Privacy Policy

SIGNET BANK

Table of Contents

I Terms Used

1. **Data subject** – an identified or identifiable natural person.
2. **Data State Inspectorate** - a supervisory authority for the processing of personal data within the meaning of the GDPR[1].
3. **Controller** – Signet Bank AS.
4. **Holder of information resources** – an employee of the Controller who, according to his or her 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.
5. **Control of information systems** – a method, measure or a set thereof for reducing the risks of processing personal data in information systems.
6. **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.
7. **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.
8. **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).
9. **Policy** – the Bank's internal regulatory document „Privacy Policy".

[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).

II General informations

10. The Policy provides information on the purposes (purposes) of the processing of personal data carried out by Signet Bank AS (hereinafter – the Bank) as a data controller, the measures implemented to ensure the requirements of the GDPR, including the implementation of the rights of data subjects.
11. Fair and lawful processing of personal data, ensuring appropriate personal data protection measures and respecting the rights of data subjects are important for the Bank.
12. Information on the processing of personal data can be found at each purpose of personal data processing (Annex 1, „Data processing form"), as well as additional information, depending on the type of banking service used, may be included in contracts and related documents. The Annex to the Privacy Policy also contains the basic conditions for the use of cookies (Annex 2, „Use of Cookies").
13. Contact details of the controller:

    Signet Bank AS
    address: 3 Antonijas Street, Riga, LV 1010, Latvia
    phone: +371 67 080 000
    e-mail: *info@signetbank.com*

III The Basic Purpose of the Policy and Implementation

14. 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.
15. The purpose of the Policy is to provide such processing of Personal Data and technological environment of personal data processing so that the information at the disposal of the Bank, including personal data, and technological resources are protected from external and internal security risks, and at the same time ensure the rights and freedoms of Data Subjects, as well as comply with the implementation of the objectives and tasks of the Bank.
16. The Bank has established an internal control system and regularly reviews a set of internal procedures, including in the field of Personal Data Security, thus ensuring the achievement of the basic purpose of the Policy.
17. The costs of the technical, technological and organisational measures to be implemented shall be commensurate with the possible losses that may be incurred in the event of an event of security risk of the information system used for the processing of personal data (if the confidentiality, integrity or availability of information resources is endangered).
18. The Bank ensures that the staff understands the duties of each employee in ensuring the security of personal data, including performs appropriate controls, follow-up of the performance of tasks and ensures regular training measures.
19. Upon establishing a Personal Data Breach, the Bank shall conduct a comprehensive investigation of the event, preservation of evidence and prevention or mitigation of the

consequences of the incident, as well as in the cases specified in the GDPR informing the Data State Inspectorate and the Data Subject.

20. The Policy, as well as amendments thereto, are accepted by the Bank's Board of Governors and approved by the Bank's Council.
21. The Policy enters into force at the moment of its approval and with its approval, the Bank's internal regulatory document „Privacy Policy" approved on 21.02.2023 expires.
22. The Policy is binding upon all employees of the Bank.

IV Classification of Personal Data

23. The purpose of classification of personal data is to identify the significance of the personal data processed by the Bank so that the protection measures applicable to them are in accordance with the value of the protected personal data.
24. Personal data are classified according to the damage that may be caused to the Data Subject's right to the protection and freedoms of his or her personal data, if confidentiality, integrity and availability are not ensured.
25. High-risk personal data is such personal data which, in the event of a personal data breach, may cause material or non-material damage to the Data Subject (for example, loss of control over his or her personal data, identity theft, reputational damage), as well as special categories of personal data and personal data related to breaches.
26. The processing of large scale personal data is the processing of high-risk personal data, including surveillance related to surveillance, and the use of new technologies or software for the processing of personal data.

V Manage the Protection of Personal Data

27. The Bank's internal regulatory documents in the field of processing of personal data and protection and the use and security of information systems lay down the following measures:
    - 27.1. Control measures for information systems, including access to personal data only for identified and authorized employees; the procedures for granting, inventorying and cancelling the rights of users of information systems; the procedures for granting the rights of the user of information systems, taking in to account the necessity of the amount of information for work duties;
    - 27.2. training of employees on the basic principles of data processing, the procedure for access to personal data and the conditions for the use of information systems;
    - 27.3. of information systems, configurations and technological solutions to reduce and prevent access of unauthorized persons to the Bank's resources;
    - 27.4. encryption and other appropriate means of protection to be used in information systems, pseudonymisation of data and procedures for reviewing the aforementioned processes in order to ensure the security and adequate protection of Personal Data throughout the entire period of their processing;
    - 27.5. for changes in information systems, introducing only tested, evaluated and accepted changes in the production;
    - 27.6. Management of Personal Data Breaches and information system security incidents in order to reduce their impact on the processing and protection of

Personal Data and the Bank's processes in general, as well as the risk of their recurrence.

28. Assesment of inpact on data protection is, inter alia, a risk analysis tool to determine the compliance of existing or planned Personal Data processing with the GDPR and other binding laws and regulations in the field of personal data protection, to identify the probability of the threat materialising and the impact of such threat on the Data Subject's right to data protection.
29. The risk management measures and technologies to be used in the Processing of personal data and the technologies to be used in the Processing of personal data shall be determined by the Board of the Bank, including by determining the holders of information resources and appointing the Information Systems Security Manager.
30. An assessment of the impact on data protection in the areas of processing of high-risk personal data shall be carried out at least once every two years and the results there of shall be used in the planning or determination of safeguards and risk mitigation measures, as well as specific tasks and deadlines for their fulfilment.
31. In order to ensure the continuity of the operation of information systems and their restoration in the event of incidents, the Bank has established a „Business Continuity Assurance Plan" and established procedures for the renewal of information systems.
32. In order to ensure the continuity of the operation of information systems and to restore it, the Bank shall perform regular backup copies of the personal data of the information system, ensuring storage of the backup copy in another geographical location, as well as ensure the verification of the updating of the information system in order to obtain assurance of the operability of the updated information system and data integrity.

V Rights of the Data Subject

33. Data Subject has the following rights in relation to the personal data processed by the Bank:
    - 33.1. to receive information whether the Bank processes the personal data of the Data Subject, and in the affirmative case in accordance with the Data Subject's request, to provide access to them;
    - 33.2. to rectify personal data if such data are inappropriate, incorrect or inaccurate;
    - 33.3. to request restriction of data processing in order to ensure the accuracy of personal data or in other cases specified in the GDPR, which affect the relationship between the Controller and the Data Subject;
    - 33.4. to withdraw the previously given consent of the Data Subject to the Processing of his or her Personal Data and to request the erasure of the relevant personal data (unless there is another legal basis for the processing of this personal data);
    - 33.5. to object to the Processing of Personal Data for marketing purposes;
    - 33.6. to receive personal data provided by the Data Subject on the basis of consent or necessary for the performance of a contract concluded with the Data Subject and used in a structured manner, in a commonly used electronic format; as well as, if it is technically possible, to request the transfer of such data to another merchant, thus ensuring the portability of personal data.

34. In order to exercise his or her rights, the Data Subject may prepare and submit a request in a way that allows the Controller to identify the particular Data Subject using internet banking options, submitting a request signed with a secure electronic signature or submitting such a request in person to the Bank's employees.
35. It is desirable to indicate in the request of the Data Subject the exact time period and information about the 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.
36. 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 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 such requests.
37. 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. 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.
38. In matters related to the processing and protection of Personal Data, the Data Subject may contact the Bank's Data Protection Officer by sending an e-mail message or an electronically signed letter to the address: *datuaizsardziba@signetbank.com.*

VI Final Provisions

39. In order to ensure the topicality and consistency of this Policy, taking in to account changes in the activities of the Bank or changes in external regulatory enactments, the Bank shall review it at least once a year.
40. Bank shall ensure the publication of the current Privacy Policy on its website.
41. In case of significant claims or disagreements, the Data Subject may submit a complaint to the Data State Inspectorate by e-mail: *pasts@dvi.gov.lv* or by sending a letter to the address: Elijas iela 17, Riga, LV-1050. The Bank shall ensure the publication of the current Privacy Policy on its website.

VIII Attachments

N. p. k.	Nosaukums
1.	Data processing form
2.	Use of cookies

* * * * *