Privacy Policy
Landsbankinn

Document No. 201806-0817-4 | Adopted in February 2023 | Review in 2025 | Audit Committee

Privacy Policy of Landsbankinn

I. Application of the Privacy Policy

Landsbankinn places strong emphasis on protecting the privacy of its customers and parties who communicate with the Bank in order to safeguard their rights. This Policy contains information on the data the Bank gathers about you, how it is used, how its security is ensured, and your rights under the Data Protection Act.

This Policy applies to the processing of personal data in the Bank's entire operation and to all persons who do business with it, including former, current and prospective customers, parties connected to customers, such as family members, and guarantors and holders of power of attorney. The Policy also applies to persons other than customers, such as individuals who are in communication with the Bank, visit its facilities or website, apply for grants or participate in events hosted by the Bank.

The Policy does not apply to the operation of legal entities, neither associated entities nor subsidiaries of Landsbankinn. The Bank may need to process information about individuals connected to legal entities who are customers, such as beneficial owners, directors of the board, executives, authorised signatories and, as the case may be, employees of the legal entity.

Please note that details about treatment of your personal data may be provided in the General Terms and Conditions of Landsbankinn hf., special terms and conditions or information provided for certain products or services.

II. Types of personal data that is collected

The collection and processing of personal data allows the Bank to provide you or companies, which you work for or are connected with, with requested financial services. The personal data you submit includes:

- *Basic information*: Name, Id. No., address, telephone number, email, name of employer and other basic information, as the case may be, on nationality, marital status, spouse, children, custodianship and connected parties such as legal guardians, holders of power of attorney or guarantors.
- *Communication and contract information*: All your interaction with the Bank that takes place via email, phone, online chat or on social media. The Bank also processes all information derived from or submitted in relation to any contracts you enter into with the Bank, e.g. for individual products or services.
- *Information about identification*: Any copies of legally required or electronic identification, including copies of your passport or driver's licence, your preferred means of identification and communication channels. This also includes the time and date of your visits to the Bank's branches if you chose to register your Id. No. when you visit.
- *Financial information*: All information about your current and previous business and transaction history, including account balance and movement, turnover, origin of funds, movement statement and information about payment cards, payment history including any late payments, and payment orders along with information about income, expenses, financial commitments, and assets and liabilities.
- *Information gathered in the course of electronic surveillance*: The recording of electronic communication and video recordings made with security cameras at the Bank's premises and ATMs.
- *Technical information and inferred data about behaviour and use*: About the equipment and devices you use to connect to the Bank's website, online banking and app, such as username, settings, IP number, type, number and settings of smart devices, operating system and browser type, language settings, how you connect to us, and the origin and type of actions undertaken.
- *Public information*: From public registries such as Registers Iceland, the Icelandic Property Registry, the vehicle registry, the Registrar of Enterprises, the Legal Gazette and other public registries.
- *Sensitive personal data*: Includes, as the case may be, racial or ethnic origin, political affiliation, religious and philosophical views, trade union membership, health information, and biometric data.
- *Other information:* The list above is not exhaustive and the Bank may process other personal data depending on the nature of the business relationship or your transactions with the Bank.

In exceptional cases, the Bank may need to gather information classified as sensitive personal data. In other instances, financial information, e.g. transaction statements for payment cards or use of current accounts, may include sensitive personal data that may indicate certain behaviour. We do not gather sensitive data about you nor do we process such data without clear authorisation and unless absolutely necessary.

Should you choose not to divulge necessary data, it may prevent the Bank from providing the requested service.

Processing of the personal data of children

The personal data of children may be processed if it is necessary in order to carry out requested transactions or provide service to minors, e.g. create a payment account and issue a debit card. The Data Protection Act states that the consent of a guardian is required for children under 13 years of age when offering electronic services online. Parents or legal guardians manage the finances of minors in their care and receive read access to their deposit accounts. For details about the processing of the personal data of children, visit www.landsbankinn.is/thjonusta-og-radgjof/ungafolkid. All marketing material, including gifts, notifications and benefits targeting children, is sent to guardians and, as the case may be, children. It is possible to opt out of such marketing material and gifts through Landsbankinn online banking or the Bank's data rights portal.

III. How is personal data used in the Bank's operation

Landsbankinn processes personal data for clear and declared purposes in accordance with the Data Protection Act, the Bank's rules and this Policy. Processing of personal data may have various purposes, such as:

- *To contact you*, *identify you* and *ensure the security and reliability of business transactions*, including via digital authentication and due diligence on customers or for the purpose of individual transactions.
- *Carry out requested transactions, provide financial services and advice and respond to enquiries*, such as establish and maintain a business relationship, perform payment and credit assessments and determine self-service authorisations, assess credit risk and prevent borrowing from exceeding repayment capacity, analyse financial standing with regard for the Bank's product and service offering in order to provide advisory service, including on asset management, pension savings or other service, receive applications for and disburse pension savings.
- For *reasons of security and safeguarding of property*, to safeguard the interests of customers, employees and others who have dealings with the Bank, ensure the traceability of transactions through such means as electronic monitoring and investigate issues or prevent money laundering, terrorist financing, fraud and other punishable conduct.
- *Develop the Bank's product and service offering*, promote innovation and boost service levels, improve functionality and carry out quality control, offer tailored services, respond to suggestions and complaints and process answers to marketing and/or service questionnaires.
- For *marketing and promotional purposes* and to provide personalised and tailored services, send messages about benefits and material that may interest you or you have requested. Note that photographs and video recordings are made at conferences, promotions and other events hosted by the Bank and that these may appear publicly on the Bank's websites, including social media.
- *Develop solutions and reports for the purposes of credit and risk management*, such as to measure and monitor credit risk, operational risk, market risk, underwriting risk and for internal treasury purposes, including the use of electronic surveillance of parties responsible for the payment of claims, i.e. a customer or guarantor.
- *Operate and maintain the Bank's websites and online services* and improve user experience online, enable you to access financial information and tend to banking business online, including in Landsbankinn's app and online banking platform, and, as the case may be, the Bank's other web-based solutions.
- Respond to *legal requests and ensure cyber and data security* by, among other things, analysing, investigating and preventing fraud and other misconduct.
- Perform *statistical analysis* on certain products, services or communication channels, front office or other individual functions in the Bank's operation. Such analysis is based on non-personally identifiable data, if possible.

Authorisation to process personal data

For the most part, the gathering and other processing of your personal data by the Bank is based on an *agreement* between you and the Bank for specific services and in order to provide the requested financial service or to *satisfy legal obligations* the Bank is subject to as a regulated entity on the financial market. In certain cases, the Bank will request your *informed*

consent to process personal data. In such cases, you can withdraw your consent at any time, and then the processing covered by the consent is terminated. Processing of personal data in connection with the following products and services is based on consent:

- 360° financial review
- Use of Landsbankinn online banking and Landsbankinn's app
- Authorisation to obtain information on an individual's finances
- Appointment for remote meeting
- Grant applications, games and lottery run by the Bank
- Processing of requests about your rights in the Bank's data rights portal and other requests
- Other ad hoc processing

Finally, your data may be processed if the Bank, you yourself or a third party has a *legitimate interest* of such processing. Such processing does not take place if it is clear that your interests outweigh the interest of the Bank or a third party of such processing. The following processing operations are based on legitimate interest:

- Processing of basic information from Registers Iceland
- Determination of benefit programmes for customers and retention of the business history of former customers
- Classification and monitoring of loans
- Development and testing of new products and services
- For marketing purposes and target group analysis
- For cyber and information security purposes
- Other ad hoc processing.

Automated decision-making

In certain instances, the Bank creates a *personal profile* using automated processing of your personal data to assess or anticipate aspects of your finances, such as development of financial standing or probability of default. Calculation of a rating grade is an example of profiling. Profiles may also be prepared for marketing and cyber and information security purposes, e.g. to determine which benefit programme suits you best, and by employing pattern analysis in online banking to maximise safety in online banking and Landsbankinn's app.

Profiling may also be a factor in *automated decision-making* that relates to you. In automated decision-making, software processes your personal data automatically to reach a decision, without the aid or involvement of human agency. An example of automated decision-making is the calculation of your credit framework that determined the amount of credit you can apply for using self-service channels.

Automated decision-making only takes place with your consent, if it is a prerequisite for the conclusion or execution of an agreement between the individual and the Bank, or if authorised by law. You can submit objections or contest automated decisions by email to personuvernd@landsbankinn.is.

IV. Where does the Bank get information from and who is it submitted to

The aforementioned personal data in the Bank's possession is usually *gathered directly from you* when you enter into a business relationship with the Bank, apply for or use a certain product or service or contact the Bank through such channels as email, online chat or by other means.

Information can also be *sourced from third parties*, including the Bank's partners, such as card issuers, payment service providers and public entities. Unconnected parties may also provide information about you, e.g. financial information agencies, customs and tax authorities and public registries. External parties are not authorised to submit information about you to the Bank unless authorised to do so, for example with your consent or legal authorisation.

The Bank may also need to disclose your personal data to a third party. Legal guardians receive read access to the bank accounts of minors in their care. Domestic or foreign partners and/or service providers to the Bank receive access to data in order to provide you with certain services. The Bank selects its partners and service providers with care and does not disclose personal data unless they comply with the Bank's security demands. Such partners include non-domestic commercial banks who receive information in connection with foreign payment and settlement, transfers and card issuance, claim collection, operation and hosting providers, financial data bureaus and custodians of financial instruments.

In certain cases, the Bank is obligate to divulge personal data to law enforcement authorities, other authorities or regulators both domestic and abroad based on legal obligation or international contracts. The Bank is focused on safeguarding the

human rights of its customers, including their privacy, and processes such requests in accordance with documented work procedures in order to ensure that it does not divulge other personal data than what is necessary each time and only based on clear authorisation.

Disclosure to third parties may also take place based on your consent, e.g. if you request that the Bank provide fintechs or other entities with your payment information or if your grant power of attorney for a third party to access your financial data. You can also authorise the Bank to divulge other information, such as your name, email or phone number, to partners for marketing purposes.

V. Your rights

The Data Protection Act affords your certain rights, including to instruction and information about whether the Bank processes your personal data and how such processing takes place in the Bank's operation. You can manage your rights through the customer data rights portal on the Bank's website and use it to request:

- *Access to your personal data*

  You are entitled to confirmation from the Bank as to whether your personal data is processed and, if so, to access this data. You are also entitled to certain minimum information about the organisation of processing, provided among other things in this Policy.

- *Transfer of personal data*

  You can request that certain personal data you have given to the Bank be transferred to another specified party, if technically feasible, or directly to you. This only applies to personal data which the Bank has gathered on the basis of your consent or for the performance of a contract and was processed automatically.

- *Correction or erasure of personal data*

  You can at any time request correction of erroneous or unreliable personal data. Under certain circumstances, you are also entitled to have personal data concerning yourself erased.

- *Limiting or objecting to the processing of personal data*

  You can at any time object to the processing of personal data, including personal profiles that serve direct marketing purposes and opt out of receiving promotional material on benefits, products and services in online banking, Landsbankinn's app or the Bank's data rights portal. You can also object to the processing of personal data based on your particular circumstances. Finally, you can in certain cases request that temporary limitations apply the processing of your personal data.

The Bank will accede to requests according to the above free of cost unless such requests are unfounded, excessive or if multiple copies of personal data are requested. Individuals must verify their identity when they wish to exercise their rights. For further information on processing of personal information, see the Bank's data rights portal.

You are also entitled to refer disputes over the Bank's handling of your personal data to the Data Protection Authority. We hope that you will contact us first with any privacy issues to allow us to help. If you do choose to contact the Data Protection Authority directly, the email address is postur@personuvernd.is.

VI. Safety of personal data

Your personal data is retained in a secure environment that safeguards it against unauthorised access, misuse or transmission. The Bank's management of information security is certified under information security standard ÍST ISO/IEC 27001:2013. The Bank also has in place an internal information security policy, rules on information security, security processes and has implemented organisational and technical security measures in accordance with laws and regulations on cyber and information security.

Landsbankinn uses electronic monitoring of both its internal and external environment to ensure the safety and traceability of transactions and to prevent fraud and misconduct. Electronic surveillance is carried out with surveillance cameras at the Bank's premises and with the audio recording of phone calls and other electronic communication. Strict access control applies to all content gathered using electronic monitoring and it is only reviewed in the case of dispute between the Bank and the customer, if there is reason to suspect criminal activity or for internal control purposes.

The Bank's products and services are designed with regard for security and privacy. The Bank regularly assesses the risk of processing personal data in its operation in order to apply appropriate security measures and ensure customer privacy in as much as possible. The Bank also promotes active security awareness amongst its employees and publishes educational material on the handling and security of personal data, in accordance with the Data Protection Act. All the Bank's employees are bound by confidentiality in accordance with the Bank's rules and laws that apply to financial undertakings. No service or software can be perfectly secure. Contact the Bank at the earliest opportunity if you are

concerned that your personal data may be compromised or if you think that someone may have acquired your password or other information by emailing personuvernd@landsbankinn.is. You will be informed of any data breaches with the Bank or its processors that affect you, in accordance with law.

VII. Cookies

The Bank's website, online banking platform and app (jointly referred to as websites), store cookies in your computer or smart device. Cookies are small text files that store information to analyse use of the Bank's websites and improve user experience. Cookies are also used to tailor websites to your needs, e.g. by boosting the function of a website, saving your settings, processing statistical information, analysing traffic through websites and, as the case may be, for marketing purposes.

The Bank's website utilises different types of cookies. So-called session cookies are generally deleted when a user leaves the website. Persistent cookies on the other hand are saved to the user's computer or device and store your actions or selections on the Bank's websites. Cookies are either first party or third party cookies, depending on the type of website. Upon your initial visit to the Bank's website, a banner appears asking you to approve optional cookies which are used by the website. You can revoke your consent at any time by changing the cookie settings either on the banner or your browser settings.

Necessary cookies, such as statistics cookies and functionality cookies, activate functions on the Bank's websites. They are a necessary prerequisite of use of the Bank's websites, allowing them to function as intended. Use of such cookies is based on the Bank's legitimate interests.

Other cookies, which are not a necessary prerequisite of use of the Bank's websites, require your consent. They often play an important role in the use and functionality of websites as they facilitate use by, for example, auto-completing forms and saving settings. First party cookies only send information about you to Landsbankinn.

Third party cookies are also used on Landsbankinn's websites, including analytic and advertising cookies from Facebook and Google. These third parties may store cookies in browsers or devices and gather information about visits to the websites. Landsbankinn gathers the following information from these cookies:

- Number of visitors, number of visits per visitor, day and time of visit.
- Which pages on the websites are viewed and how frequently.
- Type of files downloaded from the websites.
- Which devices, operating systems and browsers are used during visits.
- Which search words used in search engines lead to the websites.

A more detailed description of cookies, including the third party cookies the Bank uses, is available on the Bank's website. Information about the use of third party cookies is also available on their respective websites.

VIII. How long does the Bank retain information

Generally the Bank retains your personal data for the duration of the business relationship, as long as required by law or to satisfy the Bank's legitimate interests. The strict rules that apply to the Bank's operation may require different retention times depending on the type or nature of your personal data. The Bank is an entity subject to an obligation of transfer, in accordance with the Act on Public Archives. The obligation to transfer means that the Bank is obliged to retain all records in the Bank's archive and transfer them to a public archive when they have reached an age of 30 years. The Bank strives not to retain information in personally identifiable form for longer than is necessary and safeguards such information in every respect.

Email and other electronic communication is retained for five years. Audio recordings of telephone conversations and visual recordings from electronic monitoring is not retained longer than provided for by laws and rules of the Data Protection Authority for electronic surveillance and deleted automatically once that period elapses. Audio recordings of telephone conversations that pertain to securities transactions are retained for 5 years in accordance with the Act on Securities Transactions. Strict access control applies to content gathered using electronic monitoring. The Bank's Compliance function may listen to phone recordings as part of its monitoring of transactions with financial instruments.

Specific legislation also provides for the obligation to retain certain information such as accounting records, personal identification and other information required under the Act on Actions to Combat Money Laundering and Terrorist Financing.

IX. How do I get in touch

Landsbankinn hf., Reykjastræti 6, 101 Reykjavík, is responsible for ensuring that all treatment of your personal data complies with the Data Protection Act and rules and is considered a controller of the processing of your personal data.

Landsbankinn's Data Protection Officer is responsible for ensuring the Bank's activities comply with applicable laws and rules on personal data protection. Please direct any queries, comments and suggestions relating to the processing and handling of personal data to the Bank's Data Protection Officer by email to personuvernd@landsbankinn.is.

The Bank reserves the right to update this Policy on a regular basis. The Bank will inform you about major changes to the Policy before they become effective upon publication to the Bank's website, www.landsbankinn.is.

Approved initially on 15 June 2018

Most recently amended on 1 February 2023