

PRIVACY NOTICE

Last updated July 2020

This **privacy notice** provides an overview of how Hellenic Bank Public Company Ltd (the “**Bank**”) processes your personal data. “Personal data” refers to any information relating to you that the Bank obtains from you or other parties. The types of data processed and how they are used depends, largely, on the services you request from the Bank, or the Bank agrees to provide to you, from time to time.

In all cases, the processing of your personal data by the Bank must be in compliance with the provisions of applicable personal data protection law (including the EU General Data Protection Regulation or (“**GDPR**”), applicable as of 25 May 2018). The rights provided to you by the GDPR in relation to the processing of your personal data by the Bank are described in this notice.

Who is responsible for processing your personal data and who you can contact in this regard

Your personal data will be held by the Bank and responsibility for their processing lies with:

Hellenic Bank Public Company Limited, with Company Registration Number HE 6771, whose registered office is at Corner of Limassol and 200 Athalassas Avenues, 2025 Strovolos, P.O. Box 24747, 1394 Nicosia, Cyprus.

You can reach the Bank’s data protection officer at:

Hellenic Bank Public Company Limited 173, Athalassas Avenue, 2025 Strovolos, P.O. Box 24747, 1394 Nicosia, Cyprus.

E-mail: dataprotection@hellenicbank.com

How the Bank uses your personal data

This privacy notice is to let you know how the Bank processes your personal information. This includes information you give to the Bank about yourself, information that the Bank learns through its relationship with you and information about you that the Bank collects from other sources as explained below in *Where the Bank collects your personal data from*.

The Bank’s relationship with you will arise in any of the following ways:

- you are the Bank’s customer
- you have applied to the Bank for a service or product offered by the Bank
- you represent a customer of the Bank
- you are an officer, signatory, representative or beneficial owner of a company which is the Bank’s customer
- you are a guarantor or have provided any type of security to the Bank in relation to the obligations of a customer of the Bank
- you have parental responsibility over a customer of the Bank who is a minor

Reasons for processing your data

The law allows the Bank to use personal data, including sharing personal data outside the Bank, only if the Bank has a proper reason to do so. Specifically, the Bank must have one or more of these reasons to use your personal data:

- To fulfil a contract you have with the Bank,
- To take any steps, at your request, prior to entering into a contract with the Bank,
- When it is the Bank’s legal obligation under legislation and regulations applicable to the Bank (such as banking legislation, investment services legislation and anti-money laundering legislation),
- When it is in the public interest,
- When it is in the legitimate interests of the Bank* or another person with whom the data are shared, provided these interests do not unfairly go against what is right and best for you,
- When you consent to the use.

* A legitimate interest is when the Bank has a business and/or commercial reason to use your personal data. The Bank’s legitimate interests are described in the table that follows.

Here is a list of the ways that the Bank uses personal data, the reasons the Bank relies on to do so and what the Bank's legitimate interests are.

What the Bank uses your personal data for	Bank's reasons	Bank's legitimate interests
<ul style="list-style-type: none"> To review your application for the Bank's products and services. 	<ul style="list-style-type: none"> Pre-contractual steps. Bank legitimate interests. Bank legal obligation. 	<ul style="list-style-type: none"> Record keeping.
<ul style="list-style-type: none"> To deliver the Bank's products and services. To make and manage customer payments. To manage fees, charges and interest due on customer accounts. To collect and recover money that is owed to the Bank. To manage and provide treasury and investment products and services. To manage the relationship with you and the way the Bank communicates with you. 	<ul style="list-style-type: none"> Fulfilling contracts. Bank legitimate interests. Bank legal obligation. 	<ul style="list-style-type: none"> Keeping proper and up to date records of the Bank's activities.
<ul style="list-style-type: none"> To develop new ways to meet the Bank's customers' needs and to grow the Bank's business. To develop and carry out marketing activities. To study how the Bank's customers use products and services from the Bank. To provide information about the Bank's products and services. To carry out statistical and other analysis. 	<ul style="list-style-type: none"> Your consent. Bank legitimate interests. Bank legal obligation. 	<ul style="list-style-type: none"> Working out which of the Bank's products and services may interest you and tell you about them. Developing products and services, and what the Bank charges for them. Defining types of customers for new products or services.
<ul style="list-style-type: none"> To develop and manage the Bank's brands, products and services. To test new products. To manage how the Bank works with other companies that provide services to the Bank and/or the Bank's customers. 	<ul style="list-style-type: none"> Fulfilling contracts. Bank legitimate interests. 	<ul style="list-style-type: none"> Developing products and services, and what the Bank charge for them. Defining types of customers for new products or services.
<ul style="list-style-type: none"> To detect, investigate, report and help to prevent and prosecute crime. To manage risk for the Bank and the Bank's customers. To obey laws and regulations that apply to the Bank and its business. To respond to requests for information from regulatory and other authorities. To respond to complaints and seek to resolve them. To ensure the security and safety of our employees, customers and visitors, the protection of our premises, facilities and equipment and to prevent crime. To ensure the security, effectiveness and proper function of the Bank's IT systems, networks, and electronic communication systems. 	<ul style="list-style-type: none"> Fulfilling contracts. Bank legitimate interests. Bank legal obligation. 	<ul style="list-style-type: none"> Developing products and services, and what the Bank charge for them. Defining types of customers for new products or services.
<ul style="list-style-type: none"> To run the Bank's business in an efficient and proper way. This includes managing our financial position, business capability, planning, communications, corporate governance and audit. To exercise our legal and statutory rights, establish and defend of legal claims. 	<ul style="list-style-type: none"> Bank legitimate interests. Bank legal obligation. 	
<ul style="list-style-type: none"> To exercise the Bank's rights set out in agreements or contracts and to comply with the Bank's obligations set out in agreements or contracts. 	<ul style="list-style-type: none"> Fulfilling contracts. Bank legitimate interests. 	

Types of personal data

The Bank uses different types of personal data and groups them together as follows:

Type of personal data	Description by way of Examples
Financial	Information of your personal wealth including your assets, details of the assets, streams of incomes, expected incomes, personal financial position, employment and profession details and history, economic status, account numbers, IBAN and other financial information
Contact details	where you live and how to contact you. For example telephone number, home address, work address and email address.
Socio-Demographic	This includes details about your work or profession, nationality, education, marital status and where you fit into general social or income groups.
Transactional	Details about payments to and from your accounts with the Bank, insurance claims you make and tax information (for example information on the obligation to pay special contribution for defence), direct debit data.
Contractual	Details about the products or services we provide you with. This includes data concerning your accounts and cards, like account number, IBAN, card number and card issuance and expiry dates.
Locational	Data we get about where you are. Such may come from your mobile phone, the address where you connect a computer to the internet, or a shop where you buy something with your card.
Behavioural	Details about how you use our products and services.
Technical/digital	Details on the devices and technology you use, your digital activity and systems logs which are captured by the Bank's IT systems when you use them, IP addresses and the credentials you use to connect to our digital platforms available.
Communications	What we learn about you from letters, emails and conversations between us.
Social Relationships	Your family, friends and other relationships.
Documentary Data	Details about you that are stored in documents in different formats, or copies of them. This could include things like your specimen signature, passport, identity card, drivers licence or birth certificate.
Personal identification details including national identification numbers	Information which can directly identify you such as name, surname, date of birth and identification numbers or codes given or issued by a governmental service such as national Social insurance number, Tax identification code, ID number, Passport number, Driver's licence number
Video and sound recording	Video footages recorded by the CCTV system of the Bank in which you may be captured when you visit a branch, or voice call recordings when you call us

Special categories of personal data

The law treats some types of personal data as special. These include data concerning health and data relating to criminal convictions and offences.

The Bank may collect health data in the context of the assignment of insurance products as collateral for credit granted by the Bank. The Bank may, also, collect data relating to criminal convictions and offences of its customers and persons related to its customers as part of the Bank's initial and periodic review of its relationship with its customers, as required by law.

Where the Bank collects personal data from

The Bank collects personal data from other companies within the Bank's group of companies and from the following sources:

Data you give to the Bank:

- When you apply for the Bank's products and services
- When you talk to the Bank on the phone or in branch
- When you use the Bank's websites and digital banking (including mobile device applications, online banking and Application Programming Interface
- In emails and letters
- In insurance claims or other documents
- In financial reviews and interviews
- In customer surveys
- If you take part in the Bank's competitions or promotions.

Data the Bank collects when you use the Bank's services. This includes the amount, frequency, type, location, origin and Data from third parties:

- Your authorised representatives
- Companies that introduce you to the Bank
- Correspondent banks
- Business introducers
- Exchange of information mechanisms such as ARTEMIS
- Card associations
- Companies that process card payments, such as JCC Payments Systems Ltd
- Insurers
- Press, media and the internet
- Land agents
- Public information sources such as Companies Registry and Land Registry
- Agents working on our behalf
- Government and law enforcement agencies.
- Employers
- Other Financial Institutions
- Risk intelligence Databases
- CCTV Systems

Who receives your personal data and who the bank shares your personal data with

Within the Bank, access to your personal data is given to those officers who require such access to perform the Bank's contractual and other legal obligations.

Access is also given to third party service providers and agents employed by the Bank for these and other business purposes. Service providers and agents appointed by the Bank are required to observe the Bank's instructions in relation to the processing of personal data. These are mainly organisations from the categories listed below:

- Agents and advisers that the Bank uses to help run your accounts, provide you with our services and assist the Bank's operations. Specifically: processing of Bank references, credit reference agencies, support/maintenance of Electronic Data Processing / Information Technology applications, archiving and file storage, document destruction, data screening for anti-money laundering, property valuers and surveyors, CCTV systems providers, auditing services, advisory and professional service providers
- Other credit institutions, financial services institutions and comparable institutions. Specifically: correspondent banks, non-performing loan management companies, investment services, share registers, fund management and payment transactions
- Any party linked with you or your business's product or service
- Organisations that introduce you to the Bank
- Companies that the Bank introduces you to
- External legal advisors

The Bank may also provide your personal data to companies you ask the Bank to share your data with.

The Bank may be required to share your personal information with regulatory and other authorities and public bodies in Cyprus and the European Union:

- The Central Bank of Cyprus, the European Central Bank, the European Banking Authority
- The Cyprus Securities and Exchange Commission
- The police and MOKAS
- Tax authorities
- Artemis information exchange mechanism
- Bank Deposits Guarantee Fund, Credit and Other Institutions Resolution Fund
- Other regulators, authorities and public bodies insofar as a statutory or official obligation exists.

The Bank may need to share your personal information with other organisations to provide you with the product or service you have chosen:

- If you have a debit, credit or charge card with the Bank, the Bank will share transaction details with companies which help the Bank provide this service to you (such as JCC, Visa and Mastercard).
- If you have a Visa card or Mastercard and you have chosen to participate in a service of Visa or Mastercard to facilitate recurring transactions on replacement or renewal of your card, the Bank will share your new card details as appropriate, so that such data can be shared with participating merchants.
- If you use direct debits, the Bank will share your data with the SEPA Direct Debit scheme.
- If you apply for insurance through the Bank, the Bank may pass your personal or business details to the insurer, and onto any reinsurers.
- If you make an insurance claim, information you give to the Bank or the insurer may be put on a register of claims. This will be shared with other insurers.
- If you have a secured loan or mortgage with the Bank, the Bank may share information with other lenders who also hold a charge on the property.

The Bank may, also, share your personal information if the structure of the Bank's group of companies changes in the future:

- The Bank may choose to sell, transfer, or merge parts of the Bank's business, or the Bank's assets, or the Bank may seek to acquire other businesses or merge with them.
- During any such process, the Bank may share your data with other parties. The Bank will only do this if the other parties agree to keep your data safe and private.
- If there is such change to the Bank's group of companies, then other parties may use your data in the same way as set out in this privacy notice.

How the bank uses your personal data to make automated decisions

As a rule, the Bank does not make decisions based solely on automated processing. If the Bank uses automated procedures in certain cases, the Bank will inform you of this separately to this privacy notice, provided that this is prescribed by law.

Profiling

In some cases, the Bank processes your personal data automatically to evaluate certain personal aspects. The Bank refers to this as "profiling". For instance, the Bank uses profiling in the following cases: The Bank is required by law to take anti-money laundering and antifraud measures. Data evaluations are also carried out (in payment transactions, among other things) in this context. These measures also serve to protect you. The Bank may, for example, detect that an account is being used in ways that fraudsters work, or the Bank may notice that an account is being used in a way that is unusual for you or your business. If the Bank thinks there is a risk of fraud, the Bank may stop activity on the accounts or refuse access to them.

To provide you with targeted information and advice on products, the Bank uses evaluation tools. These enable demand-oriented communication and advertising, including market and opinion research.

The Bank uses scoring to assess your creditworthiness. The Bank calculates the likelihood that a given client will meet their contractual payment obligations. The calculation may include, for example, income levels, expenses, existing liabilities, occupation, length of

employment, experiences from the previous business relationship, repayment of prior loans in accordance with the contract, and information from credit agencies. Scoring is based on a mathematically and statistically recognised and proven procedure. The calculated score values assist us in our decision-making and are incorporated into ongoing risk management.

Information exchange mechanisms

The Bank carries out credit and identity checks when you apply for a product or service for you or your business. The Bank uses available information exchange mechanisms, such as ARTEMIS, to help with this.

If you use the Bank's services, from time to time the Bank may also search information that such mechanisms have, to help the Bank manage those accounts.

The Bank will share your personal data with those information exchange mechanisms prescribed by law (the "Mechanisms"), such as ARTEMIS and they will give the Bank information about you. The data the Bank exchanges can include:

- Name, address and date of birth
- Credit application
- Details of any shared credit
- Financial situation and history
- Public information, from sources such as the electoral register and Companies House.

The Bank will use this data to:

- Assess whether you or your business can afford to make repayments
- Make sure what you've told the Bank is true and correct
- Help detect and prevent financial crime
- Manage accounts with the Bank
- Trace and recover debts.

The Bank will go on sharing your personal information with these Mechanisms for as long as you are a customer of the Bank. This will include details about your settled accounts and any debts not fully repaid on time. It will also include details of funds going into the account, and the account balance. If you borrow, it will also include details of your repayments and whether you repay in full and on time. The Mechanisms may give this information to other organisations to which such information may be legally disclosed such as other banks that want to check credit status. The Bank will also tell the Mechanisms when you settle your accounts with the Bank. When the Bank asks the Mechanisms about you or your business, they will note it on your credit file. This is called a credit search. Other lenders may see this and the Bank may see credit searches from other lenders. If you apply for a product with someone else, the Bank will link your records with theirs. The Bank will do the same if you tell the Bank you have a spouse, partner or civil partner – or that you are in business with other partners or directors. You should tell them about this before you apply for a product or service. It is important that they know your records will be linked together, and that credit searches may be made on them. The mechanisms will also link your records together. You can find out more about ARTEMIS on its website.

Sending personal data outside the European Economic Area (the "EEA")

The Bank will only send your personal data to a country outside the EEA (a "third country"):

- If this is required for the execution of your orders (for example, when payments are made to a person in a third country, or for payment orders through a correspondent bank in a third country, such as dollar payments);
- if this is prescribed by law (for example, reporting obligations under tax law);
- if you have given the Bank your consent; or
- in the context of data processing undertaken by third parties on behalf of the Bank and according to the Bank's instructions.

If the Bank does send your personal data to a third country, the Bank will make sure that your personal data is protected in the same way as if it was being used in the EEA. The Bank will use one of these safeguards:

- Send it to a third country with privacy laws that give the same protection as the EEA, as certified by an adequacy decision of the European Commission. Learn more about this on the European Commission website.
- Put in place a contract with the recipient that they must protect it to the same standards as applicable in the EEA. Read more about this on the European Commission website.
- Transfer it to organisations that comply with binding corporate rules, or an approved code of conduct or certification mechanism that requires its protection to the same standards as applicable in the EEA.

Required personal data

Within the scope of your business relationship with the Bank, you must provide personal data which is necessary for the initiation and execution of a business relationship and the performance of the associated contractual obligations or which the Bank is legally obligated to collect. As a rule, the Bank would not be able to enter into any contract or execute the order without these data or the Bank may no longer be able to carry out an existing contract and would have to terminate it. When requesting the provision of data from you, the Bank will tell you whether you are required to provide these data and of the consequences if you do not.

Marketing

The Bank may use your personal data to tell you about services, products and offers that may be relevant for you. In order to decide which services, products and offers to tell you about, the Bank studies the personal data the Bank has on you, at any given time, to form a view on what the Bank thinks you may want or need, or what may be of interest to you.

Under the GDPR, the Bank can use your personal data to send you marketing messages to serve its legitimate interests (as defined above in Reasons for processing your data), provided the interests of the Bank do not unfairly go against what is right and best for you. The Bank does not need your consent to send you these marketing messages, but you have the right to ask the Bank to stop sending you marketing messages by contacting the Bank at any time (in the manner described below in Objecting to the Bank's use of your personal data).

If you are a customer of the Bank and you have provided your email address to the Bank in the context of services provided to you by the Bank, the Bank may use your email address to send marketing messages to you, unless you have objected. In each email message you receive, the Bank will let you know how you can exercise your right to object to receiving marketing emails from the Bank.

How long can the bank keep your personal data

The Bank processes and stores your personal data as long as necessary for the performance of the Bank's contractual and other legal obligations. In this regard, it should be noted that your business relationship with the Bank is a continuing obligation designed to last for several years.

After you stop being a customer of the Bank, the Bank may keep your personal data for up to 10 years for one of these reasons:

- To respond to any questions or complaints.
- To show that the Bank treated you fairly.
- To maintain records according to rules that apply to the Bank such as under applicable tax, banking and money laundering laws and regulations.
- To preserve evidence that may be needed for the establishment, exercise or defence of legal claims.

If the Bank holds your personal data because you are related to a customer of the Bank (e.g. you are a representative, beneficial owner, officer or guarantor), the Bank may keep your personal data for any of the above reasons for up to 10 years after the end of the relationship of the Bank with the relevant customer.

The Bank may keep your personal data for longer than 10 years from the end of the customer relationship if the Bank cannot delete it for legal, regulatory or technical reasons. For example, the Bank may keep your data for such longer periods as is necessary to preserve evidence for legal or other proceedings which have not come to a conclusion.

The Bank may also keep your personal data for a longer period for research or statistical purposes. If the Bank does, it will make sure that your privacy is protected and only use it for those purposes.

Your personal data protection rights under the GDPR and how to exercise them

Your data protection rights, granted by the GDPR, are described below. You may exercise them at any time in any of the following ways:

- by calling the Bank's Service Line (local number: 8000 9999 or, if calling from abroad, +357 22 500 500);
- through the Bank's online banking service (bank mail);
- or
- submitting your request in any of the Bank's branches.

Obtaining a copy of your personal Data

You have the right to obtain from the Bank confirmation as to whether or not your personal data is being processed and to access your data from the Bank.

Correction of inaccurate or incorrect information

You have the right to question any personal data the Bank holds about you that you think is wrong or incomplete. If you do, the Bank will take reasonable steps to check its accuracy and correct it.

Objecting to the Bank's use of your personal data

You have the right to object to the Bank's use of your personal data and ask the Bank to stop using your data in any of the following circumstances:

- You have the right to object, on grounds relating to your particular situation, at any time to processing of your personal data which is intended by the Bank to safeguard its legitimate interests or to serve the public interest. If you lodge an objection, the Bank will no longer process your personal data unless the Bank can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or unless the processing is for the establishment, exercise or defence of legal claims.
- You have the right to object to the processing of your personal data for marketing purposes. If you lodge such an objection, your data will no longer be processed for such purposes.
- You have the right to object to the processing of your personal data for scientific or historical research purposes or statistical purposes, on grounds relating to your particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Right to be forgotten

You have the right to have the Bank delete or remove your personal data in the following circumstances:

- The processing of the data by the Bank is no longer necessary for any of the reasons the data was collected and used
- You have withdrawn your consent and there is no other reason for the data processing
- You have successfully objected to the processing of the data by the Bank
- The data has been unlawfully processed
- Deletion is required by law

There may be legal or other official reasons why the Bank needs to keep your personal data. But please tell the Bank if you think that your data should be deleted.

Restriction of processing

You also have the right to restrict the Bank's use of your personal data in the following circumstances:

- pending verification by the Bank of data the accuracy of which you have contested
- the processing is unlawful but you do not want your data to be erased
- the Bank no longer needed the data but you do not want it to be erased because you need it for the establishment, exercise or defence of legal claims
- pending the Bank's assessment where you have objected to processing intended to safeguard the Bank's legitimate interests

Withdrawing your consent

Where the Bank relies on your consent for the processing of your data, you can withdraw your consent at any time. If you withdraw your consent, the Bank may not be able to provide certain products or services to you. If this is so, the Bank will tell you before giving effect to your withdrawal notification.

Data portability

You have the right to receive your personal data from the Bank in a format that can be easily re-used. You can also ask the Bank to pass on your personal data in this format to other organisations, where this is technically feasible. This right relates to the data which you have provided to the Bank and which the Bank processes electronically in reliance on your consent or for fulfilling the contract between you and the Bank.

Filing a complaint

If you are unhappy with how the Bank has used, or uses, your personal data, please let the Bank know. You also have the right to complain to the Office of the Commissioner for Personal Data Protection.

Changes to this privacy notice

This privacy notice sets out the information that the Bank must provide to you for the purposes of the GDPR which is applicable as of 25 May 2018. Any information in relation to the processing of personal data that is included in any of the Bank's existing circulars, manuals and associated forms on matters which are covered by this Privacy Notice are deemed to be superseded by the information in this notice.

The Bank may revise or update this privacy notice from time to time. The new version of this notice will be available on the Bank's website.

In case of significant changes (such as in relation to the reasons for which the Bank uses personal data or to the way in which you may exercise the rights described above), the Bank will bring these changes to your attention