ALPHA BANK

Notice

on the Processing of Personal Data

Version 1.1 / December 2021

A. NOTICE TO THE DATA SUBJECT

ALPHA BANK S.A., with the distinctive title Alpha Bank (hereinafter "the Bank"), acting in its capacity as data controller informs the natural person (irrespective of gender or identity, hereinafter the "Customer"), pursuant to the General Data Protection Regulation (EU) 2016/679 and the respective provisions of the applicable Greek legislation on the protection of personal data, that it or third parties, at its request and/or on its behalf, process personal data that concern him/her, either as a part of his/her contractual relationship with the Bank regarding a banking product or service (deposit, lending, guarantee, investment, bank insurance, payment service, investment service), or in view of a transaction with the Bank as described below.

I. What personal data does the Bank collect*?

a) **Identification data**, such as surname, name, father's name, mother's name, gender, ID or passport copy, tax registration number, tax office, date and place of birth, nationality, and other demographic data.

b) **Contact data**, such as postal and e-mail address, residential and work address, landline, and mobile phone number, as they appear on utility bills (e.g., electricity bill, water bill, phone bill)

c) **Financial, property and family status data**, such as profession, income, assets, dependent family members, details appearing on the income tax statement and other tax details, insurance and income details (indicatively E1 and E9 forms, insurance clearance).

d) Data on **the breach of financial obligations**, such as bad cheques, loan and credit agreement terminations, payment orders, seizures and payable cheques, restructuring and bankruptcy filings and judgements.

e) Data on **creditworthiness**, such as debts to credit and/or financial institutions from loans and/or credits.

f) Data on **transactional behavior**, such as data on the operation of the Customer's contract(s) with the Bank and the use of the products and/or services that have been granted to the Customer by the Bank, as well as data on the consistency with outstanding financial obligations.

g) **Credit scoring** data.

h) Data from the execution of **payment transactions** and from the use of **payment services**.

i) Data on the Customer's **knowledge and experience in the investment sector or the insurance sector**, his/her financial status, his/her risk tolerance level and his/her investment and insurance goals.

j) Data of **contracts with companies for the acceptance of cards (acquiring) that have been terminated** by the credit institutions or card issuing and management companies with which the Customer cooperates, for reasons that constitute a breach of the terms of the relevant contracts (e.g., acceptance of cards that have been declared as lost, fictitious transactions, self-financing, etc.).

k) **Recognition data of the Customer's electronic identity** and transactional behavior, which are provided by devices (e.g., mobile phones, tablets) connected to the Bank's systems or applications, such as his/her IP Address and his/her position and location data deriving from the aforementioned devices, as well as internet browsing data (cookies), which alone or in combination with unique identifiers may be used for the identification of the Customer.

l) Data on the Customer's **health** and the health of his/her dependent members, where necessary, upon the Customer's request.

m) Data on the Customer's **telephone communications or videoconferences** with the Bank, recorded pursuant to the provisions of the relevant legal framework.

n) **Image** data from the video recording systems at the Bank's premises, which bear the relevant special signs (e.g., at the entrances of the Bank's branches and main buildings, at transaction counters, on ATMs).

o) **Biometric data** regarding (i) the characteristics of the Customer's handwritten signature placed on electronic media with a special pen (e.g., tablet), such as speed, acceleration and pace and (ii) the photograph of the Customer's face in the form of a dynamic self-portrait (dynamic-selfie) submitted in the context of the remote identification procedure for the provision of the Bank's products and services, where applicable.

p) The Customer's **Qualified Certificate for Electronic Signature** issued by a Qualified Trust Service Provider in accordance with Regulation (EU) 910/2014 (eIDAS), as applicable.

(*) Except for the data mentioned under a and b which are required for any transactional and contractual relationship of the Customer with the Bank, the type and amount of the other data collected depends on each specific contractual relationship of the Customer with the Bank in each case and the banking product or banking service offered or provided.

II. Where does the Bank collect the Customer's personal data from?

The aforementioned personal data is collected from the following sources, as the case may be:

a) **Identification and contact data** (under I, **a-b** above) is collected directly from the Customer upon disclosure to the Bank, either physically or electronically, or from third parties authorized by the Customer or through databases with or without the relevant order/authorization of the Customer (e.g., eGov-KYC of the General Secretariat for Information Systems), or from companies of the Bank's Group, with which the Customer cooperates, or from public authorities and services within the scope of their responsibilities or upon authorization by the Customer (e.g., Tax Office, Public Prosecutor's Office, ministries, supervisory bodies, etc.) or from publicly accessible sources, including freely accessible social media networks on online websites (e.g., Facebook, Instagram, Twitter, LinkedIn, etc.). The Client is obliged to inform the Bank immediately in case of any change of his/her data.

b) **Data** regarding the Customer's **financial, property and family status** (under I, **c** above) is collected directly from the Customer, upon disclosure to the Bank, either physically or electronically, or from third parties authorized by the Customer or through databases with or without the relevant order/authorization of the Customer (e.g., eGov-KYC of the General Secretariat for Information Systems, eEFKA of the National Social Security Fund, etc.), or from companies of the Bank's Group, with which the Customer cooperates, or from publicly accessible sources, such as land registries, cadastral offices and the Prenotation-Mortgage System of "TIRESIAS S.A." (as defined below), as well as from freely accessible social media networks on online websites (e.g., Facebook, Instagram, Twitter, LinkedIn, etc.).

c) **Data on the breach of financial obligations**, **on creditworthiness**, **on transactional behavior** and **on credit scoring** (under I, **d, e, f and g** above), is collected from the Bank's records of transactions, the systems of "TIRESIAS S.A." (as defined below), and other records of financial behavior data, operating legally in Greece or abroad, if applicable, as well as from Debtor Information Companies of L. 3758/2009, with which the Bank cooperates, law firms and lawyers, court bailiffs, and loan service provider companies of L. 4354/2015, for relevant cases assigned to them by the Bank.

d) **Data regarding the Customer's payment transactions** (under I, **h** above) is collected either directly from the Customer or from the Bank for the payments conducted by it or from payment service providers, at the Customer's request.

e) Data regarding the Customer's **investment profile** (under I, **i** above) is collected directly from the Customer and/or the Bank in the context of his/her investment transactions with the Bank.

f) Data of **contracts with companies for the acceptance of cards (acquiring) that have been terminated** (under I, **j** above) is collected from the Bank's systems and/or the Systems of TEIRESIAS S.A. (as defined below).

g) **Recognition data** (under I, **k** above) **of the Customer's electronic identity and transactional behavior,** position, or location data, is collected from the Bank's systems or applications, which the Customer connects to, as well as from service providers (indicatively Google), cooperating with the Bank.

h) **Health data** (under I, **l** above) is submitted by the Customer's on his/her own initiative.

i) **Data** on the Customer's **telephone communications or videoconferences** with the Bank (under I, **m** above) is collected from the recording systems of the Bank.

j) **Image data** (under I, **n** above) is collected from the video recording systems of the Bank.

k) **Biometric data** (under I, **o** above) of the Customer's electronic signature is collected from the Bank's electronic device, on which it is placed with the use of a special pen (e.g., tablet), and of the Customer's photograph (dynamic-selfie) is collected from the camera of the Customer's mobile phone device or any other electronic device (e.g., computer, tablet).

l) The Customer's **Qualified Certificate for Electronic Signature** (under I, **p** above) is collected from the Qualified Trust Service Providers, which the Bank cooperates with.

The company under the tradename ''BANK INFORMATION SYSTEMS SA'' and the distinctive title "TIRESIAS SA'' is a data controller of the financial behavior data on behalf of the country's banking system. The company's registered seat is at 2 Alamanas Street, 151 25 Maroussi. You can contact the company at the phone number 210 3676700.You can obtain information on the processing which it carries out as well as on the exercise of your rights through its website (www.teiresias.gr).

III. Why does the Bank collect the Customer's personal data and how does it process it?

The personal data, collected as per the above, either before or at the beginning or the Customer's contractual relationship with the Bank, or afterwards during its operation, is processed for the following purposes:

a) The **identification and communication data** (under I, **a** and **b**) for the Customer's identification, in the context of the Bank's "know your Customer" responsibilities, for the prevention and suppression of money laundering and terrorist financing, for the drafting of the contract with the Customer, as well as for the issuing of the qualified digital certificate, in accordance with Regulation (EU) 910/2014 (eIDAS), as applicable, in the context of the submission of a relevant request to a Qualified Trust Service Provider. (The processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract (article 6 paragraph 1b GDPR), as well as for the compliance with a legal obligation to which the controller is subject (e.g., Law 4557/2018 as applicable) (article 6 paragraph 1c GDPR)).

   Communication data (under I, **b**), in addition to its processing for reasons of identification of the Customer, is also subject to processing for the following reasons:
   - To contact the Customer in the context of the performance of the contract and his/her transactions with the Bank, whenever required,
   - To contact the Customer in order to inform him/her about the utilization of the products or services provided by the Bank, their capabilities, characteristics, functionalities, usage opportunities, and developments.
   - To contact the Customer in order to inform him/her of his/her participation in the Bank's loyalty programs, lotteries, competitions and the announcement of the Customer as a potential winner.

   (The aforementioned processing is necessary for the performance of a contract to which the data subject is a party (article 6 paragraph 1b GDPR))
   - To investigate the extent to which the Customer is satisfied with the Bank's customer service and the services provided, and/or the Customer's additional needs and wants for the purpose of analyzing the efficiency of the Bank's products and/or services, as well as the design and launch of new products and/or services.

   (The aforementioned processing is necessary for the purposes of the legitimate interests pursued by the controller (article 6 paragraph 1f GDPR)).
   - To promote new products and services of the Bank or/and companies or third parties affiliated with it, to an existing Customer, provided that the Customer has given his/her explicit consent, where applicable (article 6, paragraph 1a GDPR)).

b) Data on **financial, property and family status, breach of financial obligations**, **creditworthiness**, **transactional behavior,** and **credit scoring** (under I, **c-g**) in the case of granting of any loan or credit of any type:
   i. to respond to the Customer's requests at a pre-contractual stage,
   ii. to assess the credit risk that the Bank is called upon to undertake or has already undertaken,
   iii. to monitor the development of the relevant contract and the debt, and to pursue the collection of any amounts owed to the Bank in case the Customer has defaulted on his/her contractual obligations, an obligation of the Bank under the applicable legal framework and the regulatory decisions of the supervisory authorities, as well as towards the Bank's clients and shareholders,
   iv. for the management of any claim arising from loan agreements,
   v. for the prevention and suppression of money laundering and terrorist financing,

   (The processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract (article 6 paragraph 1b GDPR), as well as for the compliance with a legal obligation to which the Controller is subject (e.g., Law 4557/2018 as applicable) (article 6 paragraph 1c GDPR) and for the purposes of the legitimate interests pursued by the controller (article 6 paragraph 1f GDPR)).

c) Data from the execution of **payment transactions** (under I, **h**) for their completion, the prevention and suppression of money laundering and terrorist financing, the prevention of fraud against the Bank, its Group companies or the Customers, as well as of any other illegal transaction. (The processing is necessary for the compliance with a legal obligation to which the Controller is subject (e.g., Law 4557/2018 as applicable) (article 6 paragraph 1c GDPR) and for the purposes of the legitimate interests pursued by the controller (article 6 paragraph 1f GDPR)).

d) Data on the **Customer's knowledge and experience in the investment sector or in the insurance sector** (under I, **i**) to provide him/her with investment or insurance products or services upon his/her request. (The processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract (article 6 paragraph 1b GDPR), as well as for the compliance with a legal obligation to which the controller is subject (e.g., MiFID II Directive, as applicable) (article 6 paragraph 1c GDPR)).

e) Data of **contracts with companies for the acceptance of cards (acquiring) that have been terminated** (under I, **j**) for the prevention of fraudulent, improper or illegal transactions and the protection of the card payment systems ((The processing is necessary for the compliance with a legal obligation to which the controller is subject (Decision of the Data Protection Authority 6/2006) (article 6 paragraph 1c GDPR), as well as for the purposes of the legitimate interests pursued by the controller (article 6 paragraph 1f GDPR)).

f) **Recognition data of the Customer's identity** (under I, **k** above) for the prevention of fraud, the protection against malware, DDoS attacks against the Bank, its Group companies, or the Bank's Customers, as well as against any other illegal act, including cases of phishing. (The processing is necessary for the compliance with a legal obligation to which the controller is subject (article 6 paragraph 1c GDPR), as well as for the purposes of the legitimate interests pursued by the controller (article 6 paragraph 1f GDPR)) .

g) **Health data** (under I, **l**) to support any request that the Customer has submitted (such as, indicatively, the request for the restructuring of his/her debts due to inability to pay due to health factors) and its assessment by the Bank. (The processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract (article 6 paragraph 1b GDPR)).

h) Data on the Customer's **telephone communications or videoconferences** with the Bank (under I, **m**) to prove the conclusion and operation of the contract and of the transactions, as well as their security (The processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract (article 6 paragraph 1b GDPR)).

i) **Image** data (under I, **n**) for the protection of the property, the safety and physical integrity of the Bank's employees, Customers and visitors. (The processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party (article 6 paragraph 1f GDPR)).

j) **Biometric data** (under I, **o**) for the remote electronic identification of the Customer and the conclusion of the contract. (The processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract (article 6 paragraph 1b GDPR), as well as for the compliance with a legal obligation to which the controller is subject (e.g., Law 4557/2018 as applicable) (article 6 paragraph 1c GDPR) and where applicable and required the processing is based on the Customer's consent (article 6 paragraph 1a GDPR)).

k) The **electronic signature** data (under I, **l**) for the issuance of the Qualified Certificate for Electronic Signature, for the signing of digital contracts concluded remotely by electronic means. (The processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract (article 6 paragraph 1b GDPR)).

In addition to the aforementioned, the Bank shall process the necessary data from the aforementioned on as the case may be:

- in order to comply with its obligations, imposed by the applicable legal, regulatory and supervisory framework, as well as the decisions of any public authorities or courts.
- in order to exercise its rights and protect its legal interests.

IV. Automated individual decision making - profiling

A. Profiling

The Bank shall create a profile of the Customer, using a combination of the data collected as described above, for the following purposes:

- For promotional purposes, provided that the Customer has given his/her consent to the Bank for this purpose (marketing profiling). In this context, the Bank processes personal data, such as that regarding the Customer's creditworthiness and transactional behavior.
- For the Customer's classification as a private or professional client in accordance with the relevant legal framework for investments (indicatively: Directive 2014/65/EU (MiFID II) which was transposed into Greek law by Law 4514/2018) and the assessment of the Customer's suitability and compatibility for the provision of investment services/products. In this context, the Bank processes the Customer's personal data, such as his/her knowledge and experience in the investment sector.
- To assess the risk of money laundering and terrorist financing. In this context, the Bank processes data such as identification data, financial and property data, and data from the execution of transaction payments.

B. Automated individual decision making

The Bank may proceed with decisions based on automated individual decision making, which may include the credit profiling of the Customer, in accordance with Article 22 of the GDPR, for the purpose of assessing the credit risk in cases of approval or rejection of an application for a loan or credit, of an application for a credit limit increase, of an application for debt adjustment, etc., (necessary for the conclusion or execution of the Customer's contract with the Bank), after the processing of the Customer's financial and property data, as well as of the data on the breach of his/her financial obligations, on his/her creditworthiness, on his/her transactional behavior and on his/her credit scoring.

In any case, the Customer has the right to object to the automated decision making and to request the review of a rejected request with human intervention in accordance with the provisions of Section VIII below.

V. Who are the recipients of the Customer's personal data?

a) **Bank employees** who are responsible for handling any requests the Customer has submitted to the Bank for the provision of products or/and services, as well as for the management and operation of the Customer's contract(s) with the Bank in order to fulfill the obligations arising therefrom and the relevant obligations imposed by law. Bank employees shall in any case abide by the legal framework, including bank secrecy laws.

b) **Natural and legal persons** to which the Bank assigns the execution of specific tasks on its behalf, provided that the professional secrecy and the obligation for discretion and confidentiality are respected in all cases, such as, amongst others, the following companies:

- debt information companies (L. 3758/2009)
- loan service provider companies (L. 4354/2015),
- telephone support – information companies (call centers),
- consultancy service companies (e.g., technical, organizational, IT services, financial, etc.), experts, specialists,
- database management companies,
- risk management service companies,
- contact data tracing and asset tracing companies,
- file storage and management companies,
- market research, research of customer satisfaction, advertising, and product promotion companies on behalf of the Bank, provided that the Customer has given his/her explicit consent
- specialized payment service providers,

as well as

- lawyers, law firms, notaries and court bailiffs,
- accredited mediators of Law 4640/2019 and centers for the provision of mediation services (e.g., OMMED)
- providers of postal services,
- providers of development services, maintenance services, configuration of computer applications and of identification via video services,
- e-mail providers, web hosting service providers, including cloud services,
- natural or legal persons who process data for the purpose of updating them, including the updating of their contact details, in case the Bank has been notified for the relevant change,
- businesses participating in the Bank's customer loyalty or reward programs for the purpose of providing the Customers with the benefits from these programs.

c) **Credit and/or financial institutions** with registered seat in Greece or abroad, which have obtained the required operating license and operate legally, as well as companies or special purpose vehicles under the meaning of Law 3156/2003 on the securitization of claims, as applicable.

d) **Claim acquisition companies** under L. 4354/2015, as applicable, as well as entities in the wider financial sector, including domestic or foreign investment companies, in the event of the assignment of claims arising from loan agreements.

e) **Companies of the Alpha Bank Group**, for the purposes of assessing the overall risk assumed, of meeting regulatory obligations, of managing the companies in a uniform manner and of servicing the Customer.

f) **Credit institutions and payment service providers or entities** with registered seat in Greece or abroad, which have obtained the required operating license and operate legally, to execute a contract or transactions (such as SWIFT, SEPA, VISA, MASTERCARD, DIAS S.A. etc.).

g) **Supervisory, auditing, independent, judicial, public prosecution and/or other authorities and entities** within the legal framework of their competencies, duties and authorities (e.g. the Bank of Greece, the Hellenic Capital Markets Commission).

h) **"TIRESIAS SA"** for data concerning the records maintained by it, such as bad cheques, unpaid bills of exchange at their maturity date, terminations of loan or credit agreements, loan and credit agreements and their development, as well as guarantee agreements.

i) **Co-financing or guarantee institutions**, as applicable, such as the European Investment Bank, the Hellenic Fund for Entrepreneurship and Development (TEKE), the European Investment Fund and the Greek State, etc.

j) **Investment, brokerage, receiving and transmitting of orders, and custody service providers** for the execution of the Customer's orders related to the aforementioned activities, and/or **insurance companies** and/or **insurance intermediaries** in the context of the execution of the Customer's orders for the provision of relevant products and/or services to him/her.

k) **Real estate management** or real estate investment companies.

l) **Qualified Trust Service Providers** in accordance with Regulation (EU) 910/2014 (eIDAS), as applicable, in the context of issuing a qualified electronic signature certificate.

m) **Audit firms**

n) Existing or potential **buyers** of all or part of the Bank's activities or assets (including its rights).

VI. Does the Bank transfer the Customer's personal data to third countries outside the EU or to an international organization?

The Bank may transfer the Customer's personal data to countries outside the EU (third countries) in the following cases:

a) The European Commission has decided that the specific third country or international organization ensures an adequate level of protection for the personal data.

b) Appropriate safeguards for the processing of personal data have been provided in accordance with the legal framework.

c) Standard contractual clauses have been signed.

d) The Customer has been specifically informed and has granted his/her explicit consent to the Bank for the transfer of his/her data, and any additional requirements of the legal framework have been met.

e) The transfer is required for the execution of a contract, such as where the transmission is necessary for the execution of payment orders to a bank account of a financial institution in a third country, or in the event of transmission for the execution of an order for the conclusion of transactions with financial instruments.

f) The transfer is necessary for the establishment, exercise or defense of the Bank's legal claims or rights.

g) The Bank has a relevant obligation arising from a legal provision, an intergovernmental or international agreement, or

h) In line with the Bank's compliance obligations with the rules on the automatic exchange of information in the field of taxation, as they arise from legal and regulatory provisions (e.g. FATCA, CRS).

For the fulfillment of the obligations under **e** and **f** above, the Bank may transfer the Customer's personal data to competent national authorities for them to forward the data to the respective authorities of third countries.

VII. What is the retention period of the Customer's data?

a) If the Customer enters into a contract with the Bank, the latter retains his/her personal data until the statutory time limit for the general waiver of claims, i.e., for a time period of up to twenty (20) years from the termination of the relevant contract in any way, and the full repayment of any financial obligations towards the Bank.
b) If the Customer does not enter into a contract with the Bank, his/her personal data will be kept for five (5) years (statutory time limit for commercial claims), upon submission of the relevant request, either through the Bank's Branch Network or through any other electronic medium made available by the Bank.

If there are any ongoing legal proceedings with the Bank or any affiliated company thereof, by the end of the retention periods mentioned above under (a) and (b), which concern the Customer, either directly or indirectly, the said retention periods of the personal data shall be extended until the issuance of an irrevocable court judgement.

The retention period shall be completed at the end of the year during which the statutory time limit shall lapse.

In case the law or regulatory acts provide for a smaller or greater retention period, the aforementioned retention periods will be decreased or increased accordingly.

Paper documents that bear the Customer's signature and his/her personal data, may be kept in electronic/digital form after the lapse of five (5) years, at the Bank's discretion.

VIII. What rights does the Customer have for the protection of his/her data?

The Customer has the following rights:

a) To know which personal data that concerns him/her is kept and processed by the Bank, as well as its source (right of access).
b) To request the rectification and/or supplementation of his/her personal data, so that it is complete and accurate by presenting any necessary documents which prove the need for such rectification or supplementation (right to rectification), which constitutes an obligation of the Customer at the same time.
c) To request the restriction of the processing of his/her personal data (right to restriction).
d) To refuse and/or object to any additional processing of his/her personal data kept by the Bank (right to object).
e) To request the erasure of his/her personal data, from the Bank's records (right to erasure).
f) To request from the Bank to transmit the data he/she has submitted thereto to any other data controller (right to data portability).
g) To revoke his/her consent, if he/she has given it in those cases that constitute a legal basis for the processing of personal data.
h) In cases of automated individual decision making, according to the aforementioned in Section IV, to request the review of his/her rejected request with human intervention.

It is noted that the fulfillment of the Customer's requests under c, d and e above, if they concern personal data necessary for the execution or the continuation of the operation of the contract, regardless of their source, entails the automatic termination of the respective contract/contracts from the Customer's part, pursuant to the terms thereof or the inability to review the Customer's request.

In addition, the Bank has the right in any case to refuse to fulfill the Customer's right to restriction of processing or erasure of his/her personal data if the processing or retention of his/her personal data is necessary for the establishment or exercise or support of its legitimate interest, lawful rights or its compliance with its legal obligations, according to the aforementioned under III.

The exercise of the Customer's right to data portability (under f above) does not entail the erasure of his/her personal data from the Bank's records, which is subject to the preceding paragraph. The exercise of the aforementioned rights acts for the future and does not concern the processing of personal data which has already been carried out.

The Customer has the right to file a complaint with the Hellenic Data Protection Authority (www.dpa.gr), which is the competent supervisory authority for the protection of the fundamental rights and freedoms of natural persons, against the processing which concerns him/her, if he/she believes that his/her rights are being infringed in any way.

IX. How can the Customer exercise his/her rights under VIII above?

For the exercise of the Customer's rights under VIII above, the Customer may contact the Bank through the following channels:

- the Bank's Branch Network, by filling in and submitting the "Exercise of Rights" Form
- By telephone, calling the number 210 326 0000
- Electronically on the Bank's website www.alpha.gr, by filling the contact form
- Via e-mail on SpecializedCustomerServicesUnit@alpha.gr

Additionally, the Customer may print the Exercise of Rights Form through the Bank's website www.alpha.gr and send the completed form via post mail to:

Alpha Bank
Customer Service Department
Specialized Customer Services Unit
276 Messoghion Avenue GR-155 62 CHOLARGOS

The Bank shall make its best efforts to respond to the Customer's request within thirty (30) days from its submission. This deadline may be extended by sixty (60) further days, provided that it is necessary, at the Bank's discretion, taking into account the complexity of the request and the number of requests. The Bank shall inform the Customer, in any case of extension of the deadline of thirty (30) days, within thirty (30) days from receipt of the request, as well as for the reasons of the extension.

If the Bank does not act on the Customer's request, it shall inform him/her without delay no later than thirty (30) days from receipt of the request, of the reasons for which it was unable to act on the request and of the Customer's right to file a complaint and take legal action.

The above service is provided by the Bank free of charge. However, if the Customer's requests are manifestly unfounded, excessive, or repetitive, the Bank may either charge a reasonable fee, informing the Customer thereof or refuse to respond to his/her request/s.

X. How are the Customer's rights protected?

The Bank implements an information security management system for the safeguarding of the Customer's privacy, the security of the processing of the Customers' personal data and their protection from accidental or illegitimate destruction, leak, alteration, prohibited dissemination or access, as well as any other illegitimate form of processing.

The aforementioned notice of the Customer is made in accordance with the Regulation (EU) 2016/679 of the European Parliament and of the European Council and with the provisions of Greek law on the protection of personal data adopted and implemented in this context, replacing any previous notice made under Law 2472/1997, which may be mentioned in contractual or other documents of the Bank.

B. CONTACT DETAILS

I) CONTROLLER:
ALPHA BANK
ADDRESS: 40 Stadiou Street, 102 52 Athens CONTACT
TELEPHONE NUMBER: +30 210 326 0000

II) DATA PROTECTION OFFICER:
ALPHA BANK
DATA PROTECTION OFFICER
ADDRESS: 105 Athinon Avenue, 104 47 Athens
CONTACT TELEPHONE: +30 210 326 6953
Email: contact-DPO@alpha.gr