline at any time the processing of personal data for marketing purposes and can decline such services in Online Banking. It may take time to update systems so the customer may continue to receive marketing material for a period of time. Please note that although the customer declines marketing material, the Bank continues to send important information to the Bank, e.g. changes to terms or to inform the customer of their contractual obligations.

8.5 Right to data portability

The customer is entitled to obtain personal data about them or which they have provided the Bank with in structured, commonly used and machine readable formats. The customer can also request that the Bank send data about them to a third party. This only applies if the processing of personal data is based on consent or in order to carry out an agreement and the processing is automated.

8.6 Withdrawing consent

In cases where consent is a condition for processing personal data, the customer is entitled to withdraw their consent. 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.

8.7 Complaints to the Data Protection Authority

Complaints can be made to the Icelandic Data Protection Authority (Persónuvernd) by contacting the organization at its headquarters at Rauðarárstígur 10, 105 Reykjavík or by e-mail at postur@personuvernd.is. 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.

9. How do we guarantee the security of personal data?

Arion Bank is obliged to guarantee the security of the personal data it processes. The Bank fulfils this obligation by setting a security policy, assessing the risk involved in the processing of data, e.g. the risk that unauthorized persons may gain access to the data or the data gets damaged or destroyed, and the Bank therefore takes measures to mitigate such risk. The security measures mainly 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. In the event of any security breach concerning the handing of personal data where it has been confirmed or is suspected that personal data has come into the possession of an unauthorized party, the Data Protection Authority and, according to circumstances, individuals are notified of the security breach, unless it poses a considerable risk to the rights and freedoms of the individual.

10. How can I contact the Bank on matters concerning data protection?

Arion Bank has a Data Protection Officer as stipulated by the Data Protection Act. The role of the Data Protection Officer is to monitor compliance with the legislation and regulations on data protection and the General Data Protection Regulation (EU) 2016/679. You can contact the Data Protection Officer by e-mail at personuvernd@arionbanki.is. For further information see section 2 on data controllers. The Data Protection Officer is the Bank's contact person with the Data Protection Authority.

11. How do we update or change the Data Protection Notice?

The Bank is authorized 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.