PRIVACY NOTICE

I. Information on Personal Data Processing

Introduction

We would like to assure you that for AEGEAN BALTIC BANK S.A. (hereinafter referred to as "AEGEAN BALTIC BANK" or the "Bank") the personal data protection of our existing or/and potential customers, persons with whom we have any type of contractual relationship (such as for instance partners, suppliers, shareholders or any other third parties on a case-by-case basis, as mentioned below) is of paramount importance. For this reason, we are taking appropriate measures to protect the personal data we process and ensure that the processing of personal data is always carried out in accordance with the obligations laid down by the legal framework, both by the company itself and by third parties who process personal data on behalf of the company.

Data Controller – Data Protection Officer (DPO)

AEGEAN BALTIC BANK, having its registered office at Amarousio, at 91 Megalou Alexandrou & 25 Martiou streets, postal code 151 24, with Tax Identification Number 099937684, email: aegean.baltic@ab-bank.com, tel: (+30) 210-6234110 website: https://aegeanbalticbank.com, informs that, for the purposes of its business, it processes personal data of its potential or/and existing customers or/and any persons with whom the Bank may have a contractual relationship in general, in accordance with the applicable national law and the European Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, hereinafter referred to as the "Regulation") as it is currently in force.

The Data Protection Officer directly (DPO) of the Bank is the law firm PISTIOLIS - TRIANTAFYLLOS & ASSOCIATES LAW FIRM – ANDERSEN LEGAL (contact details: dpo@ab-bank.com).

Which categories of personal data do we process?

Your personal data that we collect and process are the absolutely necessary, required and appropriate to achieve our objectives and are summarized as follows. The personal data collected to achieve such objectives are divided into the following two categories:

A. Personal data that you provide us, such as:

· Identification and legalization data (name and surname, date and place of birth, identity

card and passport details, Social Security Registration Number on case-by-case basis);
· Demographic data (gender, nationality and family status);
· Contact details (address, landline or mobile phone number, e-mail address);
· Data regarding your financial status and assets, (i.e. bank account information) including tax information (Tax Identification Number, tax residence, information regarding payroll and assets, profession, remuneration, dependents, tax assessments, as the case may be, E1, E2 and E9 forms);
· Image data, extracted from the video surveillance systems of the Bank's premises, where there are relevant signs;
● Data from your connection to the Bank's electronic applications, such as e-banking, in accordance with the specific privacy notice provided to this respect.
· Data from your transactions with the Bank and the use of the products or services offered by the Bank.
● Data that are declared on an obligatory basis by the linked with the Bank parties, in accordance with the provisions of the Governor's Act No 2651/2012, such as indicatively when someone is shareholder of the Bank as provided by the specific conditions of the respective declarations, or controls by virtue of par. 34, article 3 of the L. 4261/2014 directly or indirectly legal persons, or has close links with the Bank in accordance with par. 35 of article 3 of the aforementioned law and par. 1 (38) of article 4 of the EU Regulation 575/2013.

We note that the data relating to your identification and legalization, as well as your contact details, are the absolutely necessary for your transactions or contractual relationships with the Bank, while the nature and the volume of the other data depends, in any case, on the contract with the Bank, either the existing one or the one that will be concluded and/or the offered product or service.

B. Personal data collected by the Bank from other sources and which are the following:

· Data regarding the breach of your financial obligations, such as, indicatively and as the case may be, uncovered checks, unpaid (upon expiration) bills of exchange and promissory notes, termination of contracts in respect of all types of loans and credits to natural persons and companies, payment orders, auctions (of moveable and immoveable property), seizures and checks for payment based on Presidential Decree 1923, the turn of a prenotation of mortgage into a mortgage, administrative penalties imposed on tax offenders, claims and conciliation / reorganisation decisions, bankruptcy petitions, declared bankruptcies and decisions rejecting bankruptcy claims due to inadequacy of the debtor's property, petitions and decisions regarding the judicial debts settlement and orders for the restitution of the use of immoveable property);
· Companies' data (such as Articles of Association, Board of Directors' members, representation) from the websites of Government Gazette and General Commercial Registry (GEMI);
● Data that are collected in the due diligence context or sanctions' monitoring or violations of the legal and regulatory framework on the prevention of money

laundering;

- Data that are transferred by supervisory, judicial and other public and independent authorities relating to offences, imposition of measures safeguarding Public's interest, garnishments, sequestrations and commitments;
- Financial data assessing your investment and financial situation and behavior;
- Data from the use of electronic and / or digital products and services of our Bank (e.g. IDs cookies), in accordance with their specific terms.
- Data of third parties, for instance relatives of the employees/members of the Bank's Board of Directors that may arise from the declarations of the aforementioned as submitted within the framework of the Conflict-of-Interest Policy that the Bank implements in the context of its regulatory obligations.

Sources of Data

In the event that the Bank collects personal data from other sources and has not collected them from you as data subject, for the purpose of fulfilment of its legitimate interests in respect of the protection of the transactions reliability and the adoption of appropriate pre-contractual measures with prospective clients or the performance of the contract with partners/suppliers, it is likely that, as the case may be, the Bank may seek the relevant data from other sources, such as Tiresias, ICAP or other online applications or public sources such as the General Commercial Registry (GEMI), the Government Gazette, Land Registries and Cadastres and if applicable, the Internet or the employees/ members of the Bank's Board of Directors for potential data of their relatives that may arise within the context of Conflict-of-Interest Policy declarations.

In case of omnibus accounts, opened and held with the Bank by institutions in their own name for the account of third parties/beneficiaries, the Bank also collects personal data (such as name, surname, father's name and cell phone number) of the beneficiaries of such omnibus accounts directly from the institutions/account holders and/or collaborating platforms (offering the Bank's deposit products to residents of foreign jurisdictions). The collection of such personal data is required by the Hellenic Deposit and Investment Guarantee Fund (TEKE) in order to ensure the protection of deposits in accordance with the applicable deposit guarantee scheme of TEKE.
The personal data processed by the Bank are kept in written form or/and by electronic means.

We note that in respect of the personal data collected directly from you in your capacity as clients, you must inform us for any change of your data without undue delay, as well as respond to any Bank's request for their relevant update (please see below in respect of the right to rectification); otherwise the Bank has the right to seek them in any lawful manner.

How and why we use your personal data?

· For the offer of our products and services, the fulfilment and in general the smooth operation in order to meet our obligations towards you

We collect personal data e.g. when we open bank deposit accounts, when we use the information required to manage your accounts, for the processing of your transactions, for the exchange of bank notes, for the management of remittances, for the management of bank safe deposit boxes, for the acceptance of debt restructuring requests, and in general for the provision of our products and services, in order to perform our contractual relationship with you, under your customer or partner/supplier status as the case may be.

· **For our communication with you and the management of our relationship with you**
We may need to contact you by email or phone for administrative purposes and in general, for the offer of our services.

· **For keeping you up-to-date with our news and offers**
When this is covered by our legitimate interest or our contractual relationship, we will send you promotional messages about our banking services, updates, products and offers, sometimes personalized to your preferences and interests, to improve your customer experience.

· **For the amelioration of our services and the protection of our business interests**
The business purposes for which we will use your information help us improve our services and meet your expectations.

· **For the support of banking operations**
We process your personal data in order to handle complaints, terminate business relationships and in general to ensure the unimpeded provision of our banking services.

· **For the prevention of criminal acts and the compliance with legal obligations**
We process your personal data to conduct customer due diligence, transaction and name authentication checks, banknote authentication & suitability checks, risk identification and, in general, the implementation of measures to prevent and detect criminal offenses such as fraud, terrorism and money laundering, as well as other legal obligations arising from our legislative and regulatory framework governing our operation (such as for instance in the context of the mandatory automated information exchange in the fiscal sector, the Law 4261/2014 as in force), the acts of the Governor of the Bank of Greece which is our supervisory Authority, such as indicatively the Act No 2651/2012 and the Code of Civil Procedure. In the same context, we use systems for the identification of our customers and the transactions executed by them, and their processing, on the basis of relevant models, by conducting checks into international lists of politically exposed persons or imposition of sanctions in order to investigate suspicious or unusual transactions for the prevention of illegal activities.

· **For the safeguard of our legitimate interests and the protection of individuals and goods, as well as for the reliability and safety of transactions, such as the**

management of financial and credit risk of the Bank
When we use closed circuit television (CCTV) and security cameras to be able to protect the security of individuals, materials, facilities, including your deposits, when we conduct checks to certain financial data, as mentioned above in the context of our banking activity, in order to manage our credit risk.

· For the provision of access to our online platform
We process your personal data in order to provide access to our online platform.

Which are the legal grounds for processing our personal data?
The personal data you provide us are processed only when we have legal grounds to do so.

Legal grounds for processing your personal data are:
(a) your consent under the conditions set by the legislative framework and where it is required;

(b) the necessity of the processing of your data in the context of the fulfilment of our contractual obligations or during the pre-contractual stage upon your request for the provision of our services;

(c) the safeguarding and protection of our legitimate interests, which may entail the security of persons and facilities through the use of CCTV; the security of the network and the operation of banking applications; the IT support, the establishment, exercise and defense of legal claims; the organization and development of the business activity; the reliability and security of transactions; as well as the marketing executed on a B2B level.

(d) the compliance with a statutory obligation, which may entail in particular labor and tax law, including the applicable legislation within the framework of mandatory automatic exchange of information in the tax area for the prevention of tax evasion (including the obligation of information submission on cross-border transactions potentially bearing an aggressive tax design), the legislation governing our operation as a credit institution and societe anonyme, the provisions of the Code of Civil Procedure, the individual Acts of the Governor of the Bank of Greece, the Committee of Bank and Credit Issues & the Executive Committee of the Bank of Greece, as well as the legislation for the prevention and combating of money laundering and terrorism financing, along with the implementation of the legislative and regulatory framework on payment services (PSD II) and on markets in financial instruments (MiFiD II).

(e) the necessity of the processing of your personal data in the context of the performance of a duty performed in the public interest, such as, for example, for the execution of a prosecutor's order or upon implementation of measures aiming at preventing money laundering and terrorism financing;

(f) the manifest disclosure of your personal data on your own initiative of special

categories of personal data, as the case may be.

(g)the public interest by virtue of European Union's law and Law 4261/2014 on access to the activity of credit institutions and precautionary supervision of credit institutions that has transposed Directive 2013/36, the provisions of which are specified and supplemented by the Guidelines on internal governance of the European Banking Authority. This legal basis justifies the processing of special categories of personal data of third parties, if any, that may arise upon submission of the relevant declarations of the employees/ members of the Board of Directors of the Bank within the context of the Conflict-of-Interest Policy that is implemented by virtue of the aforementioned. The political relations or influences of the personnel (that may include simple or special categories of personal data of their relatives, as the case may be) are indicative examples.

Where do we disclose your data?

Aegean Baltic Bank informs you that it shares your personal data with the following indicative categories of recipients:

· **Bank's Employees**

To the Bank's employees, who are responsible for the evaluation of your requests, the management and the operation of your contract with the Bank, as the case may be, the fulfilment of the obligations arising therefrom, as well as the relevant obligations imposed by the law. Your personal data are treated in the strictest confidence and confidentiality, since the employees who process your personal data have an adequate and sufficient level of knowledge for their protection and are bound by confidentiality clauses or are under a statutory obligation of confidentiality.

· **Governmental authorities, Law enforcement agencies in the context of the exercise of their competences, supervisory authorities of credit institutions, such as the Bank of Greece, the European Central Bank, the Single Supervisory Mechanism**

We may share your information with the relevant services, law enforcement agencies and other third parties where the law permits us to do so, for the purpose of preventing or detecting criminal offenses, executing confidentiality lifting orders – provision of customer accounts details and orders on seizing of accounts and safety deposit boxes etc. It is noted that according to law 4170/2013 on Administrative Cooperation in the tax sector, as amended, amongst others by laws 4378/2016[1] and 4714/2020[2] and is currently in force, along with the law 4428/2016[3] and law 4493/2017[4] as in force, we are required to collect

[1] On mandatory automatic information exchange in the tax sector - DAC 2.

[2] On mandatory automatic information exchange in the tax sector with respect to declared cross-border arrangements - DAC6

[3] On validation of the multilateral agreement of the competent authorities on automatic information exchange on financial accounts of the Organization for Economic Co-operation and Development (CRS).

[4] On validation of the Memorandum of Understanding and Agreement of the Hellenic Republic and the

and transfer to the competent authority of the Ministry of Finance personal data of our customers (or/and any third parties included in the transaction in the case of the declared cross-borders arrangements) for further transfer to the competent participating tax authorities abroad.

· **Other banking institutions and/or companies/organizations which are payment services & payment processing providers, (such as DIAS, SWIFT, VISA etc.), to Tiresias**

Providing information to other banking institutions e.g. for the performance of a contract or a transaction that you requested, as the case may be.

Furthermore, and in accordance with the Law 4537/2018[5] we might disclose details of a customer, common with another banking institution, to the banking institution that submits the relevant request, following the request submitted by the common customer. In case of bounced checks the Bank is required to proceed with the relevant announcement to Tiresias.

· **When outsourcing to external partners (natural and legal persons where the Bank assigns certain tasks on its behalf)**

It is likely that your data are disclosed to our external partners (natural and legal persons where the Bank assigns certain tasks or the provision of certain services on its behalf) in order for the partners to perform the tasks or/and provide their services on behalf of the Bank or individually in the cooperation context with the latter, as the case may be (i.e information systems supply, support and security companies, companies of safe record -keeping and destruction of files, companies providing email services, internet hosting services providers, consulting services companies, including financial and audit consultants of the Bank, debit cards, electronic transactions and e-banking support services. Furthermore, upon initiation of our contractual relationship or for the performance of the contract or for the collection of your debts towards the Bank in case of non-fulfillment of the obligations you have undertaken by means of the contract concluded with the Bank, your details might be transferred to external partners of the Bank (i.e. cooperating lawyers or law firms, bailiffs, notaries, engineers and assessors).

· **To bodies co-financing or providing guarantees, domestic or foreign, such as the Hellenic Deposit and Investment Guarantee Fund (TEKE), the Greek State etc.**

Transferring your personal data to Third Countries

Your personal data may be transmitted and stored in locations outside the European Union (EU) or the European Economic Area (EEA), including countries which may not have the

---

USA Government for the improvement of international tax compliance and the implementation of the law on tax compliance of accounts held abroad (Foreign Account Tax Compliance Act, FATCA).

[5] On Payment services (Direct.2015/2366/EU) and other provisions

same level of protection for personal information. Reasons for the transfer of your personal data may be the existing safeguards per recipient, such as an adequacy decision issued by the European Commission or standard contractual clauses, as approved by the European Commission and are in force. In the absence of such safeguards, the transfer may be based on a specific derogation in accordance with the requirements of the Regulation, such as the necessity of the transfer for the execution of a contract between the Bank and the data subject. In addition, personal data may be transferred when necessary for the establishment, exercise or defense of legal claims or when the transfer is required on the basis of a judgment issued by a court or administrative authority or on the basis of an international agreement or the legal interests of the Bank by way of derogation. In any case, we ensure that there is an appropriate protection level, and that the transfer is lawful.

Storage Time

The data storage time is decided on the basis of the following specific criteria, as appropriate in each case:

When processing is required as an obligation under provisions of the applicable legal framework, your personal data will be stored for as long as required by the relevant provisions.

When processing takes place on the basis of a contractual relationship, your personal data will be stored for as long as it is necessary to perform the contract and for the establishment, exercise, and / or support of legal claims under the contract.

For promotional and marketing purposes, your personal data is retained until you oppose to the processing. This can be done by you at any time.

What are your rights with respect to your personal data?
Any natural person whose data is being processed by Aegean Baltic Bank enjoys the following rights:

- **Right of Access:**

You have the right to be aware and verify the legitimacy of the processing. So, you have the right to access the data and get additional information about how your date is processed.

- **Right to Rectification:**

You have the right to study, rectify, update or amend your personal data by contacting the Data Protection Officer (DPO) at the above contact details by submitting relevant documentation.

- **Right to Erasure ("Right to be forgotten"):**

You have the right to request the erasure of your personal data when we process them

based on your consent or in order to protect our legitimate interests. In all other cases (such as, for example, where there is a contract, due to an obligation to process personal data as required by law or for reasons of public interest), this right is subject to specific restrictions or may not apply, depending on the case.

- **Right to Restriction of Processing:**

You have the right to request a restriction on the processing of your personal data in the following cases: (a) when the accuracy of the personal data is questioned and until such accuracy is verified; (b) when you oppose the erasure of personal data and request (instead of erasure) the limitation of its use; c) when personal data is not needed for processing purposes, but is, however, indispensable for the establishment, exercise and support of legal claims; and (d) when you object to the processing and until it is verified that there are legitimate reasons that concern us and supersede the reasons for which you oppose processing.

- **Right to Oppose Processing:**

You have the right to oppose at any time the processing of your personal data where, as described above, such processing is necessary for the purposes of legitimate interests we seek as data controllers, as well as for processing for direct marketing and consumer profiling.

- **Right to Data Portability:**

You have the right to receive your personal data free of charge in a format that allows you to access, use, and edit it, using commonly used editing methods. You also have the right to ask us, if technically feasible, to pass the data directly to another data controller. This right exists for the data you have provided to us and is processed by automated means based on your consent or for the performance of a relevant contract.

- **Right to Withdraw Consent**

Where processing is based on your consent, you have the right to withdraw such consent freely, without prejudice to the lawfulness of the processing based on your consent prior to its withdrawal.

Process for the exercise of the aforementioned rights

In order to exercise any of the above-mentioned rights you may refer to the Data Protection Officer (DPO) through the following contact channels:

1. by sending a relevant written request to the address of the Bank's head office at 91 Megalou Alexandrou & 25 Martiou str., PC 15124, Marousi;

2. by sending a relevant written request to the Bank's e-mail address dpo@ab-bank.com;

3. in person, by completing and submitting a request form at a Bank's branch.

You must provide us with the following details with your request: name and surname, address of residence, Tax Identification Number or Identity Card Number, e-mail address, date and subject of the request. In any case, for your convenience, the Bank makes available at its branches request forms in case you wish to submit a relevant request for the exercise of your rights.

We will use our best endeavours to reply within thirty (30) days from the submission of the above requests. The said timeline may be extended by sixty (60) days, if deemed necessary, taking into account the complexity of the request and the number of the submitted requests, in which case we will inform you accordingly within the aforementioned thirty-day period.

Right to file a complaint with the Data Protection Authority

You have the right to file a complaint with the Hellenic Data Protection Authority (www.dpa.gr) through its portal https://eservices.dpa.gr/ upon filling the relevant electronic form, depending on the type of complaint.

Personal Data Security

Aegean Baltic Bank implements appropriate technical and organizational measures aimed at the safe processing of personal data and the prevention of accidental loss or destruction and unauthorized or/and unlawful access to, use, modification or disclosure thereof. In any case, the way in which the internet operates and the fact that it is free to anyone cannot guarantee that unauthorized third parties will never be able to violate the applicable technical and organizational measures by gaining access and possibly using personal data for unauthorized and / or unfair purposes.

Profiling – Automated decision-making process

AEGEAN BALTIC BANK does not take decisions based exclusively on automated processing of personal data. It may, however, proceed to profiling [any form of automated processing of personal data that involves the use of personal data to evaluate certain personal aspects of a natural person, in particular to analyze or predict aspects of personal preferences and interests or movements] -not always automated- without taking, though, an automated decision based on such profile, since no decisions are taken without human intervention.

The aforementioned profiling is performed in the context of Know Your Customer diligences in accordance with the regulatory framework upon account opening and customer management, aiming at preventing money laundering from criminal activities and terrorism financing, in the context of budget details on the basis of customers' financial analysis, the assessment and management of the Bank's credit risk, along with any financial risks, the credit control of personal guarantors, using amongst others black list details as provided by TIRESIAS. Furthermore, card transaction assessment is

conducted in the context of preventing fraud or malicious acts against the cards (anti-fraud monitoring).

II. Specific Information on data processing via video surveillance system

Data Controller – Data Protection Officer (DPO)

AEGEAN BALTIC BANK (hereinafter the "Bank"), having its registered office at Amarousio, at 91 Megalou Alexandrou & 25 Martiou streets, postal code 151 24, with Tax Identification Number 099937684, which mainly provides banking services, email: aegean.baltic@abbank.com, tel: (+30) 210-6234110, website: https://aegeanbalticbank.com.

The Data Protection Officer directly (DPO) of the Bank is the law firm PISTIOLIS - TRIANTAFYLLOS & ASSOCIATES LAW FIRM – ANDERSEN LEGAL (contact details: dpo@ab-bank.com).

Purposes and legal basis of the processing

We use video surveillance system for the purpose of protection of the persons and the goods at our premises. The processing is required for the legitimate interests that we pursue as a Data Controller (article 6 par. 1 of the GDPR).

Analysis of the legitimate interests

Our legitimate interest is based on our need to protect our premises and the goods that are placed therein from illegal acts, such as, indicatively, thefts. It further extends to our need to safeguard the life, the physical integrity, the health as well as the property of our staff and third parties who are lawfully located in the supervised area. We collect solely images and restrict the reception of images to places where we have assessed that there is an increased possibility of committing illegal acts e.g. theft, such as to the Bank's cashiers and the Bank's entrance, without focusing on places where privacy of the data subjects, from whom we collect the images, may be severely restricted, including their right to respect their personal data.

Recipients

The material that we keep is accessible only by the Bank's competent/ authorized personnel, who is charge of the safety of the premises. This material is not transferred to third parties, without the data subject's consent, with the following exceptions: a) to competent judicial, prosecution and police authorities, to the extent that it includes data necessary for the investigation of a criminal offence relating to persons or goods of the Bank, b) to competent judicial, prosecution and police authorities when they request data lawfully in the performance of their duties and c) to the victim or the offender, when such data may constitute evidence of the act.

Storage time

We keep the data for sixteen (16) calendar days in the Branches of Glyfada and Piraeus and for eighteen (18) days in the Branch of Amarousion. Following the lapse of this period, they are automatically erased. In the event that during such period an incident comes to our attention, we isolate part of the video and keep it for one (1) month more in order to investigate the incident and commence legal proceedings for the defense of our legitimate interests, while in the event that the incident concerns a third party, we shall keep the video for three (3) more months. If, during the period of sixteen calendar days, incidents of organized financial fraud or financial transaction dispute are recorded, the relevant parts of the data extracted from the video surveillance system may be kept in a separate file with appropriate security measures for as long as necessary for the investigation or the initiation of disciplinary or judicial proceedings in relation to such incidents.

Rights of the data subjects

The data subjects have the following rights:
· Right of access: you have the right to be informed whether we process your image and, if applicable, to request a copy thereof;
· Right to restriction of processing: you have the right to request the restriction of the processing, such as, for example, not to erase data that you consider necessary for the establishment, exercise or support of your legal claims;
· Right to object: you have the right to object to the processing;
· Right to erasure: you have the right to request the erasure of your personal data.

You may exercise your rights by sending an e-mail to the e-mail address dpo@ab-bank.com or a letter to the address of our registered seat or by submitting in person a request at the Bank's branches. In order to consider a request relating to your image, you should inform us about when you were within range of the cameras and give us a picture of you to make it easier for us to trace your data and hide the data of third parties' images. Alternatively, we give you the opportunity to visit our facilities and we will show you the images in which you appear. It is also noted that the exercise of the right to object or erasure does not result in the immediate erasure of your data or the change of the processing. In any case, we will respond to you in detail as soon as possible, within the time-limits provided for by the GDPR.

Right to file a complaint

In case you consider that the processing of your personal data violates Regulation (EU) 2016/679, you have the right to file a complaint to the supervisory authority.
Competent supervisory authority in Greece is the Hellenic Data Protection Authority, through its portal https://eservices.dpa.gr/, where one can fill the respective electronic form depending on the complaint type.

III. Amendments to the Privacy Policy

The information in relation to the privacy policy reflects the current situation of the data processing. In case of changes in the data processing, such information on data protection will be updated accordingly. The most recent version of such information on data protection will be always available on our website, thus permitting you to be informed on the scope of the data processing. We recommend that you keep informed on the way we process and protect your personal data. All future changes regarding this Privacy Notice will be available on our website.

November 2023