ACBA BANK GROUP
PRIVACY POLICY

Registration code	Edition number	Approval date	Entry into force date
GROUP POLICY 21#6	1	01.06.2026	08.06.2026

Developed by:

Structural unit	Position	Name Surname
	"ACBA BANK" OJSC Chief Legal and Compliance Officer	Zarine Azizyan
	"ACBA BANK" OJSC Chief IS and Cybersecurity Officer	Vagharshak Iskandaryan

Pre - approved with:

Position	Name Surname
"ACBA BANK" OJSC Chief Executive Officer	Hakob Andreasyan
"ACBA LEASING" CO CJSC General Director	Aghasi Gasparyan
"ACBA BANK" OJSC, "ACBA LEASING" CO CJSC Chairman of the Board Risk Management Committee	Ashot Karapetyan

Approved by:

Position	Name Surname
"ACBA BANK" OJSC, "ACBA LEASING" CO CJSC Chairman of the Board	Sona Ishkhanyan

Contents

SECTION 1. GENERAL PROVISIONS 3

1. PURPOSE AND SCOPE OF APPLICATION 3

2. DEFINITIONS 3

3. ROLES AND RESPONSIBILITIES 6

SECTION 2. PERSONAL DATA PROTECTION 7

4. RELATIONS WITH STAKEHOLDERS 7

5. PRINCIPLES OF PERSONAL DATA PROTECTION 7

6. PURPOSES OF PERSONAL DATA COLLECTION AND PROCESSING 8

7. CLASSIFICATION OF DATA SUBJECTS AND LIST OF PROCESSED PERSONAL DATA 8

8. GROUNDS AND CONSENT FOR PERSONAL DATA PROCESSING 9

9. TRANSFER OF PERSONAL DATA 10

10. STORAGE AND DESTRUCTION OF PERSONAL DATA 10

11. RIGHTS OF THE DATA SUBJECT 11

12. INFORMATION SYSTEMS PROCESSING PERSONAL DATA, PROCESSING METHODS 11

13. PRIVACY IMPACT ASSESSMENT 12

SECTION 3. BANKING SECRECY PROTECTION 13

14. GENERAL PROVISIONS 13

15. OBLIGATIONS OF THE BANK REGARDING THE MAINTENANCE OF BANKING SECRECY 13

SECTION 4. DATA SECURITY AND TECHNICAL MEASURES 13

16 TECHNICAL AND ORGANIZATIONAL MEASURES 13

SECTION 5. DUTIES AND RESPONSIBILITIES OF GROUP EMPLOYEES 14

SECTION 6. ACCOUNTABILITY 14

SECTION 7. TRAINING 14

SECTION 1. GENERAL PROVISIONS

1. PURPOSE AND SCOPE OF APPLICATION

1.1. The ACBA BANK GROUP Privacy Policy (hereinafter referred to as the "Policy") defines the general principles for collection, processing, storage, transfer, erasure, and protection of personal data within the Group, as well as the protection of information constituting banking secrecy.

1.2. The purpose of the Policy is to:

- Protect the legitimate interests of customers, employees, other stakeholders of the Group, and the Group itself through a reliable data protection management system,
- Ensure compliance with the requirements established by applicable national and international legislation,
- Define roles and responsibilities for all bodies and individuals who support effective data protection,
- Establish clear principles regulating any use of confidential data as defined by this Policy,
- Ensure the identification and mitigation of privacy risks through a Privacy Impact Assessment process,
- Promote the maintenance of an information security culture and the safe and proper management of data within the Group.

1.3. This Policy serves as the basis for the implementation of key solutions in the field of personal data protection and oversight within the Group. This Policy shall not be interpreted as an authorization for the processing of personal data or the provision/disclosure of banking secrecy based on grounds, scopes, or procedures not established by applicable laws, regulations, and international legislation.

1.4. The Policy applies to all levels of management within the Parent Company and Subsidiary, as well as to all business and functional units and employees. The policy is also applicable to all third parties who process personal data on behalf of the Group or a Group company, or who have access to information constituting banking secrecy.

2. DEFINITIONS

ACBA BANK GROUP or Group: Includes the Parent Company and the Subsidiary.

Parent Company or Bank: "ACBA BANK" OJSC, the primary governing body of the Group.

Subsidiary or Leasing: "ACBA LEASING" CO CJSC or any other company that the Parent Company may acquire or establish as a subsidiary in the future in accordance with the procedure established by applicable legislation.

Board of the Parent Company: The collegial management body of the Parent Company which, within the scope of powers defined by RA legislation and the Charter of the Parent Company, is responsible for the strategic oversight of the Parent Company, supervision of executive management, and the protection of the interests of shareholders and other stakeholders.

Board of the Subsidiary: The collegial management body of the Subsidiary which, within the scope of powers defined by RA legislation and the Charter of the Subsidiary, is responsible for the strategic oversight of the Subsidiary, supervision of executive management, and the protection of the interests of shareholders and other stakeholders.

Board: Collectively refers to the Board of the Parent Company and the Board of the Subsidiary.

Board Committee(s): Committees of the Parent Company's Board and the Subsidiary's Board, established to support the Parent Company's and the Subsidiary's Boards in fulfilling their responsibilities.

In the context of the Policy Board Committee(s) refers to the Board Risk Management Committee.

Chief Executive Officer (CEO) of the Parent Company or Chief Executive Officer: The sole executive body of the Parent Company, responsible for the executive management and the leadership/supervision of the day-to-day operations of the Parent Company, in accordance with the procedure established by the current legislation and the Charter of the Parent Company.

Executive-level Committee(s): Executive committees of the Parent Company that perform consulting and advisory functions. The decisions of the Executive-level Committees are made solely by the Parent Company's CEO. The opinions of the other members of the Executive-level Committee(s) shall be advisory in nature.

In the context of the Policy Executive-level Committee(s) refers to the Compliance Committee.

Top Management: Parent Company's CEO, Directors, and Chief Accounting Officer.

Business Units: resource centers composed of the Group's employees with relevant specializations, operating as complete business directions. These units include both product/service development and sales specialists, who are responsible for all stages of the business process—from development and launch to maintenance and delivery of the planned outcomes. Business Units include the following two business directions/structural units of the Parent Company: Retail Business Directorate and SME and Corporate Business Directorate, as well as the employees and units of the Subsidiary.

Functional Units: support centers composed of the Group's employees with relevant specializations responsible for providing professional, strategic, and regulatory support, as well as operational services or oversight, to all Business Units. Functional Units include the following structural units of the Parent Company: Digital Platforms and Technology Directorate, Operations Directorate, Finance Directorate, Risk Management Directorate, Credit committees and analyses directorate, Legal and Compliance Directorate, HRM and Organizational Development Directorate, AML/CFT and Sanctions Directorate, Information Security and Cybersecurity Directorate, as well as AML/CFT and Sanctions Responsible Person of the Subsidiary.

Confidential data: For the purposes of this Policy, confidential data includes personal data and information constituting banking secrecy.

Customer: A person establishing a business relationship or currently in such a relationship with the Group company, as well as a person who proposes to the Group company to perform, or performs, a one-time transaction.

Personal data: Any information relating to a natural person which allows or may allow for the direct or indirect identification of the person's identity.

Data subject: A customer, including a natural person representing a legal entity, an authorized person/beneficial owner, a physical person affiliated with a customer, as well as a third party whose data is collected by the Group company, an employee of the Group, a person affiliated with them, or a person affiliated with the Group, and applicants.

List of personal data: A list of data relating to a specific subject.

Personal data confidentiality requirements: Established rules that determine restrictions on the access, transfer, provision, and storage conditions of personal data.

Group's Compliance Function Responsible Person(s): Head of the Compliance division and Legal and Compliance Director of the Parent Company.

Data Protection Officer: A Group employee who monitors and undertakes legal, organizational, and technical measures to ensure the proper performance of personal data processing functions within the Bank in accordance with the requirements of this Procedure. The Head of the Compliance Division serves as the Data Protection Officer at the Group.

Collection of personal data: The procedure for obtaining personal data from data subjects.

Processing of personal data: Actions performed with personal data, including collection, systematization, accumulation, storage, clarification (updating, modification), use, distribution (including transfer), depersonalization, and destruction of personal data.

Consent of the data subject: A free, specific, unconditional, and conscious expression of a person's will in the form provided by this Procedure, whereby the subject signals their consent to the processing of their personal data.

Transfer of Personal Data: The provision of personal data by the Group/Group company to third parties; an action aimed at transferring data to a specific or indefinite circle of other persons or making them acquainted with it, including publishing personal data through mass media, posting it on information communication networks, or otherwise making personal data accessible to another person.

Blocking of personal data: The temporary suspension of the transfer, clarification, use, and destruction of personal data.

Destruction (erasure) of personal data: Actions as a result of which it becomes impossible to restore the content of personal data in the personal data information system and/or as a result of which the physical carriers of personal data are destroyed.

Depersonalization of personal data: Actions as a result of which it becomes impossible to determine the ownership of the personal data to a specific subject without the use of additional information.

Personal data information system: The entirety of personal data contained in databases and the information technologies and technical means that ensure their processing.

Special categories of personal data: Information concerning a person's racial or national origin or ethnic origin, political views, religious or philosophical beliefs, trade union membership, health status, and sex life.

Publicly available personal data: information that, with the consent of the data subject or through the performance of conscious actions aimed at making his/her personal data publicly available, becomes available to a specific or indefinite circle of persons, as well as information that is provided for by law as publicly available information.

GDPR (General Data Protection Regulation): The general regulation on personal data protection adopted by European Union regulation, the purpose of which is to provide data subjects who are residents of the European Union with the ability to control their personal data.

Interested person: A customer, partner, agent, consultant, contractor, supplier and vendor, intermediary, service provider, and other persons performing similar tasks or functions, as well as RA state bodies and the Central Bank of Armenia.

Authorized body: Personal Data Protection Agency of the Ministry of Justice of the RA and/or Central Bank of the RA.

Privacy Impact Assessment: A process aimed at identifying, evaluating and mitigating the privacy risks arising from new or significantly changed personal data processing activities/processes. The purpose of a privacy impact assessment is to assess the necessity and proportionality of data processing, identify the risks to the rights and freedoms of data subjects and document the controls adopted to address those risks.

High-risk data processing: Processing of personal data that is likely to result in a high risk to the rights and freedoms of natural persons, including the processing of special categories of personal data on a large scale, systematic automated decision-making with significant legal consequences. High-risk processing requires a mandatory Privacy Impact Assessment to be carried out before the process begins.

Personal data breach: An incident that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed by the Group.

Banking secrecy: the customer account information which becomes known to the Bank in the course of servicing customer, information on the operations made upon the instruction of the customer or for the benefit of the customer, as well as trade secret, information on any project or plans regarding its activity, invention, industrial design and any information thereon, which the customer has intended to keep confidential and the Bank is aware or could have been aware of this intention.

Disclosure of bank secrecy: the disclosure or dissemination of the information constituting bank secrecy through mass media or otherwise in oral or written form, its disclosure to the third party or parties, directly or indirectly enabling the third parties to obtain such information, i.e. to permit, fail to prevent or, as a result of violation of the privacy rules, make the disclosure possible, except for cases prescribed by Article 43 of the Law of the Republic of Armenia “On banks and banking”. A third party is considered to be all other persons, except for the Bank and its client, and the Central Bank, banks and credit organizations defined by the RA Law "On Credit Organizations", credit bureaus defined by the RA Law " On circulation of credit information and activities of credit bureaus", and the Deposit Compensation Guarantee Fund in cases defined by the RA Law "On guaranteeing the compensation of bank deposit to natural persons" are not third parties.

Provision of banking secrecy: Provision of information constituting banking secrecy is the communication of such information orally or in writing to state bodies, officials and citizens only in cases and on grounds prescribed by law.

3. ROLES AND RESPONSIBILITIES

3.1. ***The Board:***

- Approves the Policy and its material amendments and provides general oversight regarding the proper implementation of the requirements of this Policy.

3.2. ***Board Committee(s):***

- oversees the implementation of the Policy and assists the Board in ensuring compliance with its requirements,
- reports to the Board on compliance with the requirements of the Policy.

3.3. ***The chief Executive Officer:***

- manages and ensures the development, implementation and effective execution of the Policy within the Group,
- Ensures that the Bank's internal procedures comply with regulatory requirements.
- Assists the Subsidiary's General Director in establishing and applying unified approaches to personal data protection and the preservation of banking secrecy, ensuring compliance with the Group's overall strategy.

3.4. ***Executive-level Committee(s):***

- Reviews, disputes and pre-approves reports to be submitted to the Board and to the Board committee(s).

3.5. ***Subsidiary's General Director:***

- Ensures the implementation and day-to-day execution of the Policy requirements within the Subsidiary.
- Ensures compliance with policy provisions and methodologies set by the Parent Company

3.6. ***Group's Compliance Function Responsible Person(s):***

- Develops the Policy and is responsible for its application,
- Submits relevant reports to the Executive-level Committee, Subsidiary's General director, the Board Committee, and the Board at defined forms and intervals.

3.7. ***Data Protection Officer:***

- Acts independently and reports directly to the Board and the Chief Executive Officer/ Subsidiary's General Director on all data protection matters.
- Acts as a contact person for the Authorized Body or other regulators, as well as for personal data subjects.
- Notifies the Authorized Body of the intention to process data in cases specified in the RA Law "On Personal Data Protection".
- maintains a register of incidents related to personal data and banking secrecy,
- provides relevant advice to business and functional units regarding compliance with Policy requirements,
- organizes appropriate training courses, as well as coordinates and conducts the Privacy Impact Assessment process.

3.8. ***Information Security and Cyber Security Directorate:***

- maintains the confidentiality, integrity, and availability of information systems and data.
- Identifies and evaluates security vulnerabilities and cyber threats associated with the processing of confidential data within information systems.
- timely detects, records, and reports cyber incidents related to the security of confidential data to the Compliance Division.

3.9. ***Human Resources Management and Organizational Development Directorate:***

- Ensures the collection and processing of personal data of candidates applying for vacancies within the Group and of employees, in accordance with applicable laws, regulations, this Policy, and other internal legal acts of the Group.
- Maintains relevant records/ledgers of employees' personal data and ensures their integrity and security.

3.10.***All Employees and Involved Persons:*** Comply with the requirements of this Policy and applicable laws, regulations, and internal legal acts.

SECTION 2. PERSONAL DATA PROTECTION

4. RELATIONS WITH STAKEHOLDERS

4.1. In the field of personal data protection, the Group carries out activities aimed at identifying and satisfying the requirements of interested persons. Within the framework of these activities, the Group:

1) Maintains all information provided within the framework of agreements with customers, partners, and suppliers (including organizations controlling and processing personal data), which may contain financial, marketing, personal, and other data. These constitute confidential information and must be preserved in accordance with RA legislation and international norms in the field of information security, as well as the information security requirements effective within the Group,

2) Bears responsibility for the preservation and non-disclosure of the confidential information of interested persons, which entails financial and legal obligations,

3) Ensures that provided information is not disclosed to third parties without the permission of the interested persons or competent state authorities,

4) Informs all interested persons, in accordance with the procedure established by legislation and internal legal acts, regarding significant changes and emerging issues in the field of ensuring information security requirements related to them, which the Group company deems expedient and necessary to notify them about,

5) Ensures business continuity for the fulfillment of its obligations toward interested persons.

4.2. In turn, all interested persons undertake to ensure the implementation of procedures for the preservation of trade secrets, copyrights, and the classification of the Group's information based on relevant contract.

5. PRINCIPLES OF PERSONAL DATA PROTECTION

5.1. **Principle of lawfulness, fairness, and transparency:** Personal data must be processed in a lawful, fair, and transparent manner for the data subject. The Group must define and document the legal basis for each processing operation. Processing must not be carried out in a misleading or coercive manner, or in a way that the data subject could not reasonably expect. The Parent Company and Subsidiary must provide data subjects with clear and accessible information regarding the processing of their data through privacy notices and other communications. The Parent Company and Subsidiary must exclude the processing of data for any other purpose without the consent of the data subject.

5.2. **Principle of proportionality:** Personal data must be collected for specified, explicit, and legitimate purposes and must not be further processed in a manner incompatible with those purposes. The purposes of processing must be clearly defined before collection begins and communicated to the data subjects. Any new or secondary use of personal data must be assessed within the context of the original purpose; in case of incompatibility, a new legal basis must be established or additional consent must be obtained.

The Group shall apply the principle of Privacy by design, incorporating data protection considerations into systems, processes, services and products from an early stage of design. Privacy by default means that where there is a choice regarding the collection and processing of personal data, the strongest privacy protection settings are applied by default, unless the data subject explicitly chooses otherwise.

If the purpose can be achieved in a depersonalized (anonymous) manner, data processing must be excluded.

5.3. **Principle of accuracy:** Personal data must be accurate and, where necessary, kept up to date. The Group must take all reasonable steps to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay. The Group must implement procedures that enable data subjects to correct inaccurate data and must periodically verify the accuracy of the data stored in its systems.

5.4. **Principle of minimum engagement of subjects:** Whenever possible and upon the written consent of the data subject, the Group should collect the necessary personal data from other bodies to ensure minimum involvement of the data subject.

5.5. **Principle of storage limitation:** Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.

5.6. **Principle of integrity and confidentiality (security):** Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized access or processing, as well as against accidental loss, destruction, or damage, using appropriate technical and organizational measures. The Group must implement a multi-layered security system that includes physical and technical controls proportionate to the risk arising from each processing operation.

5.7. **Principle of accountability:** The Group, as a data processor, is responsible for compliance with all the principles mentioned above and must be able to demonstrate compliance with these established principles. The accountability principle requires the Group to adopt and implement internal legal acts for data protection and to conduct impact assessments.

6. PURPOSES OF PERSONAL DATA COLLECTION AND PROCESSING

6.1. The Parent Company and Subsidiary process personal data to achieve the following purposes:

1) Submission of reports to state supervisory bodies in accordance with the requirements of the applicable legislation,

2) Execution of banking and leasing services/operations in the market,

3) Implementation of actions within the framework of compliance with AML/CFT requirements by the Parent Company and Subsidiary,

4) Collection of data regarding credit history,

5) Regulation of labor relations between the Group company and the employee (recruitment, training, promotion, collection, and processing of personal data of candidates for vacancies),

6) Establishment of contractual relations with data subjects (customers, suppliers, contractors, and business partners) for providing banking and leasing services, as well as for utilizing various services (financial, outsourcing/delegation, training, supply of goods, repair, construction, etc.).

7. CLASSIFICATION OF DATA SUBJECTS AND LIST OF PROCESSED PERSONAL DATA

7.1. The Parent Company and Subsidiary processes the personal data of the following subjects:

1) Candidates who have applied for vacancies within the Group companies,

2) Employees of the Group companies (including persons undergoing a probationary period or training, and other workers hired on a temporary basis or within the framework of outsourcing agreements concluded with other organizations for the purpose of delegating certain functions of the Group companies),

3) Persons affiliated with the employees of the Group companies, regarding whom personal information became known to the Group companies during the conclusion of an employment contract with the employee, the updating of their personal data, the implementation of measures to monitor conflicts of interest, and other circumstances,

4) Natural person shareholders of the Group companies,

5) Partners: natural persons, representatives of legal entities, individual entrepreneurs, and persons with whom contracts have been concluded for the provision of services necessary for the Group companies to carry out their economic activities,

6) Members of the Board,

7) Customers: natural persons, individual entrepreneurs, and natural person representatives of physical and legal entities accepted for service provision by the Group companies (participants, beneficial owners, founders, directors, accountants, authorized persons, persons

confirmed by signature samples, bankruptcy managers, legal representatives, guardians, other persons affiliated with the customer, and other physical persons),

8) Indirect participants in customer transactions of the Group companies (persons associated with transactions/business relationships involving pledged property, guarantors, pledgors, family members), regarding whom personal data is collected and processed for a predetermined purpose.

7.2. The exemplary list of personal information used by the Parent Company and Subsidiary when serving customers consists of the following data:

1) First name, last name, patronymic
2) Gender,
3) Date of birth,
4) Place of birth,
5) Identification document,
6) Photograph of the person in the identification document or other documents,
7) Identification document number,
8) Date of issue of the identification document,
9) Expiry date of the identification document,
10) Registration address (residential address),
11) Residency,
12) Center of vital interests,
13) Marital status,
14) Phone numbers,
15) Email address,
16) Place of work and position,
17) Field of activity,
18) Salary,
19) Work experience,
20) Passwords used in the automated banking system.

7.3. For the purpose of serving individuals applying for various credit products and services, the Parent Company and Subsidiary may additionally process the following personal data:

1) Income,
2) Level of solvency,
3) Contact information regarding current and previous places of employment,
4) Information regarding family members and their income,
5) Information regarding property ownership rights,
6) Information regarding liabilities.

7.4. The Parent Company and Subsidiary may process other personal data permitted by law for individuals who are employees of the Parent Company and Subsidiary or persons undergoing employment procedures for the purpose of concluding an employment contract (job applicants, candidates).

8. GROUNDS AND CONSENT FOR PERSONAL DATA PROCESSING

8.1. Processing of personal data is permissible upon the consent of the personal data subject. Personal data may be processed without the consent of the data subject if the data processing is directly provided by law. The consent of the personal data subject is not mandatory for the processing of publicly available personal data.

8.2. Depending on the type of transaction or business relationship, consent may be granted through various documents used within the Parent Company and Subsidiary. For individuals holding banking accounts at the Bank, consent for personal data processing is obtained via "Know Your Customer" (KYC) questionnaires: eFO 72-02-10, eFO 72-02-11. For certain transactions, in accordance with the RA Law "On Protection of Personal Data," consent may be given orally. In all cases, the data subject's consent must be explicit and documented.

8.3. **Consent of incapacitated and limited-capacity persons**: In the event of the data subject's incapacity or limited capacity, or being a minor under the age of 16, the data subject's legal representative shall provide consent to the processing of his or her personal data.

8.4. **Processing of special categories of personal data:** Processing special categories of personal data without the person's consent is prohibited, except when the processing of such data is directly provided for by law. The processing of special categories of personal data must be terminated immediately if the grounds and purpose for processing the data no longer exist. The processing of special categories of personal data is considered high-risk data processing and a Privacy Impact Assessment must be conducted before processing begins.

9. TRANSFER OF PERSONAL DATA

9.1. The transfer of personal data is considered the dissemination of information of a personal nature through communication channels and/or electronic media, both within the territory of the RA and outside the territory of the RA to another country.

9.2. Within the Republic of Armenia, personal data may be provided to:

1) The Central Bank of Armenia,

2) "ACRA Credit Reporting" CJSC,

3) Competent state bodies (RA courts, investigation and tax authorities) in accordance with applicable legislation,

4) Representatives of auditing organizations in accordance with the contracts concluded with the latter

5) Other persons based on a court decision or with the written consent of the data subject, including during the process of system integration between the Bank and payment systems or other organizations.

9.3. During the transfer of personal data, the recipient of the information is responsible for fulfilling information security and protection requirements, as well as for preventing the leakage of such information.

9.4. Personal data may be transferred to another country with the consent of the data subject, or if the transfer of data arises from the purposes of personal data processing and/or is necessary for the realization of those purposes.

9.5. Personal data may be transferred to another state without the permission of the authorized body if an adequate level of personal data protection is ensured in that state.

9.6. An adequate level of personal data protection is considered ensured if:

1) Personal data is transferred in accordance with international treaties,

2) Personal data is transferred to any country included in the list officially published by the Authorized Body,

3) Personal data may be transferred to the territory of a state that does not provide an adequate level of protection only with the permission of the Authorized Body, provided that the personal data is transferred on the basis of a contract, and the contract stipulates such personal data protection guarantees that have been approved by the Authorized Body as providing adequate protection.

9.7. The list of countries having an adequate level of personal data protection and officially published by the Authorized Body is defined by Decision No. ATPP-001/24 "Decision of the Head of the Personal Data Protection Agency on defining the list of states ensuring an adequate level of personal data protection." The list of states ensuring an adequate level of personal data protection under the mentioned decision is presented in Annex 1.

9.8. The Group shall enter into written data processing agreements with all third parties that process personal data on behalf of the Group.

10. STORAGE AND DESTRUCTION OF PERSONAL DATA

10.1. The Group is obliged to retain personal data obtained during processing, business correspondence, all documents, copies of documents obtained as a result of due diligence of the data provided by the client, for the period specified in the Data Retention and Archiving List after the

termination of the business relationship with the client or the implementation of a one-time transaction.

10.2. The storage and destruction of personal data in information systems and in hard copy (paper) format are carried out in accordance with the provisions of the Group's internal legal acts.

10.3. The destruction of personal data processed by the Parent Company and Subsidiary is carried out in such a way that it is impossible to accurately restore the content of the personal data in the information system, or the physical carriers of the personal data (documents) are destroyed.

10.4. Data present on digital storage media used within the Group, including those containing personal data, are destroyed according to the provisions described in the "ACBA BANK" OJSC Guidelines for the Use of Data Carriers: IN 27-01.

10.5. The destruction of information stored in hard copy is performed via paper shredding (using special paper shredding equipment, if available).

10.6. In the event of the termination of relationships with a customer, partner, or persons associated with the Parent Company and Subsidiary, the Group companies may extend the storage of personal data for periods longer than those prescribed by law, if this serves the interests of the Group and is carried out within the framework of its service delivery strategy.

10.7. Depending on the purposes of certain subjects' personal data, the Parent Company and Subsidiary are permitted to perform the depersonalization of such data instead of destroying it.

11. RIGHTS OF THE DATA SUBJECT

11.1. The data subject has the right to obtain information regarding their personal data, the processing of such data, the grounds and purposes for processing, the Parent Company and Subsidiary and their locations, as well as the persons to whom the personal data may be transferred.

11.2. The data subject has the right to access their personal data and to request their rectification or removal (depersonalization) if the personal data are incomplete, inaccurate, outdated, obtained illegally, or if the purposes for their collection are no longer relevant.

11.3. The data subject may withdraw his/her consent by sending an email to the Data Protection Officer at dpo@acba.am or by submitting a request in person at any branch of the Group or at the Head Office. The Group shall acknowledge receipt of the withdrawal request within 5 business days and shall make a final decision within 30 business days. In the event of withdrawal, the Group shall notify the relevant third parties to whom the data have been transferred.

11.4. The data subject shall have the right not to be subject to a decision based solely on automated processing which produces legal or other significant effects concerning him or her, except as otherwise provided by law. Where the Group makes decisions based solely on automated processing which produce significant effects concerning the data subject, the Group shall, at the time of data collection, inform the data subject of the existence of such automated processing and its logic, allow the data subject to request a human review of the decision and allow the data subject to contest the decision and to express his or her point of view.

11.5. For the purpose of exercising their rights—to obtain information regarding personal data or to perform any action related to them, such as rectification, removal, or depersonalization—the data subject is obliged to submit a request to the Parent Company and Subsidiary in writing. The written request may be submitted to the branches or Head Offices of the Group companies, or by sending an email to the Group’s Data Protection Officer at the email address: dpo@acba.am.

12. INFORMATION SYSTEMS PROCESSING PERSONAL DATA, PROCESSING METHODS

12.1. The processing of personal data in the Bank is carried out both through the use of platform/ technologies and without them, and can be stored on both paper and electronic carriers. At the same time, the Bank and Leasing complies with all requirements for automated and non-automated processing of personal data as prescribed by the legislation of the Republic of Armenia and the EU General Data Protection Regulation (GDPR).

12.2. The processing of personal data in the Group is carried out through the following stages:

1) collection,
2) recording,

3) systematization (organization),
4) accumulation,
5) storage (backup),
6) clarification (updating, amendment),
7) use, transfer (provision is carried out in cases provided for by the RA legislation as defined in Chapter 5 of this Procedure),
8) anonymization (depersonalization),
9) blocking,
10) erasure,
11) destruction.

12.3. The classification of the primary information systems processing personal data is as follows:

1) operating systems,
2) databases,
3) software applications,
4) hardware (network and server equipment, data storage and backup systems, etc.).

13. PRIVACY IMPACT ASSESSMENT

13.1. The purpose of the Privacy Impact Assessment (hereinafter referred to as the Assessment) is to identify, assess, and address privacy risks arising from personal data processing activities prior to the commencement of such activities.

13.2. Conducting an Assessment is mandatory prior to the commencement of any of the following activities/processes:

1) Any new personal data processing activity that has not been previously carried out by the Group,
2) Any material change to an existing processing activity (purpose, categories of data, scope, recipients, retention period, or technical systems),
3) Any processing of special categories of personal data,
4) Any high-risk data processing activity, including large-scale automated decision-making or profiling,
5) Implementation of new technologies or systems involving the processing of personal data,
6) Delegation of any personal data processing function to a third-party processor.

13.3. In cases where it is unclear whether an Assessment is required, the relevant department must consult with the Compliance Division to determine the necessity of the Assessment.

13.4. Each Assessment is conducted by the Compliance Division in cooperation with the initiating department and must, at a minimum, include:

1) Description of the processing activity: its purpose, legal basis, data categories, data subjects, and retention period,
2) Necessity and proportionality: whether the processing is necessary for the specified purpose, and whether there are alternatives involving fewer privacy risks,
3) Risk identification: identification of risks to the exercise of data subjects' rights,
4) Risk mitigation: technical and organizational measures addressing the identified risks,
5) Indication of the approving body or person.

13.5. Personal data processing subject to mandatory Assessment may not commence until the Assessment is completed and the relevant approving body or person has signed it.

13.6. Approving Body: In case of Low Risk—Head of Compliance Division; in case of High Risk—Chief Executive Officer; in case of Very High Risk—the Board.

13.7. Each completed Assessment must be reviewed at least once every three years, or sooner in the following cases: a material change in the processing process, a Personal Data Breach related to the processing, or a change in applicable legislation.

13.8. The Compliance Division shall maintain an Assessment Register, recording for each Assessment: a unique identification number, start and end dates, the initiating unit, a description of the assessed processing, adopted control mechanisms, residual risk, the decision of approval or rejection, and the date of the next review. A summary of the Assessment shall be included in the quarterly report presented to the Executive-level Committee, the Board Committee, and the Board.

SECTION 3. BANKING SECRECY PROTECTION

14. GENERAL PROVISIONS

14.1. This section regulates the management and protection requirements for information constituting banking secrecy by the Parent Company. The regulations of the RA Law "On Banking secrecy" supplement the general requirements for the protection of personal data of this Policy.

15. OBLIGATIONS OF THE BANK REGARDING THE MAINTENANCE OF BANKING SECRECY

15.1. The Bank is obliged not to disclose information constituting banking secrecy to any third party without the written consent of the customer, except in cases directly permitted or required by law.

15.2. All employees of the Bank bear the obligation to maintain banking secrecy, which continues to apply even after the termination of employment relations.

15.3. Banking secrecy may be disclosed only in the cases and according to the procedure established by law. Information constituting banking secrecy may be provided to:

1) the Central Bank of the Republic of Armenia,
2) criminal prosecution bodies based on a court decision,
3) the Court based on a relevant decision,
4) the Financial System Mediator,
5) the customer's heirs (successors) upon provision of sufficient documents substantiating the rights of inheritance (successorship),
6) tax authorities based on a relevant court decision.

15.4. The Bank implements contractual and technical protection measures to ensure that third-party service providers and processors maintain banking secrecy obligations equivalent to the requirements established by applicable legislation.

SECTION 4. DATA PROTECTION

16. TECHNICAL AND ORGANIZATIONAL MEASURES

16.1. To ensure data security as defined by this Policy, the Group shall undertake the following technical and organizational measures:

1. Appropriate security measures shall be defined and applied to ensure the confidentiality, integrity, and availability of data, prevent data leaks, and establish requirements for data retention and secure disposal.
2. High-priority data, including personal data, shall be used, stored, and transmitted in an encrypted format based on its level of confidentiality; this process shall comply with established encryption requirements and rules.
3. Regular backups of databases shall be performed to ensure data integrity.
4. Mandatory authentication shall be required when accessing the information system to minimize the risk of unauthorized access to confidential data.
5. Monitoring and periodic audits of the actions of employees with access to personal data and banking secrecy shall be conducted, including audits aimed at identifying excessive access privileges.
6. All operations related to personal data and banking secrecy shall be logged.
7. Penetration testing of information systems and vulnerability assessments shall be conducted.
8. Analysis and management of events and cyber incidents shall be carried out in accordance with the procedure defined by the Information Security Incident Management Guidelines of "ACBA BANK" OJSC (IN 27-09).
9. Security assurance systems shall be implemented for all information systems utilized in the processing of personal data.

10. Access restrictions shall be applied to server rooms that form part of the information infrastructure processing, storing, and transmitting banking secrecy and personal data, in accordance with the List of Persons Authorized to Access Confidential Areas of "ACBA BANK" OJSC (LI 100-01).
11. Principles of segregation of duties shall be applied to ensure the effectiveness of protection processes for personal data and information constituting a banking secrecy.
12. Efforts shall be undertaken to raise the awareness of data processors in order to strengthen the protection of personal data and information constituting a banking secrecy.
13. Personal data and information constituting a banking secrecy shall be stored on electronic media exclusively in an encrypted form.
14. Provisions regarding the protection of personal data and information constituting a banking secrecy shall be mandatorily included in all employment contracts and service agreements.
15. Due diligence shall be conducted for all third-party vendors acting as data processors, and specific data processing provisions shall be incorporated into the agreements concluded with them.

SECTION 5. DUTIES AND RESPONSIBILITIES OF GROUP EMPLOYEES

17.1. All Group employees who have access to personal data and information constituting banking secrecy, arising from the performance of their work duties, by Employment contracts undertake obligations and are responsible for ensuring the confidentiality of such data.

17.2. If a Group employee becomes aware of an instance or attempt of unauthorized disclosure of personal data and banking secrecy, or if pressure is exerted on a Group employee to obtain such information, or if other actions are taken against a Group employee (aimed at the illegal acquisition of personal data and banking secrecy), the Group employee is obliged to immediately inform their direct supervisor and/or the Compliance Division, and/or the DPO either by sending an email to the Data Protection Officer at dpo@acba.am or via the Whistleblowing system—by sending details of the incident to the independent Whispli system or to the external email address acba.compliance@gmail.com.

17.3. Responsibility for maintaining security measures during the processing of personal data and the use of information constituting banking secrecy located on Group workstations, mobile media, and paper carriers rests with those Group employees who process such data.

17.4. In the event of a violation of the requirements of the Policy, disciplinary sanctions may be applied to employees, up to and including dismissal, as well as other liability measures defined by legislation.

SECTION 6. ACCOUNTABILITY

18.1. The Compliance Division shall submit summary information regarding cases and developments related to personal data and banking secrecy recorded during the reporting period to the Executive-level Committee, the Board Committee and the Board, within the framework of a quarterly Compliance report.

SECTION 7. TRAINING

19.1. The Group acknowledges continuous training as a vital prerequisite for the protection of personal data and banking secrecy, and for the effective management of risks related to confidentiality.

19.2. 16.2. The Legal and Compliance Directorate is responsible for organizing periodic training on personal data and bank secrecy for all employees. This training is intended to help employees be aware of their responsibilities as set out in this Policy.

19.3. 16.3 The Compliance Division shall develop and disseminate guidelines, Frequently Asked Questions (FAQs), Q&As, and other information materials for the purpose of the effective implementation of the Privacy policy.

ANNEX 1

List of countries ensuring an adequate level of personal data protection

1. Republic of Albania
2. United States of America (organizations)
3. Principality of Andorra
4. Republic of Austria
5. Argentine Republic
6. Kingdom of Belgium
7. Bosnia and Herzegovina
8. Republic of Bulgaria
9. Federal Republic of Germany
10. Kingdom of Denmark
11. Republic of Estonia
12. Iceland
13. Ireland
14. Italian Republic
15. Kingdom of Spain
16. State of Israel
17. Republic of Latvia
18. Principality of Liechtenstein
19. Republic of Lithuania
20. Grand Duchy of Luxembourg
21. Republic of Poland
22. Republic of Croatia
23. Canada
24. Republic of Korea
25. Republic of Cyprus
26. Republic of North Macedonia
27. Hellenic Republic (Greece)
28. Hungary
29. Japan
30. Republic of Malta
31. United Kingdom of Great Britain and Northern Ireland
32. Republic of Moldova
33. Principality of Monaco
34. Montenegro

35. Kingdom of the Netherlands
36. New Zealand
37. Kingdom of Norway
38. Kingdom of Sweden
39. Swiss Confederation
40. Czech Republic
41. Portuguese Republic
42. Romania
43. Russian Federation
44. Republic of San Marino
45. Republic of Serbia
46. Republic of Singapore
47. Slovak Republic
48. Republic of Slovenia
49. Georgia
50. Ukraine
51. Oriental Republic of Uruguay
52. Republic of Finland
53. French Republic