

privacy notice

privacy notice

who we are

Hellenic Life Insurance Company Ltd (henceforth the "Company") is the life insurance Company of the Hellenic Bank Public Company Ltd Group (from now on the "Hellenic Bank"). It was incorporated in 2000, under the name Hellenic Alico Life Insurance Company Ltd, through the strategic partnership of MetLife and Hellenic Bank. The company was renamed Hellenic Life Insurance Company Ltd, after the acquisition of the entire share capital from Hellenic Bank.

The Company strongly believes in protecting the confidentiality and security of your personal data. This document is referred to as the Company's "Privacy Notice" and provides an overview of how the Company processes your personal data. "Personal data" refers to any information relating to you that the Company obtains from you or other parties. The types of personal data processed and how they are used depends, largely, on the services you request from the Company, or the Company agrees to provide to you, from time to time.

The Company's Privacy Notice contains some terms which you may need help understanding. These terms are listed in the Glossary at the end of this Privacy Notice.

In all cases, the processing of your personal data by the Company 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 Company are described in this notice.

who is responsible for the processing of your personal data

Your personal data will be held by the Company and responsibility for its processing lies with:

Hellenic Life Insurance Company Ltd
66 Griva Digheni Avenue
1095 Nicosia
Cyprus
Telephone: (+357) 22501581
email: life@hellenicbank.com

how to get more help

If you want help with the Company's Privacy Notice or have questions about it, please contact the Company's Data

Protection Officer whose contact details are below:

Data Protection Officer

Hellenic Life Insurance Company Ltd
173 Athalassas Avenue
2025 Strovolos
P.O. Box 24747
1394 Nicosia
Cyprus
email: dataprotection@hellenicbank.com

If you are unhappy about any aspect of the way the Company collects, shares or uses your personal data, please let the Company know. You can contact the Company using the details above.

If you are not happy with the Company's response, you have the right to complain to the Commissioner for Personal Data Protection at:

Commissioner for Personal Data Protection

1 Iasonos Street
2nd Floor
1082 Nicosia
Cyprus
Telephone: (+357) 22818456
Fax: (+357) 22304565
email: commissioner@dataprotection.gov.cy
Website: www.dataprotection.gov.cy

how the company learns about you

Personal information is mostly provided by you when you first contact the Company and whilst you are the Company's customer, but is also information that the Company learns through its relationship with you and information about you that the Company collects from other sources as explained below in *where the Company collects your personal data from*.

The Company's relationship with you will arise in any of the following ways:

- You are the Company's customer
- You have applied to the Company for a service or product offered by the Company
- You represent a customer of the Company
- You are an officer, signatory, representative or beneficial owner of a customer of the Company
- You are a guarantor or have provided some type of security to the Company in relation to the obligations of a customer of the Company
- You have parental responsibility over a customer of the Company who is a minor

reasons for processing your personal data

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

- To fulfill a contract, you have with the Company
- To take any steps, at your request, prior to entering into a contract with the Company

- To enable the Company, fulfill its legal duty under legislation and regulations applicable to the Company (such as insurance legislation, investment services legislation, anti-money laundering legislation, terrorism prevention and sanctions screening checks, complaints and investigations or litigation)
- When it is in the public interest
- When it is in the legitimate interests of the Company* or another person with whom the personal data is 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 Company has a business and/or commercial reason to use your personal data. The Company's legitimate interests are described in the table below.

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

| What the Company uses your personal data for | Company Reasons | Company Legitimate Interests |
|---|--|--|
| <ul style="list-style-type: none"> • To evaluate your application for the Company's insurance products and services and provide insurance to you i.e. for underwriting purposes | <ul style="list-style-type: none"> • Pre-contractual steps • Company legitimate interests • Company legal duty | <ul style="list-style-type: none"> • Complying with regulations that apply to the Company • Being efficient in fulfilling the Company's legal duties and reviewing your application • Record keeping |
| <ul style="list-style-type: none"> • To deliver the Company's products and services • To make and manage customer payments • To manage fees, charges and investment returns on customer policies • To collect and recover money that is owed to the Company • To manage and provide treasury and investment products and services • To manage the relationship with you and the way the Company communicates with you • To administer your insurance policy and process claims, renewals and other transactions • To check your instructions to the Company • To notify you about changes to the Company's insurance products and services | <ul style="list-style-type: none"> • Fulfilling contracts • Company legitimate interests • Company legal duty | <ul style="list-style-type: none"> • Being efficient in fulfilling the Company's legal and contractual duties • Complying with regulations that apply to the Company • Keeping proper and up to date records of the Company's activities |
| <ul style="list-style-type: none"> • To develop new ways to meet the Company's customers' needs and to grow the Company's business • To develop and carry out marketing activities such as marketing analytics including marketing campaign optimisation and web analytics, but only in an anonymised form to enable the Company to develop and target the marketing of the Company's products and services • To study how the Company's customers use products and services from the Company • To provide information about the Company's products and services • To perform research | <ul style="list-style-type: none"> • Your consent • Fulfilling contracts • Company legitimate interests • Company legal duty | <ul style="list-style-type: none"> • Working out which of the Company's products and services may interest you and tell you about them • Developing products and services, and what the Company charges for them • Defining types of customers for new products or services • Seeking your consent when the Company needs it • Being efficient in fulfilling the Company's legal and contractual duties |

| | | |
|---|---|---|
| <ul style="list-style-type: none"> • To develop and manage the Company's brands, products and services i.e. through claims analysis to assist in the Company's product pricing • To monitor the quality of the Company's insurance products and services • To analyse, assess and improve the Company's services to customers i.e. through portfolio and experience studies • To test new products • To manage how the Company works with other companies that provide services to the Company and/or the Company's customers | <ul style="list-style-type: none"> • Fulfilling contracts • Company legitimate interests • Company legal duty | <ul style="list-style-type: none"> • Developing products and services, and what the Company charges for them • Defining types of customers for new products or services • Being efficient in fulfilling the Company's legal and contractual duties |
| <ul style="list-style-type: none"> • To check your identity/confirm or correct what the Company knows about you • To detect, investigate, report and help to prevent and prosecute fraud, money laundering, terrorism and other crimes • To manage risk for the Company and the Company's customers • To obey laws and regulations that apply to the Company and its business • To respond to requests for information from regulatory and other authorities • To respond to complaints and seek to resolve them • To provide evidence in any dispute or anticipated dispute between you and the Company • To aggregate on an anonymous basis with other data for analytical and reporting purposes | <ul style="list-style-type: none"> • Fulfilling contracts • Company legitimate interests • Company legal duty • Public interest | <ul style="list-style-type: none"> • Developing and improving how the Company deals with financial and other crime, as well as exercising the Company's legal duties in this respect • Complying with regulations that apply to the Company • Cooperating with the police and other Competent Authorities in Cyprus and the EU i.e. the Cyprus Insurance Control Service • Being efficient in fulfilling the Company's legal and contractual duties |
| <ul style="list-style-type: none"> • To run the Company's business in an efficient and proper way. This includes managing the Company's financial position, business capability, planning, communications, corporate governance and audit • To facilitate corporate transactions • To facilitate the Company's internal business purposes, which may include business and disaster recovery, document retention/storage, IT service continuity (e.g. backups and helpdesk assistance) to ensure the quality of insurance products and services the Company provides to you | <ul style="list-style-type: none"> • Company legitimate interests • Company legal duty | <ul style="list-style-type: none"> • Complying with regulations that apply to the Company • Being efficient in fulfilling the Company's legal and contractual duties |
| <ul style="list-style-type: none"> • To exercise the Company's rights set out in agreements or contracts | <ul style="list-style-type: none"> • Fulfilling contracts | |

types of personal data

The Company uses different kinds of personal data and groups them together like this:

| types of personal data | description by way of example |
|------------------------------|---|
| Financial | Your assets, income, financial position, employment details, status and history. |
| Contact | Your name, where you live and how to contact you, for example telephone, home address, work address and email address. |
| Socio-Demographic | This includes details about your life style, your work or profession, nationality, education, marital status, age or date of birth, gender and where you fit into general social or income groupings. |
| Transactional | Details about payments to and from the Company, insurance claims you make, tax information and direct debit data. |
| Contractual | Details about the products or services the Company provides to you. |
| Behavioral | Details about how you use the Company's products and services i.e. hobbies, recreational activities or sports. |
| Technical | Details on the devices and technology you use. |
| Communications | What the Company learns about you from letters, emails and conversations between us. |
| Social Relationships | Your family, friends and other relationships. |
| Open Data and Public Records | Details about you that are in public records, such as information about you that is openly available on the internet. |
| Usage Data | Other data about how you use the Company's products and services. |
| 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, driver's license or birth certificate. |
| Consents | Any permissions, consents or preferences that you give the Company. This includes things like how you want the Company to contact you. |
| National Identifier | A number or code given or issued to you by a governmental service to identify who you are, such as passport, identity card or social insurance number. |

special categories of personal data

The law treats some types of personal data as special. Special data is more sensitive including personal data concerning your health, racial or ethnic origin and personal data relating to criminal convictions and offences.

Where the Company is legally required to obtain your consent to process these special categories of personal data, the Company will ask you for it at the relevant time. If you choose not to give your consent, the Company may not be able to perform some of the tasks needed to provide certain products or services to you and may, in some cases, need to cancel your policy or your insurance cover or end the Company's relationship with you, as a consequence.

where the company collects your personal data from

The Company collects personal data from Hellenic Bank in the context of the assignment of insurance products as collateral for credit facilities granted by the Bank as well as in the instances outlined below.

Personal data provided to the Company:

- When you apply for the Company's products and services
- When you request information about the Company's products and services
- When you ask to have a Company representative contact you
- When you make a policy amendment or claim
- When you make a complaint
- When you participate in any Company surveys
- When you take part in Company competitions or promotional campaigns
- When you talk to the Company on the phone or in person at its offices
- When you use the Company's website
- In emails and letters
- In financial reviews and interviews
- By your employer, if the Company is providing insurance cover for its group employee benefits scheme
- By the policyholder, if you are covered under a group policy
- From publicly available information that you post online on social networking sites

Personal data from third parties:

- Relatives
- Employers
- Credit reference agencies
- Consumer reporting agencies
- Anti-fraud agencies
- Your authorised representatives
- Insurance intermediaries
- Financial service providers including financial advisors
- Other insurers
- Public information sources such as Companies Registry and Land Registry
- Agents working on the Company's behalf
- Health care providers and medical practitioners*
- Government and law enforcement agencies

** For some insurance products, the Company may ask your General Practitioner (GP) or other medical professional to send the Company a medical report. The Company will only do this with your prior consent.*

who receives your personal data and who the company shares your personal data with

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

legal obligations.

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

- Agents that the Company collaborates with to advise you and provide their services to you, to collect what you owe, and explore new ways of doing business
- Hellenic Bank that sells the Company's insurance products and services for the Company
- Health professionals including doctors and medical centres
- Credit reference agencies, police, consumer reporting and fraud prevention agencies to check your identity, credit history and whether you have any criminal record when the Company processes an application or claim
- Other insurers and financial services providers to prevent and detect fraudulent and exaggerated claims
- Third party administrators to assist the Company in the administration of your insurance policy or any claim you make under it
- Third parties that assist the Company in providing benefits in kind under your insurance policy
- Companies that print and distribute mailings or, where you have provided your consent, companies that perform marketing activities on the Company's behalf
- Other credit and financial services institutions, comparable institutions and processors to whom the Company transfers personal data in order to perform the business relationship with you, specifically: support/maintenance of electronic data processing/information technology applications, archiving and document retention/storage services, document processing, call center services, compliance services, controlling, data screening for anti money laundering purposes, data destruction, purchasing/procurement, space management, collection, customer management, non-performing loan management, marketing, media technology, reporting, research, risk controlling, expense accounting, telephony, video identification, website management, investment services, fund management, auditing services
- Any party linked with you or your business's product or service
- Companies that the Company has a joint venture or agreement to co-operate with
- Market researchers
- External professional advisors and consultants, including legal advisors and the Company's external auditors
- Reinsurers who help manage the Company's business and reduce the risks associated with underwritten insurance policies by spreading the Company's risks across alternative institutions
- Price comparison websites and similar companies that offer ways to research and apply for financial products and services

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

The Company may be required to share your personal information with regulatory and/or governmental and/or law enforcement authorities or other public bodies in Cyprus and the European Union such as:

- The Cyprus Insurance Companies Control Service
- The European Insurance and Occupational Pensions Authority
- The police and MOKAS
- Tax authorities
- Other regulators, authorities and public bodies insofar as a statutory or official obligation exists

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

- If you use a debit, credit or charge card in relation to any payment(s) to the Company for its services offered to you, the Company will share transaction details with companies which help the Company provide the relevant service to you (such as JCC, Visa and Mastercard)
- If you pay your policy by the use of direct debits, the Company will share your data with JCC
- If you make an insurance claim, information you give to the Company may be put on a register of claims, which may be shared with other insurers and/or reinsurers
- If you have used your policy with the Company as a collateral for a loan or mortgage, the Company may share information with other lenders who also hold a charge on the property provided that the Company will receive appropriate consent by you

The Company may, also, share your personal information if the ownership status of the Company changes in the future. The Company may choose to sell, transfer, or merge parts of its business, or its assets, or may seek to acquire other businesses or merge with them. During any such process, the Company may share your personal data with other parties, including prospective purchasers of its business and their professional advisors. The Company will only do this if the other parties agree to keep your personal data safe and private. If there is such change to the status of the Company, then other parties may use your personal data in the same way as set out in this Privacy Notice.

automated decision making and profiling

Currently, the Company does not use any technology for automated decision making and profiling. If it adopts such technology in the future, you will be notified and this Privacy Notice will be updated accordingly.

how the company protects your personal data

The Company has technical, administrative, and physical security measures in place to:

- Protect your personal data from unauthorized access and improper use
- Secure the Company's IT systems and safeguard the information
- Ensure the Company can restore your personal data in situations where the personal data is corrupted or lost in a disaster recovery situation

Where appropriate, the Company uses encryption or other security measures which the Company deems appropriate to protect your personal data. The Company also reviews its security procedures periodically to consider appropriate new technology and updated methods. Despite the Company's reasonable efforts, no security measure is ever perfect or impenetrable.

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

The Company may transfer your personal data to other countries. The countries in the EEA are considered to provide the same level of protection to personal data as the Republic of Cyprus.

The Company may also send your personal data to a country outside the

EEA (a "third country") in any of the following instances:

- If this is required by the reinsurers of the Company within the context of executing your policy or claim
- If this is prescribed by law (for example, reporting obligations under tax law)
- If you have given the Company your consent
- In the context of personal data processing undertaken by third parties on behalf of the Company and according to the Company's instructions

Where the Company transfers or shares personal data with others outside the EEA, the Company will ensure that your personal data is protected in the same way as if it was being used in the EEA, in accordance with data protection law by model clauses or other appropriate mechanisms. The Company will use one of these safeguards:

- Transfer 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 (learn more about this on the **European Commission** website)
- Transfer it to organisations in the USA that are part of Privacy Shield - a framework that sets privacy standards for personal data sent between the USA and EEA countries - which makes sure privacy 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

requirement to give personal information

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

marketing

The Company 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 Company studies the personal data the Company has on you to form a view on what the Company thinks you may want or need, or what may be of interest to you.

Up to now the Company was allowed to use your personal data to send you marketing messages if the Company had your consent or if you were a customer of the Company before July 2012 (for a special rule applicable to emails, please see the next paragraph). Under the GDPR, the Company can use your personal data to send you marketing messages to serve its legitimate interests (as defined above in reasons for processing your personal data), provided the interests of the Company do not unfairly go against what is right and best for you. The Company does not need your consent to send you these marketing messages, but you have the right to ask the Company to stop sending you marketing messages by contacting the Company at any time (in the manner described below in *your personal data protection rights under the GDPR and how to exercise them*).

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

how long can the company keep your personal data

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

After you stop being a customer, the Company 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 Company treated you fairly
- To maintain records according to rules that apply to the Company such as under applicable tax, insurance and money laundering laws and regulations
- To preserve evidence that may be needed for the establishment, exercise or defense of legal claims

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

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

The Company may also keep your personal data for a longer period for statistical purposes. In such a case, the Company 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 personal 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 Company at **22501581**
- through email at **life@hellenicbank.com**
- by submitting your request in writing to the Company's offices

The various rights are not absolute and are subject to certain exceptions or qualifications. You are entitled to receive your personal data free of charge except in the following circumstances where the Company may charge a reasonable fee to cover its administrative costs of providing the personal data for:

- Manifestly unfounded or excessive/repeated requests
- Further copies of the same information

Please consider your request responsibly before submitting it. The Company will respond as soon as it can. Generally, this will be within one month from when your request is received, but, if the request is going to take longer to deal with the Company will let you know.

An outline of your rights regarding your personal data is set out below:

the right to be informed

You have the right to be provided with clear, transparent and easily understandable information about how the Company uses your personal data and about your rights. This is why the information in this Privacy Notice is provided to you.

the right of access

You have the right to obtain access to your personal data (if the Company is processing it), and other certain information (similar to that provided in this Privacy Notice). This is so you are aware and can check that the Company is using your personal data in accordance with data protection law.

the right of rectification

You have the right to have your personal data corrected if it is inaccurate or incomplete. If you tell the Company that the personal data it holds on you is inaccurate or incomplete, the Company will take reasonable steps to check its accuracy and completeness and correct it if necessary.

the right to object to processing

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

- On grounds relating to your particular situation, at any time to processing of your personal data which is intended by the Company to safeguard its legitimate interests or to serve the public interest. If you lodge an objection, the Company will no longer process your personal data unless the Company can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedom or unless the processing is bound by the Company's legal duty under legislations and regulations or is for the establishment, exercise or defense of legal claims
- For marketing purposes. If you lodge such an objection, your personal data will no longer be processed for such purposes
- 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

the right to erasure

This is also known as the "Right to be Forgotten" and enables you to request the deletion or removal of your personal data, where there is no compelling reason for the Company to keep using it, as in the following circumstances:

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

The Company will have the right and/or obligation to retain the information, such as by virtue of legislative provisions to do so, but please inform the Company if you think that your personal data should be deleted.

the right to restrict processing

In certain situations you have the right to "block" or suppress further use of your information. When processing is restricted, the Company can still store your information, but may not use it further. This right applies in the following circumstances:

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

the right to withdraw your consent

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

the right of portability

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

the right to file a complaint

If you are unhappy with how the Company has used, or uses, your personal data, please let the Company 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 Company 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 Company'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 Company may revise or update this Privacy Notice from time to time. The new version of this notice will be available on the Company's website. In case of significant changes (such as in relation to the reasons for which the Company uses personal data or to the way in which you may exercise the rights described above), the Company will bring these changes to your attention.

glossary

Automated decision making refers to decisions reached by computer analytics including profiling, without any review or checks by any human, based on whether or not the information provided matches pre-defined acceptance criteria.

The Controller is the person or organisation which decides the purposes and means of the processing of personal data either on its own or with others.

Credit Reference Agencies are companies which collect personal data relating to the credit ratings of individuals and make it available to organisations such as insurers and banks.

Fraud Prevention Agencies collect, maintain and share, personal data internationally on known and suspected fraudulent activity.

Model clauses are standard contractual clauses which have been approved by the European Commission as providing adequate safeguards to enable personal data to be transferred outside the European Economic Area.

Personal data is any personal information relating to an individual who can be identified, directly or indirectly, by reference to that information.

Processing means any operation or set of operations which is performed on personal data such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, erasure or destruction.

Profiling means any form of automated processing of personal data where personal data is used to analyse or predict certain personal aspects e.g. an individual's economic situation, health, personal preferences, interests, reliability or behavior.

Reinsurers provide insurance to insurance companies to enable them to manage their risk.

Special categories of personal data are types of personal data which might show a person's race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, sex life or sexual orientation, details about their health and any genetic or biometric data.

