Privacy Policy

Table of Contents

I Terms Used

1. The following terms and abbreviations are used in this document:
   1.1. **Bank** - Signet Bank AS;
   1.2. **Data subject (also- individual)** – an identified or identifiable natural person, including a client, employee, visitor ad others;
   1.3. **Data State Inspectorate** - a supervisory authority for the processing of personal data within the meaning of the General Data Protection Regulation (GDPR[1]);
   1.4. **Controller** – the personal data controller Signet Bank AS or, where applicable, another Group company. The Controller's contact information is available in the 'Contacts' section of the website and in Section 9 of this Policy;
   1.5. **Group** - (for the purposes of this Policy) – the legal entities forming part of the Signet Bank AS Group to which this Policy is directly applicable: Signet Asset Management Latvia IPS, SIA Citra Development, and SIA AgroCredit;
   1.6. **Holder of information resources** – an employee of the Controller who, within the scope ot their competence, is responsible for the processing of personal data in accordance with the relevant purpose of data processing in the Controller's unit, determines the data security requirements of Persona and approves or rejects the access rights of employees of other structural units of the Controller;
   1.7. **Cyber hygiene** – a method, measure, or a set of measures aimed at mitigating personal data processing risks in information systems; a set of daily practices and habits intended to reduce cyber threats, ensure data protection, and maintain the availability, integrity, and confidentiality of information and communication technology resources;

[1] 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).

1.8. **Personal data** (for the purposes of this Procedure – data of a natural person) – any information processed by the Bank that relates to an identified or identifiable natural person, who can be directly or indirectly identified by reference to information about them, their specific characteristics, or other identifiers.

1.9. **Personal data breach** – a personal data breach (threat) resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, as well as a breach of the principle of data processing laid down in Article 5 of the GDPR.

1.10. **Processing of personal data** - any operation or set of operations performed on personal data which is performed by automated means or forms part of a filing system, where the processing of the data is not carried out by automated means.

1.11. **Security of personal data** – confidentiality of personal data (processing of personal data in a way that ensures access to these data only to the Controller's employees with appropriate powers), integrity (possibility to ensure the preservation of personal data in an unchanged form, regardless of processing methods) and availability (for an authorized person – the possibility for an employee of the Controller to access data at a specific time and place for the performance of a specific task).

1.12. **Policy** –internal regulatory document 'Privacy Policy'.

II Objective

2. The purpose of this Policy is to ensure such processing of Personal Data and such a technological environment for this processing that the information containing Personal Data, processed for the core activities of the 'Bank' and Group companies and for the implementation of tasks related to these core activities, as well as the technological resources where the information and data are processed, are protected against external and internal threats, while at the same time ensuring the rights and freedoms of Data Subjects.

3. The objective of the Group is to ensure a unified framework for Personal Data management. At the same time, the Group includes the legal entities listed in Clause 1.5 of this Policy, to which the principles of this Policy apply, as well as such legal entities as AS Primero Finance and AS Magnetiq Bank, which have a broad client base and specific operational directions differing from those of the Bank; therefore, they have established Privacy Policies equivalent to this Policy and compliant with the Data Regulation.

III General information

4. This Policy provides information on the purposes (objectives) of personal data processing carried out by the 'Bank' and the Group companies as Controllers, as well as on the measures implemented to ensure compliance with the requirements of the Data Regulation, including adherence to Cyber Hygiene practices and the exercise of Data

Subjects' rights.

5. The Bank considers the fair and lawful processing of personal data, the implementation of adequate and comprehensive personal data protection measures, and the respect for Data Subjects' rights to be essential throughout all stages of the core and supporting processes of the Bank and the Group companies.
6. Information on personal data processing is available in the 'Personal Data Processing' section of the website. For each personal data processing purpose (objective), in accordance with Annex 1 'Data Processing Form', additional relevant information is provided. Depending on the type of service used with the Bank or a Group company, such information may also be included in the contract and related documents.
7. The Data Processing Form, after its completion and approval by the Management Board, shall be published on the Bank's website in an easily accessible format. It may be supplemented or amended as necessary, independently of the Policy review. Following the approval of such amendments by the Management Board of the Bank or a Group company, the updated information reflected in the Data Processing Form shall be published.
8. Information about the cookies used on the website and the basic conditions for their use is available in the 'Personal Data Processing' section of the website under 'Cookie Notice' (Annex 2 'Use of Cookies'). The cookie information must be updated in accordance with any actual changes.
9. **Contact details of the controller:**
    - 9.1. Signet Bank AS
      address: 3 Antonijas Street, Riga, LV 1010, Latvia
      e-mail: *info@signetbank.com;*
    - 9.2. Signet Asset Management Latvia IPS
      address: 3 – 1 Antonijas Street, Riga, LV 1010, Latvia
      e-mail: *info@signetam.com;*
    - 9.3. Citra Development SIA
      address: 3 – 1 Antonijas Street, Riga, LV 1010, Latvia
      e-mail: *info@signetbank.com;*
    - 9.4. AgroCredit SIA
      address: 6 Ziedleju Street, Marupe, LV 2167, Latvia
      e-mail: *birojs@agrocredit.lv.*

IV Fundamental principles of the Privacy Policy

10. The Policy has been developed in accordance with the GDPR, the Personal Data Processing Law, the Credit Institution Law and other binding regulatory enactments in force in the Republic of Latvia, in accordance with the products and services offered by the Bank and Group companies.
11. The Bank and the Group have established an internal control system that includes the regular review and updating of internal regulatory documents, adherence to Cyber Hygiene as an essential element of Personal data protection, improvement of technological safeguards and processes, and the organization of staff training in the areas of Personal data processing, protection and cybersecurity at least once a year. In

their interrelation, these areas form a consistent security culture, ensure the protection of Personal data, and support the implementation of the objectives of this Policy.

12. The Bank and the Group process Personal data only when the intended purpose cannot be adequately achieved by other means, and only to the extent necessary for the achievement of that purpose. Personal data are not used for other tasks unrelated to the original purpose.
13. The Bank and the Group primarily process Personal data in order to provide services in line with their business activities, to conclude and perform contracts, and to deliver services to clients, including responsible lending, investment services, and/or day-to-day financial services. Personal data are also processed to fulfil legal obligations as defined by applicable laws, to serve public interests, and to ensure the implementation of core business support processes.
14. Bank and each Group company ensure that the costs of technical, technological and organizational measures implemented are proportionate to the potential losses, that could result from a personal data protection breach, including cases of non-compliance with Cyber Hygiene (compromising the confidentiality, integrity, or availability of information resources).
15. The Group promotes employee awareness of each staff member's duties and responsibilities in ensuring Personal data protection, including by performing appropriate control and follow-up measures and providing regular training activities. The Bank and the Group also educate employees in the field of Cyber Hygiene.
16. In the event of a Personal data protection breach, the Bank or a Group company conducts a comprehensive investigation, preserves evidence, and undertakes measures to eliminate or mitigate the consequences. In cases defined by the Data Regulation, the Data State Inspectorate and the Data Subject are notified. The Group companies cooperate and provide mutual assistance to promptly identify risks, mitigate potential consequences, or prevent threats.
17. This Policy and any amendments thereto are endorsed by the Management Board and approved by the Supervisory Board of the Bank.

V Classification of Personal Data

18. The purpose of Personal data classification is to identify the significance of the Personal data processed by the Bank in order to ensure that the applied physical and logical protection measures correspond to the value of the protected Personal data.
19. Personal data are classified depending on the potential harm that may be caused to the Data Subject's rights to Personal data protection and freedoms if the confidentiality, integrity, or availability of information, including Personal Data, is not ensured.
20. High-risk Personal data are those Personal data which, in the event of a Personal data protection breach, may cause the Data Subject material or non-material harm (for example, loss of control over their personal data, identity theft, or reputational damage), as well as special category personal data. Such data are subject to enhanced protection measures within the Group.
21. High-risk Personal data processing refers to large-scale processing of Personal data,

including processing involving monitoring or evaluation of individuals, as well as the use of new or innovative technological solutions in Personal data processing. For example, in the case of profiling—if the Bank or a Group company decides to use it for service provision—it carefully assesses the potential impact on the rights of the Data Subject.

VI Management of Personal Data Security

22. The Bank's internal regulatory documents in the areas of Personal data processing, protection, and Cyber Hygiene establish the following measures:
    - 22.1. Information system control measures, including access to Personal data granted only to identified and authorized employees; differentiation of information users; and procedures for granting, reviewing, and revoking user rights within information systems;
    - 22.2. regular employee training, including on the fundamental principles of Personal data processing, procedures for accessing Personal data, adherence to the 'clean desk policy' and the rules for using information systems and technological tools;
    - 22.3. ensuring the full functionality of information systems, maintaining appropriate configurations and technological security solutions to reduce or prevent unauthorized access to the resources of the Bank or Group companies;
    - 22.4. encryption and other protection tools used in information systems, data pseudonymization, and procedures for reviewing these processes to ensure the security and adequate protection of Personal data throughout their processing ('life cycle');
    - 22.5. change management procedures for information systems, ensuring that only fully tested, evaluated, and approved changes are implemented in the production environment;
    - 22.6. management of Personal data protection breaches and information and communication technology security incidents to minimize their impact on each individual Data Subject, Personal data processing, and the core business processes of the Bank and the Group, as well as to prevent or reduce the likelihood of such cases recurring.
23. The Bank and the Group use each assessment of the impact on data protection for implemented personal data processing activities as a constructive risk analysis tool to determine the compliance of existing or planned personal data processing with the General Data Protection Regulation and other applicable legal acts related to personal data processing and protection in the financial and credit sector. A comprehensive assessment of personal data processing makes it possible to identify threats, the likelihood of their occurrence, and the potential impact of such threats on the Data Subject's right to data protection.
24. The risk management measures and tools for Personal data processing governance and the technologies used in such processing are defined by the Management Board of the Bank and each Group company in their respective decisions.
25. Data protection impact assessments in areas involving high-risk Personal data

processing are carried out in accordance with Article 35 of the General Data Protection Regulation and the Bank's internal regulatory document 'Personal Data Processing and Protection Procedure'. The results of these assessments are used to plan or determine protective and risk-mitigating measures, as well as specific tasks and deadlines for their implementation.

26. To ensure the continuity and recovery of information system operations in the event of incidents, the Bank has established a 'Business Continuity Plan' and developed internal regulatory documents defining the procedures for restoring or replacing information systems and technological resources. The information systems, technological components, and personnel of the Bank and Group companies are regularly trained to ensure uninterrupted service delivery and to maintain a high level of information and Personal data protection.
27. To ensure and restore the continuity of information system operations, the Bank performs regular Personal data backups, ensures that backup copies are stored in a different geographical location and conducts verification checks to confirm the operability of the restored information systems and the integrity of the data.
28. When the Bank or the Group introduces new information systems, technological tools, or develops new products, integrated Personal data protection and data protection by design and by default principles are applied throughout these processes.

VII Rights of the Data Subject

29. Data Subject has the following rights in relation to Personal data processed by the Bank:
    - 29.1. request and receive information from the Bank or a Group company, acting as an individual Controller, regarding the processing of Personal data and, where necessary, request access to such data;
    - 29.2. submit a request to rectify Personal data if such data are inappropriate, incorrect or inaccurate;
    - 29.3. request restriction of data processing in order to ensure the accuracy of Personal Data or in other cases specified in the General Data Protection Regulation (GDPR) that concern the relationship between the Controller and the Data Subject;
    - 29.4. withdraw previously given consent for processing of their Personal data and request the deletion of the relevant Personal data (unless another lawful basis for such processing exists); the withdrawal of consent does not affect the processing carried out prior to the withdrawal;
    - 29.5. object to the Processing of Personal data for marketing purposes;
    - 29.6. receive Personal data provided by the Data Subject based on consent or required for the performance of a contract concluded with the Data Subject in a structured, commonly used electronic format and if technically feasible and legally permissible, request the transfer of such data to another entity, thereby ensuring data portability.
30. In order to exercise his or her rights, the Data Subject may prepare and submit a request in a form that allows the Controller to identify the particular Data Subject, using internet

banking options, by submitting a request signed with a secure electronic signature, or by submitting such a request in person to the customer service representatives of the Bank or a Group company.

31. It is desirable to indicate in the request of the Data Subject the exact time period and information about Personal data that the Data Subject wishes to receive, as well as the grounds for such request. The abovementioned information shall allow the Controller to prepare a more accurate reply within a shorter period of time.
32. A reply to the Data Subject's request shall be provided without undue delay, but not later than within one month. If necessary, the Bank or Group company may ask the Data Subject to submit additional information, as well as extend the deadline for providing a response by another two months, taking in to account the complexity of the request or the number of similar requests.
33. The right to the Protection of Personal Data is not absolute and, in the cases specified in regulatory enactments, as well as in certain situations it may be limited, including in order not to affect the rights and freedoms of other persons, to ensure the protection of commercial secrets and intellectual property. At the same time this means that the Bank shall provide the Data Subject only with the information that is not prohibited by regulatory enactments and which can actually or by making an asessment of the proportionality of the rights.
34. In matters related to the processing and protection of Personal data, the Data Subject may contact the Bank's Data Protection Officer including questions about Personal data processing within the Group, by sending an e-mail message or an electronically signed letter to the address: *datuaizsardziba@signetbank.com.*

VIII Final Provisions

35. In order to ensure the topicality and consistency of this Policy, taking in to account changes in the activities of the Bank or Group, as well as changes in external regulatory enactments, the Bank shall review it at least once a year.
36. Bank shall ensure the publication of the current Privacy Policy on its website.
37. The Bank and the Group highly value confidentiality and the protection of each Data Subject’s rights and are committed to finding constructive solutions in cases of disagreement. However, if the Data Subject has significant complaints, they may submit an application to the Data State Inspectorate:

    37.1. by e-mail: *pasts@dvi.gov.lv;*

    37.2. or by sending a letter to the address: 17 Elijas street, Riga, LV-1050.