EUROBANK

eurobank.gr

EUROBANK S.A.
8 Othonos Str., 105 57 Athens, GR

GCR. 154558160000

June 2026

Privacy and Personal Data Protection

High-level public statement of principles and commitments

Eurobank S.A. is committed to processing personal data lawfully, fairly, transparently and securely, and to respecting the rights and freedoms of individuals whose personal data it processes.

1. Purpose and scope

This Public Policy Statement describes the high-level principles and commitments that guide Eurobank S.A. (the "Bank") in protecting personal data. It applies to personal data processing carried out across the Bank's operations, products, services and digital channels and covers customers and prospective customers, employees and contractors, suppliers and partners, representatives, beneficial owners and other individuals whose personal data the Bank processes.

The statement also applies to third parties processing personal data on behalf of the Bank or accessing Bank systems or personal data, to the extent provided by applicable contractual and legal requirements.

2. Privacy principles

- **Lawfulness, fairness and transparency**. Personal data are processed on an appropriate legal basis and individuals are provided with clear information about relevant processing.
- **Purpose limitation**. Personal data are collected for specified, explicit and legitimate purposes and are not further processed incompatibly with those purposes.
- **Data minimisation**. Processing is limited to personal data that are adequate, relevant and necessary for the relevant purpose.
- **Accuracy**. Reasonable steps are taken to keep personal data accurate and up to date where necessary.
- **Storage limitation**. Personal data are retained only for as long as required for the processing purpose, applicable legal or regulatory requirements, or the establishment, exercise or defence of legal claims.
- **Integrity and confidentiality**. Appropriate technical and organisational measures are applied to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.
- **Accountability**. The Bank maintains governance, policies, records, assessments, controls, training and assurance arrangements to support and demonstrate compliance.

3. Governance and accountability

The Data Protection Officer (DPO) leads the Bank's data protection function and reports directly to a Deputy Chief Executive Officer who participates in the Board of Directors and the Executive Board. The DPO provides independent advice and oversight and reports regularly to the Executive Board and the Board Risk Committee on material data protection developments, risks, incidents and metrics.

The Personal Data Protection Policy is approved by the Executive Board and is regularly reviewed and updated to reflect applicable legal and regulatory requirements. Privacy requirements are embedded in the Bank's risk, compliance and governance arrangements and in the applicable Group-wide framework. Responsibilities are assigned to relevant business and control functions, while non-compliance may result in disciplinary, contractual or other appropriate action.

4. Transparency and lawful processing

The Bank provides privacy information describing, as applicable, the categories and sources of personal data, the purposes and legal bases of processing, recipients, international transfers, retention periods, individual rights and contact details. The main Information on the Processing of Personal Data is available online and may be supplemented by specific notices for particular processing activities.

Consent is requested and managed where consent is the appropriate legal basis. Individuals may withdraw consent at any time without affecting the lawfulness of processing carried out before withdrawal. The Bank does not rent or sell personal data and discloses personal data only to defined categories of recipients for explicit and legitimate purposes and subject to applicable legal, regulatory and contractual safeguards.

5. Individual rights and requests

The Bank enables individuals to exercise their rights under applicable data protection law, including rights of access, rectification, erasure, restriction, objection and data portability, the right to withdraw consent where applicable, rights relating to solely automated decision-making, and the right to lodge a complaint with the competent supervisory authority. Requests are handled through established processes and within the applicable statutory deadlines.

Where the right to erasure applies, deletion is implemented across relevant active systems and, through the applicable backup retention and lifecycle processes, across backup environments. Erasure remains subject to legal and regulatory retention obligations and other lawful grounds requiring continued retention.

6. Privacy by design and impact assessment

Privacy by design and by default is applied in the development of new products, services and digital channels and in material changes involving personal data. Privacy risks are assessed before launch and Data Protection Impact Assessments are conducted where required, including where the processing is likely to result in a high risk to individuals. Identified safeguards and risk treatments are incorporated into design, approval and implementation activities.

7. Third parties and international transfers

External service providers and other third parties that process personal data or have access to Bank systems are required to protect personal data under applicable contractual arrangements. The Bank conducts initial and periodic risk-based assessments and, where appropriate, audits of relevant third parties to assess compliance with contractual, security and data protection obligations.

Transfers of personal data outside the European Economic Area take place only where permitted by applicable law, including on the basis of an adequacy decision, appropriate safeguards or a legally available derogation.

8. Security of personal data

The Bank's Information Security Policy is based on a framework of continuous improvement and supports the confidentiality, integrity, availability and protection of information and personal data. Appropriate safeguards include multi-factor authentication, role-based access controls, encryption and de-identification techniques, applied according to the nature and risk of the relevant processing. The Bank maintains capabilities to monitor, detect, respond to and recover from information security threats and incidents.

Eurobank maintains ISO/IEC 27001 and ISO/IEC 27701 certifications. Internal audits and other assurance activities support monitoring of the effectiveness of the security and privacy management framework.

9. Personal data breaches

The Bank maintains a formal process for identifying, escalating, assessing and managing personal data breaches. The competent supervisory authority and affected individuals are notified where required by applicable law. Incidents and remedial measures are monitored through the relevant governance arrangements.

10. Training, monitoring and review

Privacy and data protection training is provided to all employees and contractors, including at onboarding and through periodic refresher and awareness activities. The

Bank conducts risk-based privacy assessments and audits of relevant processes, technologies and third parties.

The effectiveness of the privacy framework is monitored through management reporting, risk assessments, audits, incident analysis, rights-request monitoring and policy review. This statement is reviewed periodically and updated when material legal, regulatory, technological or operational changes warrant it.

11. Exercising rights and contacting the DPO

Information about individual rights and how to exercise them is available at Eurobank's GDPR information page. Individuals may contact the Data Protection Officer at dpo@eurobank.gr or by post at 6 Siniosoglou Street, 14234 Nea Ionia, Greece.

Related public information

This statement should be read together with the following public information:

- Eurobank GDPR - General Data Protection Regulation
- Eurobank Sustainability Statement
- Eurobank Security Hub - How we protect your transactions