

PRIVACY NOTICE

Last updated May 2018

This privacy notice provides an overview of how Hellenic Bank Public Company Ltd (the **"Bank"**) processes personal data of persons who submit an application for a job with the Bank or any subsidiary company of the Bank ("applicants") in the context of the review of their application. **"Personal data"** refers to any information about an applicant that the Bank collects from the applicant or other sources.

Who is responsible for the processing of applicant data – contact details

The personal data of applicants is collected and held by the Bank, which is responsible for their processing. If you, as an applicant, wish to contact the Bank in relation to the processing of your personal data you may do so using the following contact details:

Hellenic Bank Public Company Limited, with Company Registration Number HE6771, whose registered office is at Corner of Limassol and 200 Athalassas Avenue, 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

In all cases, the processing of your personal data by the Bank must be in compliance with the provisions of the 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.

How the Bank uses applicant personal data

The law allows the Bank to use personal data only if the Bank has a proper reason to do so. Relevant reasons include:

- To take any steps, at the request of the individual concerned, before he/she enters into a contract with the Bank.
- When it is the Bank's legal obligation, pursuant to applicable laws and regulations (such as law relating to employment and social insurance matters and to the provision of banking and investment services).
- 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 the individual concerned.
- When the individual concerned consents to the use of his/her personal data.

* A legitimate interest is when the Bank has a business and/or commercial reason to use applicant personal data. Other persons outside the Bank may also have a legitimate interest to receive certain applicant personal data for their regulatory purposes (for example, where regulatory consent is required for the applicants to be recruited in a particular position).

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

What the Bank uses applicant data for	Reasons	Legitimate interests
Current recruitment process <ul style="list-style-type: none"> • To review the application and assess the applicant's suitability. • To verify and, if required, obtain confirmation of the applicant's qualifications and prior work experience. • To communicate with the applicant. • To obtain, if required, regulatory consent to the applicant's recruitment. 	<ul style="list-style-type: none"> • Pre-contractual steps. • Bank legitimate interests. • Bank legal obligation. 	<ul style="list-style-type: none"> • Complying with applicable law and regulations. • Being efficient in fulfilling the Bank's legal duties and reviewing applications. • Record keeping.
Future vacancies <ul style="list-style-type: none"> • To consider the possibility of recruiting the applicant in case of future vacancies (if the applicant is not recruited during the current recruitment process). 	<ul style="list-style-type: none"> • Applicant consent. 	
Whilst data are held by the Bank <ul style="list-style-type: none"> • To establish, exercise or defend any legal claims. • To detect, investigate, report and help to prevent and prosecute crime. • To comply with laws and regulations that apply to the Bank and its business. • To respond to requests for information from regulatory and other authorities. 	<ul style="list-style-type: none"> • Bank legitimate interests. • Bank legal obligation. 	<ul style="list-style-type: none"> • Developing and improving how the Bank deals with financial and other crime. • Fulfilling the Bank's obligations and exercising its rights under applicable laws and regulations. • Cooperating with the police and other authorities in Cyprus and the EU.

Sources and types of personal data

The Bank collects personal data from the applicants themselves through their job application and during any interviews that take place during the recruitment process. Data is also collected from the persons who provide references for the applicants and/or from recruitment agencies with which the Bank cooperates for the provision of recruitment services.

The Bank collects different types of personal data in relation to applicants:

- Identification data (name and identity card and/or passport number)
- Contact details (residential address, telephone number and email address)
- Qualifications (education, academic and professional qualifications, relevant certificates and licences)
- Work experience (previous positions and experience)
- Past criminal record (as required by law)

Special categories of personal data

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

The Bank collects data relating to criminal convictions and offences (e.g. clean criminal record certificates) as may be required by law.

Requirement to give personal data

The data requested in the job application are necessary for the assessment of the applicant by the Bank for the relevant position. Depending on the particular position, the data may include confirmation that the applicant has the qualifications and/or experience required by the Bank and any law or regulations applicable to the Bank. As a rule, the Bank would not be able to properly assess the application and enter into any employment relationship without these data.

When requesting the provision of any additional data from applicants, the Bank will inform them whether they are required to provide these data and of any consequences if they do not.

Who has access to applicant personal data

Within the Bank, access to applicant personal data is given to those employees who are involved in the recruitment process. Access is also given to third party service providers and agents engaged by the Bank for business purposes. Such service providers and agents 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 the recruitment process
- Organisations that process data on behalf of the Bank, including support / maintenance of Electronic Data Processing / Information Technology applications, archiving and file storage, document processing, data destruction, compliance services, auditing services
- External legal advisors

The Bank also discloses personal data to governmental, regulatory and other authorities and public bodies in Cyprus and the European Union to the extent required by law, regulation, directive or court order:

- Governmental departments and ministries (such as the Department of Social Insurance)
- The Human Resource Development Authority
- The Central Bank of Cyprus, the European Central Bank, the European Banking Authority, the Single Supervisory Mechanism
- Other regulators, authorities and public bodies insofar as a statutory or other obligation exists

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

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

- If this is prescribed by law (for example, any reporting obligations under tax law);
- If the applicant has consented; 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 transfer personal data to a third country, the Bank will make sure that the relevant personal data are protected in the same way as if they were being used in the EEA. The Bank will use one of these safeguards:

- Transfer the data 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 means 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 in the USA that are part of Privacy Shield. This is a framework that sets privacy standards for data sent between the USA and EEA countries. It makes sure those standards are similar to what is used within the EEA. Learn 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 require its protection to the same standards as applicable in the EEA.

How long the Bank keeps applicant personal data

The personal data of applicants who enter into an employment contract with the Bank will be retained by the Bank in its employee records as described in the Bank's Privacy Notice for employees, which is provided to such successful applicants before they enter into the employment contract with the Bank.

Submission of an application of general interest

An application of general interest and related personal data will be maintained by the Bank for a period of two (2) years following submission of such application.

If an applicant wishes to be considered for employment with the Bank after this period, the applicant will have to submit a new application and related personal data.

Submission of an application for a specific job position

An application for a specific job position as published by the Bank from time to time and related personal data will be maintained by the Bank, for the purpose and/or in the context of the procedure for filling such specific job position, for a period of two (2) years following submission of the application for such specific job position.

If an applicant wishes to be considered for any future job vacancy after this period, the applicant will have to submit a new application and related personal data.

Data protection rights under the GDPR and how to exercise them

The data protection rights granted by the GDPR are described below. You may exercise them at any time by contacting the Bank's (data protection officer using the contact details provided above).

- **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 are held and processed by the Bank and to access your data.

- **Correction of inaccurate or incorrect information**

If you think that the Bank has information about you which is wrong or incomplete or out of date, you have the right to bring this to the attention of the Bank. If you do, the Bank will take reasonable steps to correct and update the data (subject, where appropriate, to verification of the accuracy of the relevant data).

- **Withdrawing your consent**

If you have consented to the retention of your data by the Bank after the completion of the current recruitment process, you have the right to withdraw your consent at any time. If you withdraw your consent, the Bank will delete your personal data and will not consider you in case of future vacancies during the retention period unless you submit a new application.

- **Objecting to the Bank's use of your personal data**

You have the right to object, on grounds relating to your particular situation, to processing of your personal data which is intended by the Bank to safeguard its legitimate interests. 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 defense of legal claims.

• Right to be forgotten

You have the right to have the Bank to 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 were collected and used (e.g. because you decide to withdraw your application)
- You have withdrawn your consent to the retention of your data by the Bank and there is no other reason for the processing of these data
- You have successfully objected to the processing of the data by the Bank
- The data have 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 needs the data but you do not want them to be erased because you need them for the establishment, exercise or defense of legal claims
- Pending the Bank's assessment where you have objected to processing intended to safeguard the Bank's legitimate interests

• 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.

• 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

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) during the recruitment process or the period of retention of your data, the Bank will bring these changes to your attention.