

Privacy Statement

Last updated on 11 February 2021

We are committed to respecting your privacy and keeping your personal information secure. Please take a moment to familiarise yourself with our data protection principles and practices.

Ancoria Insurance Public Ltd (“we”, “us”, “our”, “Ancoria”) is committed to protecting your privacy and handling your personal information in an open and transparent manner. No matter where you reside, your personal information will be used in the ways described in this Privacy Statement, which provides an outline of our privacy policies and procedures and your privacy rights. The reason why we have to provide this information to you is because, under the data protection legislation, we are the ‘data controller’ of your personal information.

- ***What personal information we collect and from where***
- ***Why and on what legal basis we collect and use personal information***
- ***Minors’ personal information***
- ***How long we keep personal information***
- ***How we protect personal information***
- ***Sharing of personal information with third parties***
- ***Sharing of personal information between pension plan holders and Ancoria***
- ***Transfer of personal information to international organisations outside the EU***
- ***Recruitment***
- ***Third-party data protection practices***
- ***Privacy rights***
- ***Privacy Statement updates***
- ***Contact us***
- ***Cookies***

What personal information we collect and from where

Type of Personal Data	Details
Information you give us through our application forms, websites and mobile application	<ul style="list-style-type: none"> ▪ Personal details e.g. name, address, passport/ID number, date of birth ▪ Contact details e.g. telephone number, email address ▪ Photo identification ▪ Authentication data e.g. signature ▪ Job title/profession or function ▪ Bank account information ▪ Financial information e.g. source of wealth, salary ▪ Politically Exposed Person, Common Reporting Standard (CRS) and Foreign Account Tax Compliance Act (FATCA) status ▪ Tax residence and Tax Identification Number (TIN) ▪ Investment strategy, investment objectives ▪ Transaction details ▪ Employment details e.g. employee ID, work email address, employment start date, salary ▪ Information relating to participation in our scholarship competitions and other prize competitions/draws

Information we receive about you from individuals or organisations who have a policy with us to which you are connected or related e.g. as an insured person, beneficiary, member	<ul style="list-style-type: none"> ▪ Personal details e.g. name, address, passport/ID number, date of birth ▪ % entitlement to policyholder's death benefit ▪ Employment details e.g. employee ID, work email address, employment start date, salary
Information collected when you contact us via phone, email, websites or mobile application	<ul style="list-style-type: none"> ▪ Contact details e.g. telephone number, email address
Information collected automatically from your device through cookies or other tracking methods when you use our websites or mobile application	<ul style="list-style-type: none"> ▪ IP address, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform, information about your visit e.g. URL, clickstream to, through and from our websites e.g. date and time, products you viewed or searched for, page response times, download errors, length of visits to pages, page interaction information e.g. scrolling, clicks and mouseovers and methods used to browse away from the page ▪ Country, platform (iOS or Android), device model, mobile OS version, number of installs and uninstalls
Information from publicly available sources e.g. Department of Registrar of Companies and Official Receiver, InfoTorg-Spar, other public registers, press, media and the internet	<ul style="list-style-type: none"> ▪ Personal details e.g. name, address, date of birth, gender, marital status, place of birth, country of residence, legal guardianship status ▪ Job title/profession or function ▪ Politically Exposed Person status ▪ Other personal information published online or in other form, which may be found when conducting general searches through the web

We do not collect any sensitive personal information but if we ever have to, we will request it directly from you and will ask you to specifically agree to us using it.

You can refuse to provide us with your personal information at any time but, if you choose to do so, we may not be able to provide or continue to provide you with our products and services. If this is the case, we will let you know.

Why and on what legal basis we collect and use personal information

We use your personal data for the following reasons:

- To check your identity and decide whether or not to accept an application from you for one of our products or services.
- To check your identity and decide whether or not to enrol you as a member under the Ancoria Pension Plan.
- To perform our contractual duties and communicate with you in the course of our business relationship.
- To meet our legal and regulatory responsibilities e.g. under insurance laws and regulations, laws on know-your-customer and anti-money laundering procedures, sanctions and anti-terrorism requirements, tax laws including the Foreign Account Tax Compliance Act (FATCA) and the Common Reporting Standard (CRS), laws on the Deposit Guarantee and Resolution of Credit and Other Institutions Scheme, etc.
- To respond to requests from public authorities within or outside your country of residence.
- To protect our own or a third party's legitimate interests e.g.:
 - For the prevention, detection and investigation of suspected illegal activity e.g. fraud or money laundering.
 - For the establishment and protection of our own and our customers' legal rights.
 - For the initiation and preparation of legal claims.
 - For the resolution of complaints and handling requests about your data protection rights.
 - For the analysis and management of insurance, financial and other commercial risks.

- For research and statistical analysis that help us develop our products, services, systems, business relationships, websites and mobile application
- For the effective management of our business operations e.g. for auditing, financial, accounting, billing, IT, disaster recovery, business continuity, website hosting, mobile application hosting, record and print management purposes, etc.
- For the performance of data analytics.
- For the development and improvement of our IT and systems security.
- To provide you with marketing information about our products or services or for any other reason for which you have provided us with your specific consent to use your personal information. You have the right to withdraw your consent at any time by contacting our Data Protection Officer.

Minors' personal information

Our websites and mobile application are not designed to be used or accessed by minors and we do not provide online services to minors. If we need to collect personal information about a minor under the age of 18, we will only do so with the consent of his or her parents or legal guardians.

How long we keep personal information

Under anti-money laundering laws, we may need to hold information about you and your transactions for up to ten years. Generally, we will not hold your personal information for more than ten years after our business relationship with you has terminated, unless we need to because of a potential or ongoing claim or another legal reason.

How we protect personal information

We store personal information on our secure servers and premises and have strict technical and organisational security procedures and features in place to prevent or detect unauthorised access or unlawful use, alteration and destruction.

To access our Ancoria Online Service website or mobile application, we give you a unique password to log in, which must be changed upon your first login. You must keep your new password confidential and not share it with anyone. At the end of each session, you must sign out of your account, even if you do not share your computer or mobile phone with someone else.

Our Ancoria Online Service website and mobile application are encrypted using 256-bit encryption but, unfortunately, providing information online is not completely secure. Although we do our best to protect your personal information, we cannot guarantee that all information you provide through our websites, mobile application or via email will be secure or that information you provide via email will be delivered to us. If we believe that the personal information we keep about you may not be secure, we will let you know as soon as possible.

Sharing of personal information with third parties

We may need to share your personal information with third parties for the following reasons:

- Provision and promotion of our products and services.
- Improvement of our websites and mobile application.
- Communication with customers and members of the Ancoria Pension Plan via text messages.
- Fulfilment of legal responsibilities.
- Detection (through identity checks) or reporting of high-risk or illegal activity, responding to official requests from information from public authorities, participation in fraud investigations.
- Enforcement of our legal rights and those of customers or other third parties.
- Managing, printing and destroying records.
- Sale, merge assignment, transfer or reorganisation of our business or assets.
- You have agreed to us sharing your personal information for a specific reason.

The third parties that we may share your personal information with are the following:

- Google analytics and search engine providers that help us improve our websites and mobile application.
- Advertisers and advertising networks (but only aggregate and anonymous information will be provided).
- External third-party service providers such as:
 - Actuaries.
 - Auditors.
 - Lawyers.
 - IT systems providers.
 - Information security service providers.
 - Asset storage, records management and secure shredding providers.
 - Data centres.
 - Cloud service providers.
 - Support and hosting service providers.
 - Record management and printing service providers.
 - Advertising and marketing agencies (only if you have consented to the use of your personal information for marketing purposes).
- Public authorities.
- Banking and financial services partners or intermediaries servicing our accounts.
- Other third-party service providers that assist us in our business activities.
- Purchasers and prospective purchasers.

Before we share personal information with third parties, we make sure that they have suitable policies and procedures and security measures in place in order to keep to data protection laws and regulations and, if appropriate, we also ask them to commit to meeting their data protection responsibilities contractually.

Sharing of personal information between pension plan holders and Ancoria

Pension plan holders share with us personal information about prospective and existing members of the Ancoria Pension Plan in order to facilitate the registration process and ensure the smooth running of the scheme. This is done through our Ancoria Online Service website or, manually, by filling in our forms and applications (depending on the pension plan holder's preferred method of enrolment).

Pension plan holders are also responsible for updating the personal information they provide to us in case there are any changes. Such information includes:

- Personal details e.g. name, employee ID.
- Contact details e.g. email address, telephone number.
- Employment details e.g. employment start date, salary.

Pension plan holders must provide the individuals with a link to this Privacy Statement so that they can read and understand how their information will be used by us and also obtain their permission before they disclose any personal information to us.

We use and protect any personal information which is shared with us like any other personal information we collect, keep and use.

Transfer of personal information to international organisations outside of the EU

We do not transfer your personal information outside the EU. If you choose to enter into an agreement with a third-party organisation based outside the EU through your Ancoria Life Policy, you must make sure that the organisation meets the EU data protection standards.

Recruitment

We treat all applicants' personal information as confidential and do not disclose it to anyone outside Ancoria, unless we have a legal responsibility to do so or you have agreed to us disclosing it. If your

application is not successful, we will keep your CV in our records for 6 months, unless we need to hold it for longer because of a potential or ongoing claim or another legal reason.

Third-party data protection practices

We cannot guarantee that the privacy practices of third parties are lawful. Therefore, you must assess third party links on our websites yourself before sharing your personal information with them.

Privacy rights

You have the following rights which you can exercise by sending an [email](#) or letter to our Data Protection Officer:

- **Right to be informed about what personal information we collect and use about you, why and how we use it.** This information is included in this Privacy Statement.
- **Right to a copy of the personal information that we hold about you.** You can view most of the personal information we keep for you on the Ancoria Online Service website or mobile application. You can also request a copy of the personal information that we keep to be sent to you, but we will only provide information that does not reveal other people's personal information or confidential communications with our legal advisers and is not linked to any ongoing criminal or fraud investigation.
- **Right to ask us to correct incomplete or inaccurate personal information that we hold about you.** You can correct some of the personal information that we keep for you via the Ancoria Online Service website or mobile application. If you contact us to correct personal information, we will have to verify the accuracy of any updated personal information you provide to us before making corrections.
- **Right to ask us to delete your personal information.**
 - If there is no good reason for us to continue using it;
 - If you gave us permission to use the information and you now wish to withdraw it;
 - If you have objected to us using the information;
 - If we have used the information unlawfully;
 - If we have a duty to delete the information to fulfil our legal and regulatory responsibilities.

Please note, however, that we may not be able to fulfil your request for specific legal reasons that we will explain to you. For example, as a regulated financial undertaking, anti-money laundering laws require us to keep certain customer information for at least five years. If those responsibilities take priority, we will let you know.

- **Right to request the transfer of your personal information to you or to a third party (if we are processing it by automated means).** If we can and are allowed to transfer it, we will provide it in a structured, commonly used, machine-readable format.
- **Right to ask us to suspend specific types of processing.**
 - If the personal information we hold about you is not accurate;
 - If we have used your personal information unlawfully but you do not want us to delete it;
 - If we no longer need your personal information but you want us to keep it so you can establish or defend a legal claim;
 - If you have withdrawn your permission for us to use your personal information but we are still in the process of processing your request.
- **Right to withdraw your permission or object to us using your personal information. Note that you can only withdraw your permission for future processing so any previous processing will continue to have been lawful.** In such a case, we may have to reject an application from you or refuse to execute instructions from you or even terminate our business relationship with you to meet the request.

- **Right to object to us using of your personal information (if we are using it solely on a legitimate interests basis).** However, in some cases, we may have important, overriding reasons to continue using it.
- **Right to object to the use of your personal information for direct marketing purposes.** You can also untick the option of receiving direct marketing material from us yourself, via the Ancoria Online Service website or mobile application.
- **Right to be informed in case there is a data breach that may put your rights at high risk.**

Privacy Statement updates

Occasionally, we will review and improve our data protection practices in line with developments relating to our business or legal requirements. When this happens, we will update our Privacy Statement and let you know through our websites, mobile application or via email if appropriate. If you want to follow up on any changes or updates to our policy and practices, please check back with us frequently.

Contact us

If you have any questions or concerns about our data protection practices or wish to exercise your rights or file a complaint, you may send your request to our Data Protection Officer by post at 36 Laodikias street, Strovolos, 2028 Nicosia, Cyprus or via email at dpo@ancoria.com. For security reasons, please note that we cannot process your request if we are unsure of your identity.

If you are unhappy with the way we have handled your personal information, you can complain directly to the [Office of the Commissioner for Personal Data Protection](#).

Cookies

Our websites use cookies. To learn more about cookies, you can read our [Cookie Policy](#).

Last update date appears at the top of this page.