



ALPHA BANK

Notification

On the Processing of Personal Data

A. PROVISION OF INFORMATION TO DATA SUBJECTS

ALPHA BANK A.E. (hereinafter referred to as "the Bank"), in its capacity as data controller, in accordance with the Regulation (EU) 2016/679 and under the provisions of the Greek legislation on the protection of personal data, informs the natural person (hereinafter referred to as "Customer" regardless of its gender or status), that the Bank itself and / or third parties, acting on the Bank's instructions and on its behalf, will process personal data relating to him, in the context of any transactional relationship established between them for any product or service offered by the Bank (deposit, loan, guarantee, investment product, bancassurance, payment service, investment service), in the way described as below.

I. What kind of data do we collect*?

- a) Identification data, such as name, father's name, gender, Identity Card Number (IDN), VAT number, date and place of birth, nationality and other demographic data.
- b) Communication data, such as postal and e-mail address, phone number and mobile phone number.
- c) Economic, family and property status data, such as profession, earnings, dependent members, income tax return form, other tax and income related documentation (for example E1 and E9 forms).
- d) Data related to Customer's default status on his financial obligations, such as bad checks, terminations of loan and credit contracts, orders of payment, seizures and checks to be paid, claims and decisions for resolution and bankruptcy.
- e) Creditworthiness data, such as amounts owed to credit and/or financial institutions in the context of loan and/or credit contracts.
- f) Data related to credit profiling and credit scoring.
- g) Data related to subject's transactional behavior (marketing profiling).
- h) Data derived from the performance of the Customer's contract (-s) with the Bank and the use of the products that have been provided to him.
- i) Data related to Customer's knowledge and experience in the investment or insurance sector, his financial status, his level of risk tolerance and his investment objectives.
- j) Data derived from payment transactions and payment services.
- k) Data related to Customer's ID identifiers and his transactional behavior provided by devices or applications he uses, such as IP address or other data provided through devices used by the Customer as location identifiers and cookies, which alone or in combination with unique identifiers, can be used for the Customer's identification and profiling.
- l) Health data concerning the Customer and/or family members dependent from him, under special circumstances.
- m) Data concerning phone conversations records with the Customer, which are recorded in accordance with the legislative requirements.

* Except for items (a) and (b) mentioned above, which are strictly necessary for every transaction or contractual relationship between the Customer and the Bank, the type and number of the rest collected data depends, ad hoc, on the type of the relationship and the offered or supplied product or service.

II. Where do we collect your data from?

The above mentioned personal data are collected from the following sources, as appropriate:

- a) Identification and communication data (under points I, a-b above) from the Customer and/or publicly accessible sources, including social networks on an internet site.
- b) Economic, family and property status data (under point I, c above) from the Customer and/or publicly accessible sources, such as land registers, cadastral offices and the "Mortgages and Prenotations to Mortgages System" of TIRESIAS SA (as defined below).
- c) Default financial obligation data (Default Financial Obligation System), credit status data (Credit Consolidation System) and credit scoring data (Credit Bureau Scoring) (under points I, d – f above) from the above mentioned registers (Systems) of the TIRESIAS SA company (as defined below), as well as from Companies working in collaboration with the Bank and providing notification services to debtors (under the provisions of the Greek Law No 3758/2009), from law firms, lawyers and Loans and Credit Management Companies (under the provisions of the Greek Law No 4354/2015), for any relevant cases assigned to them by the Bank.
- d) Data related to subject's transactional behavior and data from the operation of the Customer's contract (-s) with the Bank (under points I, g and h above) from the "Credit Consolidation System" of the TIRESIAS SA (as defined below).
- e) Data related to Customer's investor profile (under point I,i above) from the Customer himself.
- f) Data related to Customer's payment transactions (under point I, j above) from the Customer himself or from payment service providers, acting on Customer's instructions.
- g) Data related to Customer IDs identifiers or location identifiers (under point I, k above) from services or applications the Customer uses, or/and from publicly accessible sources, including social networks and service providers working in collaboration with the Bank (for example Google).
- h) Health data (under point I, l above) are provided by the Customer on his own initiative.
- i) The data (under point I, m above) from the phone conversations with the Customer.

As far as the processing of the above mentioned personal data shall be based on Customer's consent, the Bank follows the procedures provided by law, in order to inform the Customer and obtain his consent.

The company by the name "Bank Information Systems SA" and the trade mark "TIRESIAS SA" is the economic-behavior data controller acting on behalf of the coun-

try's banking system. You can contact TIRESIAS SA, established at 2, Alamanas Street, 151 25 Maroussi, at the telephone number 210 367 6700. You can also check out www.teiresias.gr for additional information relating to the processing of your data and the exercise of your rights.

III. Why do we collect your data and how do we process them?

Personal data collected in the way described above, either on the launch of the transactional relationship, or later, are processed for the following purposes:

- a) For the identification of the Customer and the communication with him in case of any transactional, pre-contractual or contractual relationship established between him and the Bank, in order for the Bank to fulfil its contractual and / or legal obligations.
- b) In the case of granting loans or credits of any kind and for the purposes of complying with the Bank's legal obligations or defending Bank's legitimate interest:
 - i. for the assessment of the credit risk that the Bank is either required to assume or has already assumed,
 - ii. to monitor the performance of the relevant contract and debt,
 - iii. to prevent or reduce the likelihood of default of the relevant obligations,
 - iv. to seek the recovery of the liabilities owed in case of breach of the relevant obligation, which (recovery) is mandatory for the Bank under the law and the regulatory decisions made by the supervisory authorities, being also a Bank's obligation towards all its Customers and Shareholders;
 - v. for the management of liabilities arising from the credit contracts.
- c) For the conclusion of the Customer's contract, its execution and generally its smooth performance and for the fulfillment of the Bank's obligations towards the Customer.
- d) For the documentation of any request submitted by the Customer (such as a request for debt settlement due to a health incapacity) and its examination by the Bank.
- e) For the prevention and repression of money laundering and financing of terrorism, and in order to counter fraud against the Bank or its Customers and any other illegal activity.
- f) In order for the Bank to comply with the obligations imposed by the applicable legal and regulatory framework and the supervisory requirements, as well as with the decisions made by authorities or courts.
- g) For the defense of Bank's rights and legitimate interests and for the protection of retail customers, including, for example, safeguarding the Bank's security procedures, preventing crime, identifying and collecting evidence related to infringing conduct (instances of fraud etc.).
- h) For the communication with the Customer, in the context of a contract's performance, in order to inform him about the full use of products or services

provided by the Bank, their capabilities, characteristics and developments, as well as in order to investigate the degree of Customer's satisfaction in relation to Bank's services and/or any further Customer's wishes or demands, for the purposes of servicing Bank's legitimate interest.

- i) To promote new products and services provided by the Bank and/or its coordinated companies or third parties, to an existing and/or potential Customer, as far as there is an explicit Customer's consent to that effect.

The Bank may apply partially automated methods to achieve the objectives mentioned:

- under points (b) and (c) above combined with credit profiling, based on the Customer's economic data, as well as his solvency status data and his credit-worthiness data,
- under point (e) in accordance with the relevant international standards and
- under point (h) and (i) combined with marketing profiling, based on Customer's transactional habits.

IV. Who are the data recipients?

- a) The Bank's employees, who are responsible for the management and performance of the contract(s) signed between the Customer and the Bank, for the fulfillment of the obligations arising therefrom, as well as for the relevant obligations imposed by the law, have to comply with the legal framework, including banking secrecy.
- b) Natural persons and legal entities, to which the Bank assigns the execution of certain tasks on its behalf, such as, inter alia, companies providing notification services to debtors (under the provisions of the Greek Law No 3758/2009), loans and credit management companies (under the provisions of the Greek Law No 4354/2015), call center companies, lawyers, law firms, notaries and bailiffs, accredited mediators and mediation centers, experts, database management companies, risk management companies, research companies of communication and/or property data, file storage and record-keeping companies, market research, advertising and promotion companies acting on behalf of the Bank, as well as postal services providers, providers of services related to the development, maintenance and customization of IT applications, e-mail services providers, companies providing web-hosting services, including cloud services, companies providing specialized payment services. In all cases, the persons and entities mentioned above should act in compliance with professional secrecy and the duty of confidentiality and discretion.
- c) Credit and / or financial institutions having their registered office in Greece or abroad, licensed and operating legally, as well as special purpose companies or entities within the meaning of Law 3156/2003 on securitization.
- d) Debt collection companies under Law 4354/2015, as applicable, as well as entities of the financial sector, including domestic or foreign investment companies, in the event of the transfer (assignment) of claims arising from credit contracts.

- e) Companies belonging to the Alpha Bank Group, for the purposes of assessing the overall risk assumed, fulfilling their prudential obligations and treating the Customer in a single way.
- f) Credit institutions and payment services providers with a registered office in Greece or abroad, licensed and operating legally, for the execution of services or transactions.
- g) Supervisory, audit, independent, judicial, public and/or other authorities and bodies within the scope of their statutory tasks, duties and powers.
- h) TIRESIAS S.A. for data relating to records kept by TIRESIAS S.A. itself, such as data relating to bad checks, dishonored bills of exchange, termination of loan or credit contracts, loan and credit contracts and their development, as well as guarantee contracts.
- i) Co-financing or guarantee institutions, where relevant, such as the Hellenic Fund for Entrepreneurship and Development (ETEAN SA), the European Investment Bank, and the Greek State.

V. Are the data transferred to non-EU countries (third countries) or an international organization?

- a) where the European Commission has decided that the third country or the international organization in question ensures an adequate level of protection,
- b) when the Customer has been specifically informed and has given his express consent to the Bank, provided also that the rest conditions laid down in the legislative framework are met,
- c) where the transfer is necessary for the execution of contractual obligations, such as in case the transfer is necessary for the execution of payment orders to a bank account held in a third-country credit institution, or for the execution of orders for transactions in financial instruments,
- d) where the transfer is necessary for the foundation, exercise or support of legal claims or the defense of the Bank's legal rights,
- e) where the transfer is necessary under a statutory provision or a transnational or international convention, or
- f) for the purposes of the Bank's compliance with rules relating to automatic exchange of information in the tax area, provided for by the statutory and regulatory framework.

In order to fulfill the obligations under points e or f above, the Bank may transfer the Member's personal data to the competent national authorities, in order for them to forward these data to the relevant authorities of third countries.

VI. For how long are the data retained?

If a contract has been concluded with the Bank, then the latter retains personal data of the Customer up to the statutory general limitation period for the claims, i.e. for up to twenty (20) years from the termination of the relevant contract, regardless of the way in which this termination occurs.

If, by the expiration of the above period, there are ongoing judicial proceedings with the Bank or any connected company, concerning directly or indirectly the Customer, then, the above period for the retention of the data will be extended until a final judicial decision is issued.

In the case that no contractual relationship has, after all, been established, the personal data of the Customer will be retained for up to five (5) years from the date of their collection, upon submission of a relevant request (statutory limitation period for any claims under non-contractual liability).

Where a shorter or longer time period for the retention of data is provided for by law or regulatory acts, then the retention period mentioned above will be reduced or increased proportionately.

The contractual documents bearing the Customer's signature, in which personal data are included, may, after the expiration of a five-year period, be retained, at the option of the Bank, in electronic/ digital form.

VII. What rights does the Customer have for the protection of his data?

The Customer has the following rights:

- a) To know which personal data, concerning him, are being stored and processed by the Bank, as well as their source (right of access).
- b) To request for the rectification and/or supplementation of these data, so as to be complete and accurate, by submitting any necessary document which shows the need for supplementation or rectification (right to rectification). This is at the same time a Customer's obligation.
- c) To request for the restriction of processing concerning his personal data (right to restriction of processing).
- d) To deny and/ or object to any further processing of his personal data retained by the Bank (right to object).
- e) To request for erasure of his personal data from the Bank's records (right to be forgotten).
- f) To request for the transfer of the data he has provided to the Bank to another controller (right to data portability).

It should be noted that the fulfilment of the requests mentioned under points c, d and e, insofar as they relate to data necessary for the conclusion or continuation and operation of the contract, whether granted by the Customer or obtained from any public source, implies the automatic termination of the relevant contract or contracts by the Customer, in accordance with their relevant terms, or the inability to examine the subject's request.

Furthermore, the Bank has, in any case, the right to refuse the request for restriction of processing or erasure of Customer's data if the processing or maintenance of these data is necessary for the establishment, exercise or support of the Bank's legitimate interest, its legal rights or for the compliance with its legal obligations, as mentioned under Sections I and III above.

The exercise of the subject's right to data portability (under point f above) does not imply the erasure of the data from the Bank's records, which erasure takes place under the conditions laid down in the immediately preceding paragraph.

The exercise of these rights shall have effect for the future and does not concern already performed data processing.

The Customer has the right to file a complaint with the Personal Data Protection Authority (www.dpa.gr), which is the competent supervisory authority for the protection of the fundamental rights and freedoms of natural persons with regard to their processing, when he assumes that his rights are infringed in any way.

VIII. How can the Customer exercise his rights, as mentioned under Section VII above?

In order to exercise his rights, as they were mentioned under Section VII above, the Customer may:

- address the Bank's branch network by submitting the Request to Exercise Rights Form,
- contact the Bank by phone to the telephone number 210 326 0000,
- contact the Bank by electronic means via the Bank's website www.alpha.gr, by submitting the Communication Form,
- contact the Bank by e-mail to the CSO@alpha.gr,
- furthermore, the Customer may print from the Bank's website www.alpha.gr the Request to Exercise Rights Form and send it by post to:

Alpha Bank

Department of Supporting Functions
Special Customer Services
105, Athinon Street, 10447 Athens

The Bank will endeavor to respond to the Customer within thirty (30) days of the submission of his request, but this period may be extended for sixty (60) additional days, if the Bank considers it necessary, taking into account the complexity of the request and the number of the requests. The Bank shall inform the Customer whenever the thirty (30) day-period is extended, within thirty (30) days from the receipt of the request, and mention the reasons of this extension.

If the Bank does not take action in relation to the request of the Customer, it shall inform the Customer without delay and within thirty (30) days of the receipt of his request at the latest, for the reasons it did not take action and for the possibility of the Customer to submit a complaint and open a judicial procedure.

The above service is provided free of charge. However, if the Customer's claims are manifestly unfounded, excessive or recurrent, the Bank may either impose a reasonable charge on the Customer, while providing him with the relevant information, or refuse to respond to such requests.

IX. How are the Customer's rights protected?

The Bank applies an information security management system to ensure the confidentiality and security of the Customers' data processing procedure and to protect them against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access and any other form of unlawful processing.

The above Customer's information is provided in accordance with Regulation (EU) 2016/679 of the European Parliament and the Council and under the provisions of the Greek legislation on the protection of personal data, as adopted and applied in the context of this Regulation, and it replaces any prior information which has been received under Law No 2472/1997 and may refer to contractual or other Bank documents.

B. CONTACT DETAILS

I) DATA CONTROLLER

ALPHA BANK S.A.
ADDRESS: 40, Stadiou Street, 102 52 Athens
CONTACT PHONE NUMBER: +30 210 326 0000

II) DATA PROTECTION OFFICER

ADDRESS: 15, Charilaou Trikoupi Street, 106 78 Athens
CONTACT PHONE NUMBER: +30 210 326 6953
Email: contact-DPO@alpha.gr