PERSONAL DATA PROTECTION POLICY

OF KVIKA HF.

Adopted in September 2020/ Responsible party: CEO

1. INTRODUCTION AND SCOPE

This Personal Data Protection Policy (hereafter "the policy") provides information on what personal data Kvika hf, Katrínartún 2, 105 Reykjavík (hereafter "Kvika" or "the bank") collects on its customers; how the bank processes personal data and for what purpose; how long this data can be expected to be stored; where and to whom it may be communicated; and how its security is assured in the bank's operations. Information is also provided on customer's rights regarding the processing of personal data by the bank. The policy has been adopted with the aim of ensuring fair and transparent processing of personal data in compliance with the law on protection of personal data and its processing.

This Personal Data Protection Policy has been drafted with reference to Art. 17 of Act No. 90/2018, on Data Protection and the Processing of Personal Data. This policy applies only to individuals and not to legal entities. The term "personal data" includes all information that can be linked to a specific person directly or indirectly, e.g. through reference to his/her personal identification, such as a name, Id. No., username, loan no. etc. This policy applies to the bank's former, current and future customers, parties connected to the customer (e.g. family members), guarantors and other relevant parties, such as the beneficial owner of funds, a customer's agent, authorised signatories and parties related to the customer in the case of a legal entity. The policy also includes, as the case may be, individuals other than the customer, e.g. employees of the bank's contractors and persons visiting the bank's offices or website, www.kvika.is, as further described in this policy. References to "the customer" in this policy apply to all of the above parties. Kvika is responsible for all personal data that the bank collects and processes on its customers and is therefore responsible for ensuring that the processing of personal data complies with applicable personal data protection laws.

2. TYPES AND SOURCES OF PERSONAL DATA

When a customer applies to establish a business relationship, Kvika requests information, both from the customer and other parties. The collection of such information is necessary to fulfil the bank's statutory obligations, in particular, the Act on Measures to Combat Money Laundering etc., the Act on Consumer Credit, the Act on Financial Undertakings and the Act on Securities Transactions. The following is a list of most categories of personal data that the bank processes and a description of its purpose in processing this data:

- **Contact information**: name, address and other contact information such as e-mail address, telephone number and job title to enable the bank to communicate with the customer.
- **Id. No., identification and electronic ID:** Id. Nos., identification, information on nationality, e.g. such as a passport, driver's licence and electronic ID, to enable the bank to identify the customer.
- **Financial data**: Business history, turnover, account movements and account balances, account numbers, credit card information, interest terms, income, financial obligations, defaults, credit ratings, credit score etc. for the purpose, among other things, of making decisions on creditworthiness and solvency and prevent customer over-indebtedness.

- **Information on contracts:** Details concerning agreements that the customer has concluded with the company and information on the products and services that the bank provides to the customer so that the provisions of the agreements can be implemented.
- **Information on the communications:** Information that the bank receives from the customer in letters and e-mails that the customer sends to the bank to enable the bank to provide the customer with services, improve them and respond to messages and suggestions.
- **Publicly available information:** E.g. information from the National Registry, the Real Estate Registry, the Register of Limited Liability Companies and other public registers, as well as information that can be accessed from a financial information provider or information that has been made public on the Internet. This information is used for various purposes in connection with the bank's operations.
- **Information for customer due diligence:** Information to enable the bank to carry out due diligence as provided for in Act No. 140/2018, on Measures to Combat Money Laundering and Terrorist Financing, and to ensure compliance with international sanctions, including determining that the purpose and nature of a business relationship accords with law and whether the client is a politically exposed person.
- **Electronic surveillance:** The bank's offices are monitored using surveillance cameras for security and asset protection purposes.
- **Recording of telephone conversations**: The customer's telephone calls to the bank may be recorded. This processing takes place, e.g. in order to be able to prove whether a transaction has taken place and for security purposes.
- **Consent:** Any approval or authorisation given by the customer to the bank. This includes information on how the customer wishes to be contacted, e.g. whether he/she declines to receive mailings from the bank or communication based on cookies.
- **Cookies:** Cookies are small computer files that are sent to the customer's computer or smart device when the customer visits a website. They are stored in the customer's device and are sent back when he/she revisits the website. The cookies contain information about the customer's visits to websites, e.g. so that he/she need not enter a username or password on each visit, or to analyse website traffic, see further Kvika's terms for the use of cookies on the bank's website.
- **Information on eligibility:** The bank assesses the client's eligibility to conclude transactions and for this purpose processes information on the client's education and experience, financial situation and risk appetite in order to classify the client as a retail client or professional client.
- **Information about behaviour and usage:** Information on how the customer uses the bank's products and services to enable the bank to make improvements to them, and also to monitor whether everything is in order, both in terms of security and usage.
- **Technical data:** E.g. information about the equipment with which the customer connects to the bank and derivative data from that connection, such as IP addresses, versions of operating systems and actions performed. The purpose is to improve service and for debugging.
- **Information on job applicants:** Information provided by applicants seeking to work for the bank included in their CVs, such as name, Id. No., address, telephone number, e-mail address, education and qualifications, work experience etc.
- **Sensitive personal information:** Some personal information is classified as sensitive under the Act on Data Protection and the Processing of Personal Data. This includes information relating to race or ethnic origin, political views, religion or philosophical convictions, trade union membership, genetic data, biometric data and health information. Kvika neither collects nor processes this personal information without the customer's consent except with special legal authorisation. In individual instances, processing may prove necessary for the bank with reference to the public interest or in order to establish, bring or defend legal claims.

The above list is not exhaustive and the bank may process other information about the customer as necessary at any given time, depending on the nature of the business relationship or the customer's communication with the bank.

It should be noted that the customer can always choose whether to provide personal information. Failure to provide information may, however, affect Kvika's ability to provide services to the customer.

3. USE OF PERSONAL DATA AND PROCESSING BASIS

The authorisation for processing personal data depends upon the nature of the customer's contractual relationship with Kvika and the purpose of processing. Kvika uses the customer's personal information in particular to contact the customer, to identify him/her and ensure the security and reliability of business transactions, to execute orders and provide financial services, to develop the bank's products and services offered, to respond to legal requests and to ensure network and information security. Kvika's authorisations for processing personal data are in most cases based on the following:

a. To fulfil the bank's contractual obligations

Personal data is processed to provide banking and financial services in accordance with an agreement concluded with the bank's customer. The purpose of the processing varies depending on the services provided, such as accounts and payment services, credit facilities, asset management, advice and custody, personal pension savings, corporate advisory etc. Further details concerning the purpose of processing based on the bank's agreements with the customer can be found in the relevant agreements and their terms and conditions.

b. To fulfil statutory obligations

Kvika's processing of personal data is based to a large extent on various statutory obligations that require Kvika to process certain personal data for a specific purpose. These include obligations in the following acts:

- Act No. 161/2001, on Financial Undertakings;
- Act No. 120/2011, on Payment Services;
- Act No. 140/2018, on Actions to Combat Money Laundering and Terrorist Financing;
- Act No. 33/2013, on Consumer Credit;
- Act No. 108/2007, on Securities Transactions;
- Act No. 87/1998, on Official Supervision of Financial Activities;
- Act No. 129/1997, on Mandatory Guarantee of Pension Rights and Operation of Pension Funds;
- Act No. 90/2003, on Income Tax;
- Act No. 145/1994, on Accounting;
- Act No. 118/2016, on Consumer Mortgage Credit;
- Act No. 32/2009, on Guarantors.

Gathering of information for the purpose of identifying the customer, carrying out due diligence, assessing creditworthiness and suitability to engage in securities trading, fulfilling statutory reporting obligations and managing the bank's risk is based, among other things, on the above-mentioned acts.

c. To safeguard legitimate interests of the bank or third parties

In cases where processing is necessary due to the legitimate interests of Kvika, a third party or the customer, the bank may process personal data of the customer beyond what is necessary to fulfil and enforce the bank's contractual obligations, unless the customer's interests take precedence. Kvika's processing of personal data on this basis is connected, in particular, with the bank's asset and security custody, e.g. in connection with:

- enforcing claims of the bank or third parties;
- risk management;
- prevention of fraud and organised crime;
- the bank's information security;
- surveillance of the bank's offices and access controls;
- general customer management and communication;
- marketing, unless the customer has objected; and
- auditing and optimisation of services.

d. On the basis of consent

If the customer has given consent for the bank's processing of personal data for a specific purpose, such consent is the basis for this processing, e.g. connection with obtaining a credit rating and credit score from CreditInfo hf. The customer can always withdraw this consent. Withdrawal of consent does not, however, affect the legality of the processing of personal data that took place prior to revocation.

4. COMMUNICATION OF PERSONAL DATA

Insofar as this is necessary to enforce the bank's contractual obligations to the customer, Kvika's employees have access to personal data. In addition, Kvika's service providers, who process personal data on the bank' behalf, have access to personal data. These are companies that provide payment services, financial services, hosting and IT services, postal services, printing, telecommunications, debt collection, consulting, auditing and sales and marketing services. Kvika deals only with service providers who offer adequate protection for personal data in accordance with data protection legislation.

Kvika also shares information with companies within the bank's group in connection with statutory risk management. Finally, Kvika is obliged to provide public parties, such as the Central Bank, tax authorities, regulators, police authorities, liquidators and courts, with access to personal data. With regard to disclosure of personal data to parties outside the bank, it should be noted that Kvika's employees are legally bound by obligations of confidentiality in all matters concerning the situation of the bank's clients and other matters of which they may become aware in the course of employment and should be kept secret pursuant to Art. 58 of the Act on Financial Undertakings, No. 161/2002, unless obliged by law to provide this information or if the customer has given consent for such disclosure.

Examples of such disclosure of personal information are cases where, for example, there is an obligation to assist in the recovery of funds that have been credited to a customer's accounts by mistake; when it is necessary to trace funds on suspicion of fraud or financial crime; for the collection of claims in default; in connection with the handling of cases before complaints tribunals or courts; and where the law provides for the disclosure of information.

5. DISCLOSURE BEYOND THE EUROPEAN ECONOMIC AREA

In certain cases, data may be transferred out of the country and outside the European Economic Area (EEA), for example, to fulfil contractual obligations to the customer or obligations imposed on the bank by law. Kvika only transmits personal data to countries outside the EEA if this is necessary in order to carry out the customer's requests, such as payment requests or requests for transactions, if this is required by law, such as obligations to notify under tax legislation (CRS and FATCA), or if the customer has consented to such disclosure. When such transmission occurs, Kvika is responsible for ensuring that the recipient has appropriate protection measures in place to ensure adequate protection of personal data.

6. PRESERVATION OF DATA

Personal data is preserved as long as the business relationship is in effect and the law prescribes or as Kvika's business interests require and there is valid reason for so doing. There is considered to be valid reason if processing of the data is still underway in accordance with the original purpose of its collection or due to the bank's commercial interests, e.g. to define, present and protect the bank's claims.

Kvika endeavours to avoid storing data in personally identifiable form for longer than necessary. Kvika bases its retention period in particular on the Accounting Act, the Income Tax Act, the Value-added Tax Act, the Act on Money Laundering etc., the Act on Securities Transactions, the Act on Official Supervision of Financial Activities, Guidelines of the Financial Supervisory Authority (FME) on Information Systems of Supervised Entities, the Act on Limitation of Claims Rights etc. If data is considered to have historical value, it is made non-personally identifiable by erasing personal identification.

7. CUSTOMER RIGHTS

In connection with the processing of his/her personal data, the customer is entitled to:

- request information on how Kvika processes the personal data and receive a copy of that data;
- request the correction of incorrect personal data processed by Kvika or request that incomplete personal data be completed;
- request that the personal data be deleted if the customer considers the information no longer necessary for the purpose of its collection. The same applies when the customer withdraws the consent on which the processing of personal data is based and there is no other legal basis for its processing or if the processing of the information is unlawful;
- request that Kvika limit its processing of personal data in certain cases, such as when processing has been objected to;
- request to receive the personal data in a systematic, common and computer-readable format and have it sent to another institution;
- revoke previously granted consent for the processing of personal data. Withdrawal of consent does not affect the legality of the processing based on consent that took place prior to revocation;
- object to processing for the purpose of direct marketing;
- object to the processing of personal data by Kvika on the basis of legitimate interests, such as processing that involves the creation of a personal profile (personal profiling);

- file a complaint with the Data Protection Authority if the customer considers that Kvika's processing of his/her personal data violates applicable law.

If the customer objects to the processing of personal data, Kvika will cease processing the personal data unless the bank can demonstrate a legal obligation or legitimate interests that take precedence over the customer's interests.

If you wish further information about your rights or how you can exercise them, you are advised to contact Kvika's Data Protection Officer (see contact details in Section 11).

8. AUTOMATED DECISION-MAKING (ADM) AND PERSONAL PROFILING

Automatic decision-making means that a decision is made on the basis of automatic data processing, without the involvement of Kvika's employees or other individuals, and such a decision has legal effect vis-à-vis the customer, such as automatic rejection of an online loan application. At present, no business decisions are made automatically; however, if this changes, Kvika will provide the bank's customers with further information.

Kvika processes personal data with the aim of assessing certain personal aspects concerning the customer (personal profiling). The bank uses personal profiles in the following cases:

- Under the Act on Money Laundering etc. the bank is obliged to monitor regularly the customer's transactions, incl. transfers and card transactions, in order to check whether they are consistent with the information provided about the customer and his/her activities when the business relationship began.
- As part of the bank's statutory risk management, customers are classified according to creditworthiness. This calculation is based, among other things, on income, expenses, obligations, employment, duration of employment, business history and information from CreditInfo hf.

9. SECURITY AND PROTECTION OF PERSONAL DATA

Kvika takes appropriate measures to protect customers' personal data from misuse, compromise and damage, unauthorised access, alteration or disclosure. The measures that the bank relies on are, in particular:

- implementing technical and organisational measures designed to ensure the lasting confidentiality, continuity, availability and resilience of processing systems and services;
- controlling individuals' access to Kvika's offices and maintaining security surveillance;
- controlling access by employees and others to systems that contain personal data;
- ensuring that persons with access to the customer's personal data have taken appropriate protection measures to ensure the security of personal data; and
- when required by law, deleting, pseudonymising or encrypting the customer's personal data.

In all processing work involving information security, Kvika follows the ISO 27001 data security standard and FME Guidelines no.1/2019 concerning risk in the operation of IT systems of supervised entities. Kvika has adopted a written policy on information security management.

In the event of a security breach in the processing of personal data, where it is confirmed or suspected that personal data has fallen into the hands of an unauthorised party, the Data Protection Authority and, as the case may be, the customer, are notified of the security breach, i.e. unless it involves no major risk to the customer's rights and freedom.

10. CHANGES TO THE PERSONAL DATA PROTECTION POLICY

This policy will be updated regularly to accord with changing business practice and legal obligations. If Kvika makes significant changes to the manner in which the bank processes personal data, the policy will be updated to reflect those changes. Kvika encourages the customer to review this policy regularly in order to keep informed about how the bank uses and protects personal data.

11. CONTACT INFORMATION

The customer can contact Kvika's Data Protection Officer concerning all matters related to the processing of his/her personal data and the exercise of rights under the Act on Data Protection and the Processing of Personal Data.

Any questions concerning the processing of personal data or comments on this policy should be directed to Kvika's Data Protection Officer by letter or e-mail.

Kvika hf.
Katrínartún 2, 105 Reykjavík
c/o Data Protection Officer
E-mail: personuvernd@kvika.is

This Personal Data Protection Policy was last reviewed in September 2020.