MAGNETIQ BANK

Privacy Policy

Approved in Board meeting

Riga, 28.08.2025.

Magnetiq Bank Privacy Policy

1. Terms and Abbreviations

1.1. **Processor** – a natural or legal person, public authority, agency or other body which processes Personal data on behalf of the controller.

1.2. **Processing** – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.3. **Bank** – Magnetiq Bank, registration No. 50103189561, the legal address: Brivibas iela 54, Riga, LV-1011, phone number (+371) 6 777 2 999, e-mail: info@magnetiqbank.com, website: www.magnetiqbank.com. In scope of this Policy the Bank acts as **the Controller**, defining the processing means and purposes, as well as evaluating and choosing the Processors.

1.4. **Data Regulation** – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

1.5. **Data Subject** – an identifiable natural person who can be identified, directly or indirectly (for example, clients, representatives of clients – legal entities based on requirements of the law, employees, visitors of the Bank, shareholders, beneficial owners in scope of certain deals). All private persons whose Personal Data is processed by the Banka re considered to be the Data Subjects.

1.6. **DSI** – Data State Inspectorate: a regulator, which supervises implementation of the Data Regulation and protection of the Personal Data.

1.7. **Group** – Signet Bank AS, registration No. 40003043232, legal address: Antonijas iela 3, Riga, LV-1010, Latvia and all of its subsidiaries.

1.8. **Personal Data** – any information directly or indirectly relating to a Data Subject, such as name, surname, personal identity number, address, phone number, date and time of birth, financial data, data on the banking services, identifiers assigned by the Bank.

1.9. **Policy** – the Bank's Privacy Policy providing the Data Subjects with information on the Bank's Personal Data Processing operations**.**

1.10. **Third Party** – a natural or legal person, institution or organization, which has its own independent purposes for Processing the Personal data and that is not a Data Subject, Bank, Processor, or Processor's employees, and other persons engaged by the Bank or Processor to Process the Personal Data.

2. General Conditions

2.1. The Policy has been developed in compliance with the Data Regulation, Personal Data Processing Law, Credit Institution Law, and other respective legal acts in force in the Republic of Latvia, as well as the Bank's products and services.

2.2. The Bank provides due protection of the Personal Data, as well as all necessary technical and organizational means of Processing in order to prevent the unauthorized access to data, unlawful Processing, accidental loss, destruction or damage and other activities that directly or indirectly endanger confidentiality, integrity and accessibility of the Personal Data or in any other way breaches the Data Regulation and other legal acts.

2.3. The Bank processes the Personal Data just in case the Processing purpose cannot be achieved by some other means in a due manner. The Bank primarily processes Personal Data to conclude and perform contracts, comply with its legal obligations stated by the legal acts, for the performance of the tasks carried out in the public interest, as well as in accordance with its legitimate interest. The Bank requests from the Data Subject and from the Third Parties only the Personal Data and other information that is limited for achieving specific purposes, and ensures that the Third Parties receive only minimal required amount of the Personal Data.

2.4. If the Data Subject refuses to provide Personal Data and other information for any reason whatsoever, the Bank is entitled to refuse, suspend, or terminate the provision of services (operations), entering into contracts, and other rendering other actions related to the banking services. The Bank may request the Data Subject's consent for Processing for the purposes not related to receiving the service, concluding or performing contracts, or other purposes stated in the Policy hereto.

2.5. The Bank provides access to the Personal Data only for duly authorized Bank's employees who need such access in order to fulfill their official working duties. All Bank employees comply with the Personal Data protection principles and rules when processing the Personal Data. The Bank ensures that the personnel understand the duties implied by the Personal Data protection principles, implies the due controls and after-checks, and organizes regular learning sessions on Processing principles, rules of access to the Personal Data and conditions for using the information systems.

2.6. The Bank has implemented the Personal Data breach system in order to minimize the impact of the breaches on the Processing operations and Personal Data protection, the banking processes in general, as well as minimize the risk of repeated breaches. The Bank regularly analyzes possible risks related to Personal Data protection and their impact on the Data Subjects.

In case the Personal Data breach is identified, the Bank conducts the thorough inspection of the detected incident, provides the evidences hereto and mitigates or minimizes the respective consequences; in cases specified in the Data Regulation, DSI and the impacted Data subjects are informed.

3. Personal Data Processing Principles

The Bank complies with the principles relating to Processing of Personal Data stipulated by the Data Regulation:

- processes the Personal Data lawfully, fairly and in a manner transparent to the Data Subject in compliance with the 'lawfulness, fairness and transparency' principle, including but not limited with the following:
    - *timely informs the Data Subject on the Processing and the respective purposes of Processing in cases when enforceable regulations do not limit provision of such information;*
    - *provides information about the legitimate disclosure of the Personal Data (the Processing operations defined by the law might make an exception hereto);*
    - *initiates the Processing only based on the compliant legal grounds of Processing;*

- collects the Personal Data for specified, explicit and legitimate purposes and further processes the collected Personal Data only in a manner that is compatible with these purposes aligning with the 'purpose limitation' principle:
    - *evaluates the necessity of Processing operations to prevent collection and Processing of the Personal Data that does not achieve the pre-formulated purpose of the Processing;*
    - *does not collect, store the Personal Data for probable or unspecific future purposes;*
- complies with the 'data minimization' principle by processing minimal volume of the Personal Data limited to what is necessary in order to achieve the specified Processing purposes. The Bank regularly reviews the purposes and their compatibility with the Processing operations in order to prevent the excessive Processing;
- ensures accuracy of the Personal Data, keeps them up to date and timely, without any delay, deletes or corrects the Personal Data in line with the 'accuracy' principle. For example, the Bank might request the Data Subject to update his or her information provided in the client questionnaires or in any other way in a course of banking service provision;
- keeps the Personal Data for no longer than is necessary for the purposes for which the Personal Data are processed; and after the set retention term expires, the Bank deletes or anonymizes the Personal Data thus implementing the 'storage limitation' principle.
    - *The Personal Data can be kept longer in case further Processing takes place based on other legitimate purposes, e.g., when the Bank faces the need to comply with the regulatory requirements or in case of the legal proceedings.*
- The Bank ensures compliance with the Data Regulation, including the lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, integrity, and confidentiality principles in a manner to be able to demonstrate compliance with these principles, i.e. providing for 'accountability'.

4. Personal Data Types, Processing and Grounds for Processing

4.1. The Bank generally receives the Personal Data through via the following ways:

4.1.1. the Data Subject themselves provides personal information, *for example*, when filling out the forms to apply for the Bank services, questionnaires, payment orders, filing complaints and requests, as well as via communication with the Bank (verbally, by phone, e-mail and other communication channels;

4.1.2. via the Third Parties, *for example*, **state institutions and officials, public registers:** financial institutions, investigator offices, tax administration offices, courts, sworn bailiffs, sworn notaries, insolvency administrators, as well as in a process of applying for the Bank services, i.e., when a spouse provides data for another spouse in scope of lending process, also regarding the relation with politically exposed persons;

4.1.3. via security systems – video surveillance tools;

4.2. The Bank mostly processes the Personal Data of the following **categories of the Data Subjects**:

4.2.1. the Bank's clients and potential clients who express their intention to become clients of the Bank and their legal representatives (the authorized persons, Board members and procurators), shareholders, beneficial owners, family members, heirs;

4.2.2. participants of the deals of the Bank's clients and potential clients who express their intention to become clients of the Bank, as well as their representatives, payees and payers;

4.2.3. The Bank's business partners and their representatives (such as board members, procurators, authorized persons, contact persons), as well as shareholders and beneficial owners;

4.2.4. The Personal Data obtained in a process of cooperation with the state institutions and officials in compliance with the regulatory acts (from sworn bailiffs, sworn notaries, State and Municipal Police, the Bank of Latvia, the State Revenue Service, Prosecutor General Office, Financial Intelligence Unit);

4.3. The Bank processes the following categories of the Personal Data to ensure banking services and other types of operation for certain purposes, including but not limited to:

- **identification:** name, surname, personal identity number, birth data, as well persons' identity document (passport, ID card) data, for example, issue number and expiry date, photo;
- **communication with the Data Subject:** phone number, e-mail address, residence address;
- **provision of the Bank services and quality assurance, reporting purposes:** data received when the Data Subject attends the places where the Bank ensures its basic services, voice pitch, the data which the Data Subject provides in a course of written communication and phone calls, the level of authorities of the Data Subject, tax payer number and tax residence, IP addresses;
- **ensuring financial deals:** account number, information about the incoming and outgoing payments, transactions, total income and expense levels, obligations, deposit type chosen and purposes hereto, completed deals with financial instruments;
- **provision of lending deals:** owned movable and immovable property, estimated creditworthiness, credit obligations and history, including the payment discipline, experience in the finance area, amount of the credit obligations, sum of the debt obligations;
- **risk analysis**, **crime prevention, ensuring the compliance with obligations stipulated by the legal acts:** employment and economic activity, the source of income, type of the employment sphere and a period worked therein, citizenship, employee roles, commercial trade requests, as well the information on:
  - education level,
  - relation to the political organization and politically exposed persons,
  - related business partners,
  - political opinions,
  - inclusion into sanction lists,
  - reputation,
  - origin of the financial resources,
  - residence permit, if the Bank has a legal ground to perform such Processing;
  - criminal records and violations – to ensure compliance with anti-money laundering and terrorism financing prevention requirements in respect to a customer and

potential customer, its beneficial owners' and their representatives' economic criminal records, complying with the applicable data protection requirements;

- **security and property protection purposes:** data that might be obtained in a process of video surveillance – the looks, i.e., appearance, height, facial features, physique;
- **user identity verification, security of the information systems:** user names assigned to the Data Subjects, unique customer codes, used passwords;
- **marketing purposes:** information provided or accepted when the Data Subject provides the consent, for example, name, surname, e-mail address, and country – to ensure communication in the stated location; information on the used products aimed at presenting the personalized offer;
- **other types of Personal Data** in connection with provision of the payment services whereas the Data Subject is not the Bank's clients (for example, the payer, payee, payers' Personal Data);

4.4. The Bank processes biometric data in the process of unique video identification and photoidentification of the Data Subject via the mobile application in accordance with the legal acts. The Bank does not have the access to the biometric data stored in the mobile device of the Data Subject and the Bank does not process such data types.

4.5. The Bank might process the Personal Data of any other category of the Data Subject not stated in the Policy and categories of the Personal Data not specified herein, if the Processing takes place in accordance with the legal grounds of Processing and legit purposes hereto complying with provisions of the Data Regulations.

5. Legal Grounds for Processing

The Bank processes Personal Data in accordance with the legal grounds of Processing as set forth in the Data Regulation:

- **Conclusion and Performance of Contract with Data Subject**
  The Bank processes Personal Data to draft and execute a contract before it is signed, as well as throughout the term of the contract in force to ensure fulfilment of contractual obligations. This legal basis also applies when the Bank discloses the Personal Data to the Third Parties, such as international payment card organizations (VISA, MasterCard) and correspondent banks to execute relevant client's transactions based on the contract;
- **Compliance with the Legal Obligations**
  The Bank processes Personal Data in accordance with its obligations stipulated by the regulatory acts. For example, the Bank has or may have the following obligations: client identification, client due diligence, providing information to the client about changes in the service terms and Bank's tariffs, providing information about the client and the credit granted to them in accordance with the Law on Credit Register, risk monitoring, or providing information in response to requests from the state institutions, officials, and other Third Party requests as stated in the Credit Institution Law, as well as to provide the information in order to ensure compliance of the Group's activities with the regulatory acts, and in other scenarios;
- **For performance of a task carried out in the public interest,**
  the Bank conducts client due diligence in accordance with the requirements of the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing, sanctions risk management in compliance with the regulatory acts, and provides client identification and due diligence information to other credit institutions and financial institutions;

- **Legitimate interests of the Bank**: for example, the Bank ensures Processing for evaluation of the creditworthiness of borrowers and credit risk management, to the extent that the Processing extends beyond the fulfilment of a legal obligation for the Bank; the Bank is entitled to provide information to credit information bureaus, conduct contract performance monitoring and measures for prevention of various types of frauds, provide payment initiation services, as well as ensure video surveillance for property safeguarding and security purposes, phone call recording to keep evidences for the protection of its interests and service quality improvement, and in all cases to bring a claim to the court for of its affected interests;
- **Data Subject's consent** is collected to allow the Bank to send its clients commercial notifications, as well as carry on the chosen cookie Processing (marketing, statistics). The consent is freely given by the Data Subject and does not relate to the risk of not obtaining the Bank's service or creating some other kind of negative consequences (whereas not obtaining bonuses and loyalty is not considered as the negative consequences. Before collecting the consent, the Banka provides the Data Subject with information about the processed Personal Data categories and purposes hereto and further explains the Data subject how the given consent can be revoked. Upon the consent revocation, the Bank stops the Processing for the purposes for which the revoked consent was initially provided. At the same time, the Bank is entitled to process the Personal Data for other purposes based on another legal grounds, for example, in order to maintain the evidences about the legitimacy of the Data Subject consent which makes up a separate legitimate interest of the Bank to protect the Bank's interests in case of any disputes.

When processing the Personal Data, the Bank can make automated individual decisions, which might also include the profiling (i.e., using Personal Data to evaluate specific personal aspects related to the Data Subject, especially concerning their financial status, transactions, personal preferences, interests, behavior, location, etc.), if it is necessary for the conclusion and performance of a contract with the Data Subject or based on the Data Subject's consent, or the processing of Personal data is required by regulatory enactments. The Bank uses automated Processing solutions for certain processes related to risk management and client due diligence for the purpose of anti-money laundering and terrorism financing prevention; however, an employee of the Bank always takes part in making a decision regarding the Data Subject.

6. Data Subject Rights

6.1. Data Subject has the following rights in respect to Processing of their Personal Data:

- **to receive information** whether or not the Bank processes the Personal Data of the Data Subject, and in case the Bank does, the Data Subject is entitled to access their Personal Data and receive information about the processed categories of the Personal Data, purposes of their Processing, types of recipients and providers of the Personal Data, the Personal Data retention period, as well as information on the possibilities of the Data Subject to request the rectification, erasure, or restriction of the Processing of Personal Data, the right to object to the Processing, the right to lodge a complaint with the DSI, to receive information on automated decision-making, including profiling;
- **request the rectification of his or her Personal Data**, in case the Personal Data is inaccurate or incorrect;
- **withdraw the previously given consent** for the Processing;
- **object to the Processing of their Personal Data**, whereas the legal basis of the Processing is the Bank's legitimate interests or the performance of a task in the public

interest, if the Data Subject duly specifies their specific reasons based on which such Processing operations should be interrupted;

- **request the erasure of their Personal Data**, if the Data Subject has withdrawn consent to the Processing, the Personal Data is no longer necessary for the initial purposes, or the Personal data were processed unlawfully;
- **restrict the Processing of their Personal Data** if the Data Subject disputes the accuracy of the Personal Data (for a period during which the Bank verifies the accuracy of Personal Data), the Processing is no longer necessary for the Bank and yet the Data Subject needs the information hereto to raise, exercise or defend legal claims, or the Processing is illegal, but the Data Subject requests the restriction of the Processing rather than erasure of the Personal Data; the Data Subject has objected against the Processing carried out in the legitimate interests of the Bank or **for performing a task** in the public interest (for the period while the Bank performs the assessment of the rights of the Data Sand the legal grounds indicated by the Bank);
- **request the portability of their Personal data** in respect to the Personal Data personally submitted by the Data Subject based on the consent, or for the purpose of concluding and performing a contract, for example, by filling in the Bank's forms, applying for the Bank's products and services, taking into account that this is possible only for the Personal Data, the Processing of which is carried out by the automated means;
- **lodge a complaint**. The Data Subject is entitled to submit a respective claim to the DSI, the address: Elijas iela 17, Riga, LV1050, e-mail: pasts@dvi.gov.lv, phone number +371 67 22 31 31.

6.2. The Data Subject rights specified herein are not absolute, and there may be certain restrictions on the exercise of these rights and disclosure of information laid down in the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing, the Credit Institution Law and other regulatory acts. When providing a response to the Data Subject request, the Bank, where needed, indicates the existence of such restrictions.

6.3. The Data Subject must submit the requests in a written form to the Bank in one of the following ways:

1) in person at the Customer Service Centre at Brivibas iela 54, Riga, also presenting identity document (passport or identity card);
2) by sending a message via the Bank's internet bank;
3) by sending an e-mail signed with a secure electronic signature to the datuaizsardziba@magnetiqbank.com.

6.4. The Bank examines the Data Subject's request and provides the respective reply within one month from the date of receipt of the corresponding Data Subject request. The Bank has the right to extend the one-month period by two further months, taking into account the complexity and the number of the Data Subject requests.

6.5. The Bank provides the answer to the Data Subject, as well as performs any other activities exercise the Data Subject rights (for example, correction and rectification of the Personal Data), free of charge, except those cases when the Data Subject request is apparently ungrounded, excessive or incompatible with the Bank's resources, i.e., as a result of exercise of the Data Subject request or its conditions, the Bank's operations or

other Data subjects' rights are endangered. If the Data Subject request (request) does not comply with adequate Data Subject's care about the lawfulness of the processing of the Personal Data, the Bank is entitled to request the charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested or refuse from its execution

6.6. In cases where the Data Subject request is not submitted in Latvian, Russian or English, the Bank is entitled to apply a reasonable fee to cover the translation costs of the Data Subject request, or to refuse to fulfill the Data Subject request.

7. Personal Data Recipients

7.1. The Bank transfers the Personal Data to the Third Parties only to the extent and in scenarios stipulated in the regulatory acts of the European Union and the Republic of Latvia, in most cases that happens for the performance of a contract with the Data Subject or to ensure the provision of high-quality and efficient services to the Data Subject, or in order to fulfil legal obligations or to protect the legal rights and interests of the Bank or other legitimate interests hereto.

7.2. The Bank mostly transfers the Personal Data to the following Third Parties:

- Group enterprises, if the transfer of the Personal Data is based on the compliant Processing purposes and legal grounds, as well as:
  - Personal Data is protected with sufficient technical and organizational means;
  - Data Subject is informed about the recipient of the Personal Data, if a regulatory act does not stipulate otherwise.
- members of the European and international payments systems and the related parties hereto;
- other credit institutions and financial institutions, financial service intermediaries, and the Third Parties involved in the execution of payments and reporting;
- the Bank's auditors, legal and financial consultants;
- courts, sworn bailiffs, sworn notaries, insolvency administrators, State and Municipal Police, the Bank of Latvia, the State Revenue Service, Prosecutor General Office, Financial Intelligence Unit, etc.;
- private and legal persons who warrant for the due implementation of the customer's obligations, for example, warrantors, guarantors, or collateral pledgers;
- those parties that maintain registers, from whom the Bank receives or provides information about the Data Subject (for example, the Credit Register of the Bank of Latvia, the Account Register, commercial registers, registers which receive data about the transactions with financial instruments, etc.);
- Third Parties related to the provision of Bank services, for example, postal services, information technology and telecommunication service providers, and couriers.

The Processors receive the Personal Data in accordance with conditions of an agreement signed between the Bank and a particular Processor, whereas types of the processed Personal Data, their volume, the methods and security requirements in respect to protection of the Personal Data, etc.

The Bank ensures that the Processing is carried out by the authorized employees who need the access to the Personal Data in scope of their official duties, and who complies with the Processing principles, purposes and legal grounds of the Processing stated in this Policy.

8. Personal Data Transfer Outside the European Union/European Economic Area

8.1. The Bank mostly processes the Personal Data within the European Union or the European Economic Area (EU/EEA), and there may be cases when the Personal Data of the Data Subject is transferred outside the EU/EEA.

8.2. Before actually transferring the Personal Data to a recipient in a country that is located outside the EU/EEA, the Bank verifies in advance whether the level of the Personal Data protection within the meaning of the Data Regulation has been acknowledged adequate in the particular country, and whether it is possible to ensure the safeguards that comply with requirements of the Data Regulation

8.3. If the pre-conditions stated in the Clause 8.2 above are not met, the Bank transfers the Personal Data of the Data Subject for Processing outside the EU/EEA only in case sufficient security measures are taken in accordance with requirements of the legal acts and if any of the conditions below is observed:

- the transfer of the Personal Data is necessary to conclude or fulfill the service agreement with the Data Subject, or for the conclusion and performance of a contract between the Bank and a Third Party in the interests of the Data Subject;
- Data Subject provides consent for the Processing outside EU/EEA;
- Transfer of the Personal Data is necessary for the protection of vital interests of the Data Subject or other persons, if the Data Subject is not able to provide the consent for such Processing physically or legally;
- The transfer of the Personal Data is necessary for the Bank to comply with the regulatory acts' requirements or in order to pursue its legal claims, for example, to raise a claim via the court.

9. Personal Data Storage Period

9.1. The Bank defines and regularly reviews the Personal Data storage period, thus ensuring that it is processed as long as it is necessary to achieve the respective Processing purpose.

9.2. The Personal Data storage period may be dependent on the term of the contract or business relations, requirements of regulatory acts, the Bank's legitimate interests or the moment when the Data Subject withdraws their consent. When the Personal Data retention period finalizes, the Bank deletes or anonymizes the Personal Data, as a result of which the Data Subject can no longer be identified by the Bank.

10. Data Protection Officer

10.1. The Bank has appointed the Data Protection Officer, who:

- oversees the compliance of Processing operations with the Processing principles stipulated by the Data Regulation and other regulatory acts;
- ensures measures required for implementation of the Data Regulation within the Bank;
- informs and consults the Bank's employees in relation to their duties resulting from the Data Regulation;
- supports the process of conducting the data protection impact assessment (DPIA) and oversees its implementation;
- ensures cooperation with DSI;

- manages the records of processing activities;
- maintains records of Personal Data breaches.

10.2. Contact information of the Data Protection Officer: datuaizsardziba@magnetiqbank.com, or, please, reach out to the Data Protection Officer via post by the address Brivibas iela 54, Riga, LV-1011, marking the letter with a following notice – to the Data Protection officer of Magnetiq Bank.

11. Informing the Data Subjects on Changes

The Bank regularly reviews and updates the Policy in accordance with changes in the Bank's Processing operations and amendments to the regulatory acts.

The latest version of the Policy is published on the Bank’s website, and any update of the Policy enters into force upon its publishing on the Bank’s website magnetiqbank.com.