



PRIVACY NOTICE

Update 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 protection of our customers' personal data is of paramount importance. For this reason, we are taking appropriate steps 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 Amarusio, at 91 Megalou Alexandrou & 25 Martiou streets, 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 customers in accordance with 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.

For any matter concerning the processing of personal data, please contact the Data Protection Officer directly (DPO), email: [e-mail: dpo@ab-bank.com](mailto:dpo@ab-bank.com), telephone: 210-6234110.

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);
- Demographic data (gender, nationality, family status);
- Contact details (address, landline or mobile phone number, e-mail address);



- Data regarding the financial status and assets, including tax information (Tax Identification Number, tax residence, information regarding payroll and assets, profession, remuneration, dependents, tax assessments, as the case may be, E1 and E9 forms);
- Image data, extracted from the video surveillance systems of the Bank's premises, where there are relevant labels;
- Data from your transactions with the Bank and the use of the products or services offered by the Bank.

We note that the data relating to your identification and legalization, as well as your contact details, are 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 individuals and companies, payment orders, auctions (of moveable and immovable 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 immovable property);
- Companies' data from the Government Gazette and the General Commercial Registry (GEMI);
- Data from the use of electronic and / or digital products and services of our Bank (e.g. cookies IDs), in accordance with their specific terms.

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, it is likely that, as the case may be, the Bank may seek the relevant financial data from other sources, such as Tiresias Risk



Checking System or other public sources such as the General Commercial Registry (GEMI), from Government Gazette issues and, if applicable, from the Internet.

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 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 for the fulfilment of 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.

- **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**

If you have consented to or are covered by our legitimate interest, 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 diagnostics checks, name authentication and banknote authentication 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 corporate framework, the acts of the Governor of the Bank of Greece which is our supervisory authority and the Code of Civil Procedure. In the same context, we use systems for the identification of our clients and the transactions executed by them, as well as the processing of them, on the basis of relevant models, by conducting checks into international lists of political exposed persons or sanctions lists 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 the 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 transactions; the establishment, the exercise, the defense of



legal claims; the organization and the development of the business activity; the reliability and security of transactions; as well as the marketing executed on 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 the mandatory automatic exchange of information in the tax area for the prevention of tax evasion, 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, as well as the legislation for the prevention and combating of money laundering and terrorism financing;

(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;

(f) the manifest disclosure of your personal data on your own initiative or special categories of personal data, as the case may be.

Where do we share your data?

Aegean Baltic Bank informs you that it shares your personal data with the following 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 privacy lifting orders and orders on seizing of accounts and safety deposit boxes. It is noted that according to laws 4170/2013, 4428/2016 and 4493/2017, as applicable, we must collect and transmit personal data of



our clients to the competent authority of the Ministry of Finance in the context of the mandatory automatic exchange of information in the tax area for the prevention of tax evasion.

- **Other banking institutions and/or foreign payment services providers such as SWIFT , VISA etc.**

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

- **When outsourcing to external partners (lawyers, law firms, consulting companies, technical companies, etc.)**

It is likely that your data are disclosed to our external partners in order for the latter to take all the necessary actions for the legal handling of your case (these are special cases in which it is deemed necessary to have a qualified lawyer to handle the case) or to proceed with all necessary actions to make an assessment of the value of your real estate or a machine owned by you in your capacity as borrower or guarantor in relation to financing.

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

Furthermore, Aegean Baltic Bank may transmit your data to third-party associates for the purpose of sending promotional material and information about products, services, and offers, after ensuring the relevant legal basis for such process and the written assignment of processing, as mentioned hereinabove.

The Bank has lawfully ensured that the processors acting on its behalf fulfil the conditions and provide sufficient guarantees as to the implementation of appropriate technical and organizational measures in such a manner that the processing of your personal data ensures the protection of your rights.

Transferring your personal data to Third Countries

Your personal data may be transmitted and stored in locations outside the European Union (EEA) or the European Economic Area (EEA), including countries which may not have the same level of protection for personal information. Reasons for passing on your personal data may be the existing safeguards per recipient, such as an adequacy decision issued by the European Commission or standard data protection clauses, as approved by the European Commission and are in force. In the absence of such safeguards, the transmission may be based on a specific derogation in accordance with the requirements of the Regulation, such as the necessity of the transmission for the execution of a contract



between the Bank and the data subject or the latter's consent. In addition, personal data may be transmitted to third parties where necessary for the establishment, exercise or defense of legal claims or when the transmission is required on the basis of a judgment issued by a court or administrative authority or on the basis of an international agreement or on the basis of the legal interests of the Bank by exception. In any case, we ensure that there is an appropriate protection level and that the transmission 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 is done on the basis of a contractual relationship, your personal data will be stored for as long as is necessary to perform the contract and for the establishment, exercise, and / or defense of legal claims under the contract.

For promotional and marketing purposes, your personal data is retained until your consent is withdrawn. This can be done by you at any time. Withdrawal of consent does not affect the legality of consent-based processing for the period before its revocation.

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 data is processed.

Right to Rectification:

You have the right to study, correct, update or modify 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 it 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 required by law, for reasons of public interest), this right is subject to specific restrictions or and 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 reestablishment, exercise, defense 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 processors, 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 them, using commonly used editing methods. You also have the right to ask us, if technically feasible, to pass the data directly to another processor. 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.

In order to exercise any of the above-mentioned rights you may refer to the Data Protection Officer (DPO) by sending a relevant written request either to the Bank's e-mail address dpo@ab-bank.com or to the address of the Bank's head office at 91 Megalou Alexandrou & 25 Martiou.

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 requested, 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 the Hellenic Data Protection Authority (www.dpa.gr): Telephone: +30 210 6475600, Fax: +30 210 6475628, email: contact@dpa.gr

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 / or unauthorized 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

Profiling is defined as 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.

AEGEAN BALTIC BANK does not take decisions based exclusively on automated processing of personal data. It may, however, proceed to profiling – 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 for customer management purposes, provision of banking services, performance of regulatory obligations, risk assessment, management of partners and transactions safety. Indicative examples are the Know Your Customer check which is imposed by the regulatory framework, the preparation and the dispatch of reports to the competent regulatory authorities, cards reports, the assessment and the management of Bank's credit risk, as well as in general the financial risks.

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.

January 2020