APPROVED
by Order No V 2018/(1.7.E-260603)-02-113 of the Chairman of the Board of the Bank of Lithuania
of 20 July 2018
(as amended by Order No V 2019/(28.23.E-2800)-98-46 of the Chairman of the Board of the Bank of Lithuania
of 6 August 2019)

GENERAL PERSONAL DATA PROCESSING REGULATIONS OF THE BANK OF LITHUANIA

CHAPTER I
GENERAL PROVISIONS

1. The General Personal Data Processing Regulations of the Bank of Lithuania (hereinafter – Regulations) shall establish the principles of personal data processing, personal data processing, requirements for organisational and technical personal data processing and security means and measures, implementation of the rights of data subjects, and investigation of personal privacy breaches at the Bank of Lithuania (hereinafter – Lietuvos Bankas (LB)).

2. The Regulations were drawn up in accordance with the 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) (hereinafter – Regulation) (OJ 2016 L 119, p. 1), the Republic of Lithuania Law on Legal Protection of Personal Data, and other legal acts regulating the processing and protection of personal data.

3. The controller of personal data processed by LB shall be LB.

4. Personal data shall be processed only for clearly defined purposes, which are necessary in carrying out the functions and activities of the Bank of Lithuania, or where established so in the legal acts.

5. The owner of personal data shall be the structural unit of LB collecting and processing personal data for the defined purpose(s).

6. The owner of personal data shall be responsible for the compliance of personal data processing with the provisions of these Regulations, the General Data Protection Regulation and other legal acts regulating personal data processing.

CHAPTER II
DEFINITIONS AND ABBREVIATIONS

7. **Personal data** shall mean any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, for example, a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

8. **Personal data processing** shall mean any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, for example, collection, recording, sorting, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination with other data, restriction, erasure, or destruction.

9. **DPO shall** mean a data protection officer of LB.

10. **Information system** shall mean the whole of means designed for the creation and transmission of information, composed of an information processing system and

organizational resources (people, technical means, funds, etc.) required for the whole operation.

11. **Inspectorate** – State Data Protection Inspectorate.

12. Other definitions used in the Regulations shall have the meanings provided for in the Regulation, the Republic of Lithuania Law on Legal Protection of Personal Data, Regulations for Information Security of the Bank of Lithuania approved by Order No V 2018/(1.7.E-260603)-02-8 of the Chairman of the Board of the Bank of Lithuania on the approval of the regulations for information security of the Bank of Lithuania of 16 January 2018, and other legal acts regulating personal data protection.

CHAPTER III
PRINCIPLES OF PERSONAL DATA PROCESSING

13. Personal data shall be processed in accordance with the following principles of personal data processing established in Article 5 of the Regulation:

13.1. **principle of lawfulness, fairness, and transparency** means that personal data in relation to data subject shall be processed lawfully, fairly, and in a transparent manner;

13.2. **principle of purpose limitation** means that personal data shall be collected for specified, explicitly defined, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 Paragraph 1 of the Regulation, not be considered as incompatible with the initial purposes;

13.3. **principle of personal data minimisation** means that personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;

13.4. **principle of accuracy** means that personal data being processed shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

13.5. **principle of storage limitation** means that personal data being processed shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 Paragraph 1 of the Regulation subject to implementation of the appropriate technical and organisational means and measures required by this Regulation in order to safeguard the rights and freedoms of the data subject;

13.6. **principle of integrity and confidentiality** means that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational means and measures.

CHAPTER IV
DATA PROTECTION OFFICER OF THE BANK OF LITHUANIA

14. The function of DPO shall be carried out by an employee of LB. When appointing an employee to perform the functions of the DPO, their expert knowledge in data protection law and practice, professional qualities, and abilities to perform the functions assigned to the Data Protection Officer shall be taken into account.

15. LB shall ensure the guarantees in respect of DPO established in Article 38 of the Regulation.

16. LB shall inform the Inspectorate about the appointment of a DPO.

17. The purpose of a DPO is to assist in creating the processes that ensure the security of personal data at LB, to implement the appropriate measures, while enabling LB to observe the Regulation and other legal acts regulating the protection of personal data and privacy, and promote the data protection culture at LB.

18. The DPO shall carry the following functions:

18.1. notify the employees of LB of amendments of legal acts regulating personal data processing and protection, actual case law and best practice relating to personal data processing and protection, liabilities of employees while implementing provisions of legal acts;

18.2. consult the employees of LB and shall make recommendations regarding the improvement of implementation of provisions of legal acts relating to personal data protection and the improvement of processes;

18.3. provide data subjects with information regarding personal data processing and implementation of their rights by LB;

18.4. monitor the compliance of the provisions of legal acts in relation to the protection of personal data by LB, examine and inspect that the data processing activities are in line with the personal data and privacy protection requirements;

18.5. maintain records on personal data processing activities;

18.6. submit proposals to data owners regarding the elimination of personal data security breaches and assessment of impact on privacy of a person, and draw up reports on data protection breachs to the Inspectorate and data subjects;

18.7. arrange and carry out training and upskiling of LB employees involved in personal data processing operations;

18.8. consult the LB employees on data protection impact assessment and monitor the way it is carried out. In the course of the data protection impact assessment, shall provide recommendations so that the assessment is in compliance with the provisions of article 35 of the Regulation and provide his/her opinion on the conducted data protection impact assessment;

18.9. cooperate with the Inspectorate;

18.10. act as the contact point when the Inspectorate appeals to LB on issues relating to data processing: shall arrange the prior consultations referred to in Article 36 of the Regulation if data processing results in a high risk in the absence of measures taken by the controller to mitigate the risk, and shall consult the Inspectorate, where appropriate, with regard to any other matter relating to personal data processing and protection by LB;

18.11. carry out other functions laid down in the Regulation, the Regulations, and other legal acts regulating personal data processing and protection.

19. While carrying out the functions, the DPO shall be entitled to:

19.1. obtain from the employees of LB any information and documents necessary for performing the functions;

19.2. sign documents while submitting explanations for data subjects and applying to the Inspectorate for the consultation;

19.3. consult with the Inspectorate, information protection officer, other employees of LB and external experts;

19.4. use financial resources, infrastructure (providing of premises, means, equipment), where appropriate, after consultation with the managers, to involve other employees;

19.5. increase qualification and give time for deepening the latest knowledge relating to data protection.

20. The DPO shall be directly subordinated and shall report to the Director of the Security Department. The DPO shall notice the Director of the Security Department of the identified incompliances of data protection that may have a significant effect on personal privacy, human rights and freedoms which are incompatible with the Regulation and the consultancy of the DPO and directly inform the Chairman of the Board of the Bank of Lithuania of the incompliances found in the Security Department.

CHAPTER 5
PERSONAL DATA PROCESSING

21. Personal data processing shall be performed by LB in accordance with the Regulation, the Republic of Lithuania Law on Legal Protection of Personal Data, other legal acts, recommendations of the Inspectorate, Desription of Procedure for Personal Data Processing by the Bank of Lithuania approved by Order No V 2016/(1.7-260603)-02-186 of the Chairman of the Board of the Bank of Lithuania on the approval of the procedure for personal data processing by the Bank of Lithuania of 28 October 2016, and these Regulations.

22. Specific purposes of personal data processing shall be established in internal legal acts regulating the activities of LB structural units and published by DPO in the website of LB, under Personal Data Protection.

23. Personal data may be processed by LB via automated and not automated means.

24. The general requirements for the storage of personal data processed by LB in the official electronic documents shall be defined in the Rules for Management of Documents by the Bank of Lithuania in Unstructured Data Repository and Group Work System and Management of Electronic Documents approved by Order No V 2017/(1.7-260603)-02-29 of the Chairman of the Board of the Bank of Lithuania of 16 January 2017 on the approval of rules for management of documents by the Bank of Lithuania in unstructured data repository and group work system and management of electronic documents.

25. Personal data processed in electronic and paper document files, shall be stored within the time limit set in the Index of Terms for Storage of General Documents approved by Order No V-100 of the Chief Archivist of Lithuania of 9 March 2011 on the approval of the index of terms for storage of general documents, legal acts and the documentation plan of the Bank of Lithuania and shall be irreversibly destroyed in accordance with the procedure laid down in the Rules of Documentation and Record Keeping of the Bank of Lithuania approved by Order No V 2013/(1.7-260402)-02-228 of the Chairman of the Board of the Bank of Lithuania of 3 December 2013 on the approval of rules of documentation and record keeping of the Bank of Lithuania.

26. Consents (or their withdrawals) concerning the personal data processing shall be stored from the date of their receipt onwards and for 2 years after the expiry of the storage period for the personal data regarding which the consent to process had been given. The head of the structural unit may extend the storage period due to substantiated reasons.

27. Personal data in information systems may not be stored longer than the storage period established for the same data in documents and special legal acts regulating their processing (e.g. laws, rules). Upon expiry of the set data storage period, data should be anonimysation and irreversibly destroyed.

CHAPTER VI
PERSONAL DATA SECURITY

28. Considering the nature, scope, context and purposes of personal data processing as well as the probability of unauthorised processing and the potential consequences thereof to the rights and freedoms of natural persons, LB shall implement technical and organisational measures to ensure and be able to prove that personal data are processed by LB in compliance with the requirements of the Regulation, the Republic of Lithuania Law on Legal Protection of Personal Data and other legal acts regulating the protection of personal data and privacy.

29. The security of personal data processed by automated means shall be regulated by the Operational Security Policy of the Bank of Lithuania approved by Resolution No 03-100 of the Board of the Bank of Lithuania of 15 June 2015 on the approval of the operational security policy of the Bank of Lithuania, Information Security Regulations of the Bank of Lithuania, Information System Protection Policy of the Bank of Lithuania approved by the Resolution No 19 of the Board of the Bank of Lithuania of 20 March 2003 on the approval of the information system protection policy of the Bank of Lithuania, and other rules regulating the protection of information systems (hereinafter – IS).

30. Personal data protection measures are established in Annex 1 herein. The owner of personal data shall assess whether the implemented protection measures of personal data processed via automated means are in compliance with the measures specified in the List of Protection Measures of Personal Data Processed by Automated Means (see Annex 1). This assessment shall be carried out by the owner of personal data together with the Information Technology Department of the Organisation Service (OT ITD). The assessment of whether the implemented protection measures of personal data processed via automated means are in compliance with the measures specified in the List of Protection Measures of Personal Data Processed by Automated Means shall be performed before releasing for operation a newly acquired IS in which personal data will be processed, or after implementing major modifications in the IS. The assessment shall be also carried out according to the plan coordinated by the owner of the data with OT ITD when compliance with the data protection

requirements has not been assessed before or had been performed more than 5 years ago. The owner of the data shall inform the DPO by submitting the assessment performed and, where any non-concompliance has been established, the DPO shall be informed of the measures planned to be implemented to ensure compliance or to assume the risk.

31. The protection of information in databases of LB shall be established in the Rules for Protection of Databases of the Bank of Lithuania approved by Order No V 2018/(1.7.E-260603)-02-83 of the Chairman of the Board of the Bank of Lithuania of 29 May 2018 on the approval of rules for protection of databases of the Bank of Lithuania.

32. The management and the control of access to personal data shall be performed in accordance with the Rules for Identification and Access Management of the Bank of Lithuania approved by Order No V 2014/(1.7-260402)-02-257 of the Chairman of the Board of the Bank of Lithuania of 20 October 2014 on the approval of rules for identification and management of access of the Bank of Lithuania, the Rules for Access to Remote Information Resources of the Bank of Lithuania approved by Order No V 2013 /(1.7-260402)-02-54 of the Chairman of the Board of the Bank of Lithuania of 29 March 2013 on the approval of rules for access to remote information resources of the Bank of Lithuania and the Rules for Granting the Rights to Access the Information Resources in the Bank of Lithuania approved by Order No 02-125 of the Chairman of the Board of the Bank of Lithuania of 22 May 2002 on the approval of rules for granting the rights to access the information resources in the Bank of Lithuania.

33. The physical information security means and measures shall be established in the Description of Security Requirements for Unauthorised Access to the Premises of the Bank of Lithuania approved by Order No 01RN of the Chairman of the Board of the Bank of Lithuania of 30 March 2005 on the approval of security requirements for unauthorised access to the premises of the Bank of Lithuania, the Rules of Procedure of the Bank of Lithuania approved by Order No V 2017/(1.7-260603)-02-72 of the Chairman of the Board of the Bank of Lithuania of 2 March 2017 on the approval of the rules of procedure of the Bank of Lithuania and the Description of Procedure for the Movement of Visitors, Values, and Property in/out of the Bank of Lithuania approved by Order No V 2016/(1.7-260603)-02-96 of the Chairman of the Board of the Bank of Lithuania of 2 June 2016 on the approval of description of procedure for the movement of visitors, values, and property in/out of the Bank of Lithuania.

34. The use and maintenance of hardware and software shall be performed in accordance with the procedure laid down in the Rules for the Use of Computerised Workplaces of the Bank of Lithuania approved by Order No 02-138 of the Chairman of Board of the Bank of Lithuania of 20 July 2005 on the approval of rules for the use of computerised workplaces of the Bank of Lithuania, the Rules for the Protection of Mobile Devices of the Bank of Lithuania approved by Order No V 2017/(1.7-260603)-02-106 of the Chairman of Board of the Bank of Lithuania of 28 April 2017 on the approval of rules for the protection of mobile devices of the Bank of Lithuania and the Rules for the Use of Portable Computers of the Bank of Lithuania approved by Order No V 2013/(1.7-260402)-02-69 of the Chairman of the Board of the Bank of Lithuania of 17 April 2013 on the approval of rules for the use of portable computers of the Bank of Lithuania.

35. Personal data back-up copies shall be made in consideration of the development of technical capacities, implementation costs, and nature, scope and purposes of data processing, as well as danger of different probability and seriousness caused by data processing to the rights and freedoms of natural persons. Personal data back-up copies shall be made in accordance with the procedure laid down in the Rules for Copying the Information of the Bank of Lithuania approved by the Decree No V 2016/(26.53.E-2602)-84E-2 of the Director of the Information Technology Department of the Organisation Service of 8 January 2016 on the approval of rules for copying the information of the Bank of Lithuania.

36. The testing of IS should not be performed with real personal data, except where necessary. In such cases, additional organisational and technical security measures should be used (e.g. pseudonymisation) ensuring the security of real personal data. The cases of testing with real data must be agreed with the DPO and information security officer.

37. Security measures for obtaining (providing) personal data that must be taken while obtaining or providing personal data are the following:

37.1. the use of secure protocols and (or) passwords must be ensured when personal data are transmitted through external data transmission networks;

37.2. when personal data are obtained (provided) in an external data storage medium, personal data security control must be ensured: data to be provided in an external medium shall be encrypted, and these data shall be erased from the external medium after their use;

37.3. while transmitting personal data by email to addressees that are out of the network of LB, the information being transmitted shall be encrypted or other safe ways of information exchange with the third parties shall be used.

38. In consideration of the nature of personal data being processed and the risk raised to personal privacy by their processing, additional organisational and technical personal data security measures may be provided for, such as:

38.1. encryption of personal data saved in active (operating) database;

38.2. personal data pseudonimisation;

38.3. periodic assessment of risk in the information system;

38.4. periodic inspection of emergency recovery of personal data from external media while carrying out practical tests;

38.5. recording of actions with personal data: files connected, actions performed with personal data (input, verification, alteration, destruction, and other actions relating to personal data processing);

38.6. control of actions carried out by persons administering database(s), service station(s), and information system shall be performed applying additional security measures.

39. The following organisational and technical personal data security measures must be implemented while processing personal data filing systems by non-automated means:

39.1. time limit(s) for personal data storage and actions to be performed after the expiry of this time limit must be indicated;

39.2. procedure for giving, destroying, and amending the power to process personal data must be indicated;

39.3. access to premises where documents and their archives are stored must be controlled.

40. All employees shall sign an understanding to keep the personal data secret (see Annex 2). This understanding shall be stored in the signatory‘s file.

41. Where LB involves third parties in supplying the services related to personal data processing, the processing of personal data must be subject to the security requirements no lower than those established in Annex 1 to the Regulations.

CHAPTER VII
MANAGEMENT OF PERSONAL DATA SECURITY BREACHES

42. Personal data security breaches shall be managed in accordance with the Description of Procedure for Security Incident Management of the Bank of Lithuania approved by Order No V 2019/(1.7.E-260603)-02-23 of the Chairman of the Board of the Bank of Lithuania of 26 February 2019 on the approval of the description of procedure for security incident management of the Bank of Lithuania.

43. All facts related to the breach of personal data protection (cause of the breach, what happened and what personal data were affected, impact and effects of the breach, incident elimination actions, decisions on breach elimination) shall be saved in the Information System of Incident Management in accordance with the procedure established in the Description of Procedure for Security Incident Management of the Bank of Lithuania.

44. When it is determined that a breach had no impact on a data subject’s privacy, the Inspectorate and the data subject shall not be informed about the incident.

45. When it is determined that a breach of data security may pose a danger to the rights and freedoms of natural persons, it shall be reported to the Inspectorate within the time limits set in Article 33(1) of the Regulation and without unreasonable delay to a data subject provided that the conditions laid down in Article 34(3) of the Regulation are absent.

CHAPTER VIII
IMPLEMENTATION OF THE RIGHTS OF DATA SUBJECTS

46. LB shall ensure that the rights laid down in the Regulation concerning data subjects, whose personal data it processes, are implemented.

47. The rights of data subjects shall be implemented by LB in accordance with the Procedure for the Implementation of the Rights of Data Subjects of the Bank of Lithuania approved by Resolution No 03-86 of the Board of the Bank of Lithuania of 24 May 2018 on the approval of the procedure for the implementation of the rights of data subjects of the Bank of Lithuania.

CHAPTER IX
PROVISION OF DATA

48. LB provides personal data to data recipients – third parties and data processors.

49. Personal data shall be provided to the following third parties:

49.1. state institutions and bodies;

49.2. courts;

49.3. law enforcement authorities;

49.4. other third parties to which LB is obligated by laws or other legal acts to provide personal data or when it is necessary to do so in the course of performing the functions delegated to LB, implementing the duties of LB as an employer, in accordance with the Regulation or when executing the procurement contracts.

50. Personal data shall be provided to third parties under an agreement on the provision of personal data (repeated provisions of personal data), procurement contracts (execution of procurement contracts), at request (one-off provision of personal data) or in accordance with the procedure established by legal acts.

51. Where personal data are provided under an agreement on the provision of personal data or a procurement contract and the data recipient is the controller of personal data, the agreement or the contract should stipulate the purpose of personal data use, legal grounds, conditions and procedure for provision and receipt of these data and the scope of personal data requested. If personal data are provided upon request, it must include the purpose of data storage, legal grounds for provision and receipt of these data and the scope of personal data requested.

52. Personal data shall be provided to third persons only where legal grounds for the provision of personal data exist, in consideration of the purpose of personal data processing and the scope of these data.

53. LB may provide personal data to data processors who provide their services to LB or perform other works and process personal data on behalf of LB as a data controller.

54. Data processors invoked by LB shall ensure that the technical and organisational measures of data processing be implemented in a way that the data processing complies with the requirements of the Regulation and ensures the protection of rights of the data subject.

55. The provisions pertaining to the processing and protection of personal data shall be included in the contracts concluded with the data processors that should contain the following conditions:

55.1. subject-matter and duration of personal data processing;

55.2. purpose and nature of personal data processing;

55.3. personal data type and data subject categories;

55.4. rights and obligations of the data controller and data processor;

55.5. permission or prohibition for the data processor to invoke other data processors;

55.6. commitment of the data processor to process the personal data received while performing the contract on behalf of LB and only under the instructions of LB in compliance with the requirements of the legal acts regulating data protection;

55.7. obligation of the data processor to implement suitable technical, organisational and legal data protection measures to ensure the security of personal data transferred;

55.8. obligation of the data processor to assist LB in implementing the rights of the data subject;

55.9. obligation of the data processor to provide to LB all information necessary to ascertain and to prove that the personal data are processed lawfully, and to enable and help LB or a person authorised by LB to perform the personal data processing audit, including inspections;

55.10. with regard to the nature of data processing and information possessed by the data processor, its commitment to assist LB in implementing the obligations set out in legal

acts and associated with the personal data security breaches, data protection impact assessment and prior consultations;

55.11. prohibition for the data processor to use the personal data transferred for purposes other than specified in the data processing agreement or for its own marketing purposes;

55.12. obligation of the data processor to be liable for unauthorised personal data processing and to compensate LB for the damages sustained, fines or compensations paid due to unauthorised personal data processing performed by the data processor;

55.13. obligation of the data processor to destroy the personal data transferred or return them to LB upon expiry of the agreement;

55.14. other terms necessary to ensure the lawfulness and security of the processing of personal data transferred.

56. LB may transfer personal data to a third country or an international organisation, if:

56.1. it complies with the resolutions of the European Commission on adequate protection of personal data in third countries: Andora (2010/625/EU), Argentina (2003/490/EC), Jersey (2008/393/EC), Faroe Islands (2010/146/EU), Guernsey (2003/821/EC), Israel (2011/61/EU), Canada (commercial organisations) (2002/2/EC), Isle of Man (2004/411/EC), New Zealand (2013/65/EU), Switzerland (2000/518/EC), Urugway (2012/484/EU), and Japan (EU) 2019/419);

56.2. it complies with the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield and the data recipient in the US is included the public list of organisations, which were certified in accordance with the Privacy Shield (*https://www.privacyshield.gov/welcome*);

56.3. such provision has been established by a compulsory and enforceable mutual document of LB and a public authority or an institution located in a third country;

56.4. standard data protection clauses adopted by the European Commission or Inspectorate are observed (Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (2004/915/EC) (OJ 2004 L 385, p. 74);

56.5. transfer of personal data is based on an approved certification mechanism.

57. Where the provision of personal data to a third country or an international organisation cannot be based on at least one of the conditions provided for in paragraph 56 herein, the permission of the Inspectorate should be obtained to provide personal data, or personal data may be provided without the permission of the Inspectorate as established in paragraph 58 below.

58. Where none of the conditions established in paragraph 56 herein are met and the permission of the Inspectorate is not obtained, personal data may be transferred provided that the following conditions are satisfied:

58.1. the transferral is required due to important reasons of public interest[1] and this interest has been recognised under the law of the European Union or the Republic of Lithuania;

58.2. data transfer is necessary for lodging, exercisind or defending of legal claims.

59. When applying to the Inspectorate for a permission to transfer personal data to a third state or an international organisation to be issued, the Procedure for the Issue of Permissions for the Transfer of Personal Data to Third Countries or International Organisations approved by Order No 1T-68 (1.12.E) of the Director of Inspectorate of 18 July 2018 on the approval of the procedure for the issue of permissions for the transfer of personal data to third countries or international organisations shall be followed and an application in the form approved by Order No 1T-52 (1.12.) of the Director of Inspectorate of 24 May 2018 on the approval of the recommended form of the application for the permission to transfer personal data to third states or international organisations shall be submitted.

60. Where it is planned to ground the transfer of personal data on the condition stipulated in subparagraph 56.3 herein or contracts and aggreements in respect of which the

[1] For example, in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport, and in other cases provided for in p. 112 of the Preamble of the Regulation.

Inspectorate issues a permission, such agreements and contracts, when drafted, should include the provisions obligating the data recipients to implement the principles associated with data processing, and measures enabling the implementation of such principles, and provide for effective remedies to be made available for the data subjects.The following obligations for data recipients are recommended to be set out in the contracts:

60.1. to process personal data only for those purposes they were transferred for;

60.2. to ensure the confidentiality of personal data received, including the duty to ensure that the personal data received could be processed only by those employees of the data recipient who are required to do so as part of an assigned task or functions;

60.3. to ensure the security of personal data received;

60.4. to reply to the inquiries of data subjects and data provider concerning the personal data processing;

60.5. to cooperate with the data provider, data subject and data protection supervisory authority on issues of personal data processing;

60.6. other provisions required in specific cases.

CHAPTER X
FINAL PROVISIONS

61. The DPO contact details and information on personal data processing (purposes of data processing, data providers and recipients, data being processed, legal grounds for processed data, and data storage duration), rights of data subjects and their implementation shall be published on the website of the Bank of Lithuania, under Personal data protection.

62. The Regulations shall be reviewed, amended and updated periodically, however not less than once per year or after the amendment of legal acts or upon the implementation of organisational or structural changes.

63. The employees of the Bank of Lithuania processing personal data shall be personally responsible for proper processing and security of personal data. The employees of the Bank of Lithuania shall be subject to responsibility laid down in the legal acts for breaches of personal data processing and security.

64. The Regulations shall be introduced to all employees of LB, who shall confirm this by their signatures.

_____

Annex 1
to the General Personal Data
Processing Regulations of the
Bank of Lithuania

LIST OF PROTECTION MEASURES OF PERSONAL DATA PROCESSED BY AUTOMATED MEANS[2]

1. Management and control of access to personal data		
1.1.	Access to personal data is provided only to the persons, who need personal data to carry out their functions.	☐
1.2.	Only actions authorised in respect of the user can be carried out regarding person data.	☐
1.3.	A two-factor authentication is used to access the personal data – employee's ID card with the certificate and a PIN code. _____ (please specify if another authentication method is used)	☐
1.4.	Control of access to personal data: 1.4.1. 3 failed login attempts allowed; 1.4.2. records of logins of individuals to the information systems processing personal data are registered: login identifier, date, time, duration, outcome of the login (successful, failed); 1.4.3. records of logins and actions are stored for _____ (please enter the deadline)	☐ ☐
2. Physical measures of personal data security		
2.1.	Security of premises in which personal data are stored is ensured: 2.1.1. restricted entry of unauthorised persons to the LB premises; 2.1.2. access of authorised persons only to the relevant (increased security) areas is ensured.	☐ ☐
3. Measures for security of personal data receipt (provision)		
3.1.	Where personal data are received/provided in an external data storage medium: 3.1.1. personal data are deleted after using them; 3.1.2. personal data provided are encrypted.	☐ ☐
3.2.	When transferring personal data by email to a recipient outside the LB network, information is encrypted or other secure methods for data exchange with third parties are used. _____ (please specify the exchange methods used)	☐
3.3.	Where personal data are received/transferred via external data transmission networks, use of secure protocols (e.g. SSL) and/or passwords is ensured.	☐
4. Destruction or anonymisation of personal data		
4.1. 4.2.	Irreversible destruction of personal data is ensured upon expiry of the established personal data storage period. Anonymisation of personal data is ensured upon expiry of the established personal data storage period.	☐ ☐
5. Use and maintenance of hardware and software		
5.1.	Protection of hardware against harmful software is ensured (e.g. installation of antivirus applications, updates).	☐
5.2.	Backup copies of personal data are made.	☐
5.3.	Actions of personal data recovery from data copies are registered (who	☐

[2] If a measure is not relevant to this IS, specify this under the appropriate item in footnotes.

	ordered; when and who performed the actions).	
5.4.	Backup copies of personal data in external data storage mediums are encrypted.	☐
5.5.	Backup copies of personal data are stored in at least two external data storage mediums, which are kept separately, in another room or geographic location.	☐
5.6.	It is ensured that information system testing is not performed with real personal data.	☐
5.7.	Official data stored on mobile devices (portable computers, tablets, smart phones, etc.) are encrypted or protected by measures corresponding to the risk of personal data disclosure.	☐
6. Risk assessment of information systems		
6.1.	Pre-operational Risk assessment or risk re-assessment of the information system in which personal data are processed risk has been carried out (please specify the assessment date and document number in footnotes).	☐
7. Additional data security measures		
7.1.	Personal data stored in an active (functioning) database are encrypted.	☐
7.2.	Personal data pseudonymisation.	☐
7.3.	Periodical risk assessment of information systems is carried out. _____ (please specify the frequency)	☐
7.4.	Periodical inspection of emergency personal data recovery from external mediums is carried out via practical tests. _____ (please specify the frequency)	☐
7.5.	Registration of records of actions with personal data: files that were accessed, actions with personal data performed (input, review, modification, destruction and other personal data processing actions). _____ (please enter the period for which records of actions are stored)	☐
7.6.	Measures used to control the actions of persons administering the database/server/information system. _____ (please specify the measures used)	☐
8. Other information _____ (please specify other personal data security measures used, if any)		

Position, name and last name of employees who performed the assessment _____

Annex 2
to the General Personal Data
Processing Regulations of the
Bank of Lithuania

DECLARATION OF THE EMPLOYEE OF THE BANK OF LITHUANIA TO UPHOLD PERSONAL DATA SECRECY

I understand that:

- in the course of my employment, I shall process personal data, which may not be disclosed or transferred to unauthorised persons or institutions;
- it is prohibited to transfer to unauthorised persons passwords and other data allowing to gain access, via software and technical means, to personal data or otherwise enable them to familiarise themselves with personal data;
- inappropriate personal data processing may incur liability according to the laws of the Republic of Lithuania.

I hereby undertake to:

- uphold the personal data secrecy throughout the entire duration of my service (employment) and upon termination of service (employment) at the Bank of Lithuania, if such personal data is not intended to be made public;
- abstain from disclosing or transferring the information processed to any person who is not authorised to use it within the Bank of Lithuania or outside it, or from enabling them to familiarise themselves with such information by any means;
- use personal data only when and to the extent necessary when carrying out the assigned functions and tasks;
- abstain from using personal data for my own personal purposes and interests or those of my family members, relatives or friends;
- abstain from copying, photographing or otherwise reproducing personal data, if this is not necessary for the performance of the assigned functions and tasks;
- keep the documents and data files suitably and safely in order to prevent accidental or unauthorised destruction, alteration or disclosure of personal data as well as any other unauthorised personal data processing;
- notify my supervisor, persons responsible for data security and Data Protection Officer of any suspicious situations that might threaten personal data security.

I am aware that:

- I shall be liable for the non-observance of this obligation and breach of any legal acts regulating the personal data protection in accordance with the laws of the Republic of Lithuania in force;
- data subjects are entitled to material and non-material damages incurred due to unauthorised personal data processing or other acts or omissions of the data controller, data processor or other persons;
- data controller, data processor or another person shall compensate the damages inflicted to the person and recover the losses in accordance with the procedure established by the laws from the employee through whose fault the damages appeared.

I have familiarised myself with the 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), the Republic of Lithuania Law on Legal Protection of Personal Data, General Personal Data Processing Regulations of the Bank of Lithuania and legal acts of the Bank of Lithuania referred to in the General Personal Data Processing Regulations of the Bank of Lithuania to the extent they apply to me in my service (work) when processing personal data, and with the liability for their breaches.

_____

(position of the employee) (name and last name) (signature)