Monument Assurance Luxembourg S.A.

Client Privacy Notice

Version July 2025

1. Introduction

The purpose of this Privacy Notice is to inform you in detail of the processing of personal data concerning you implemented by Monument Assurance Luxembourg S.A. ("MAL"), in compliance with the General Data Protection Regulation ("GDPR").

The Privacy Notice contains important information about our privacy practices with respect to personal data relating to our customers and their designated representatives, members of the general public visiting our website, external job applicants, contractors and other business partners, including, but not limited to, investment firms, potential suppliers and business targets, suppliers of goods and services, and shareholder representatives.

We invite you to read this Privacy Notice carefully. Any enquiries regarding this Privacy Notice should be directed to us using the contact details provided in Section 10 of this Privacy Notice.

This Privacy Notice explains how we collect, process and protect your personal data when you interact with MAL.

The categories of personal data we collect and how we process that data depend on the nature of our relationship and the ways in which we interact, including when you visit our website.

In this relationship and under the terms of the GDPR, MAL operates as a controller of your personal data.

Any significant updates to this Privacy Notice will be communicated to you by post or email if MAL has an email address. On request, this Information Notice can be sent to you by the desired communication channel (simple mail or email). This Privacy Notice is available on our company's website, the contact details of which can be found in Section 10 of this Privacy Notice.

Third-party websites that you may access via our website are not covered by this Privacy Notice. MAL is not responsible for the use and protection of any personal data you may provide to these third-party sites. You should exercise caution and read the data protection document of the relevant third party before providing any personal data to them.

2. Sources of collection of personal data

We may collect your personal data in the following ways:

- **Direct collection** - We collect personal data that you provide to us directly, such as when you contact us by email, post or telephone.
- **Acquisitions and administration of insurance policies** – When acquiring new portfolios, we obtain the management of new insurance policies. This means that we collect all the information related to the original insurance contract. As we continue to administer these contracts, we may collect new personal data when policyholders wish to make a change to the contract, submit a claim or make a request for information or enquiry in relation to your rights mentioned in Section 9 of the Privacy Notice.
- **Publicly available sources** - We may collect personal data from publicly available sources, such as social media.

3. Categories of Personal Data We Collect

We collect different categories of personal data about you depending on the nature of our relationship. For example, personal identification, financial information, recruitment information, policyholder and claims information, sensitive data collected for equal opportunity monitoring, compliance information, and contract information.

We may collect one or more of the following categories of personal data about you, depending on our relationship:

- **Personal identification** : name, surname(s), contact information (such as email address, postal address, telephone numbers), date of birth, title, employer, and visual data.
- **Financial information** : bank account name and number, sort code, credit reports, participation fees, and other financial data appropriate to support business transactions and/or accreditation verifications.
- **Detailed information about the insured** : this includes:
  - **Personal identification data** : name, gender, year and place of birth, date of death, national identification number, contact details, tax identification number.
  - **Location data** : street and number, postal/zip code, and country of residence.
  - **Personal life data** : marital status, identity of partner, number of children.
  - **Financial data** : bank account details.
  - **Professional data** : date of service, social status, salary, employment history, employer, professional sector; etc.
  - **Special categories of personal data**, including data relating to criminal offences and convictions ("criminal data") and health-related data, e.g. weight, height, diseases and treatments, smoking and pregnancy.
- **Detailed information about your claims** : including personal data about policyholders, witnesses, related parties, appointed adjusters and third-party service providers; and special categories of personal data such as medical reports, disability information and criminal data.
- **Sensitive data collected for purposes other than claims and policy management** : information regarding racial or ethnic origin, age, gender, religious or philosophical beliefs, sexual orientation and/or disability, for equal opportunity monitoring purposes and only with your explicit consent.
- **Tracking information** : video surveillance, including CCTV footage upon entry into our premises and technical information gathered through the use of cookies, web beacons, and/or similar tracking technologies that we place and may allow third parties to place on our website(s), including online identifiers such as IP addresses and unique device identification, and online activity information, such as direct and social media interaction with our website.
- **Compliance information** : results of background checks, including against criminal data, international sanctions, politically exposed persons or export control registries, complaints or claims, investigations and other information relating to monitoring, reporting and corrective actions; and
- **Contract information** : contracts to be entered into between us and other individuals or third parties, information regarding existing contracts between the individual and third parties.

4. How do we legally use your personal data?

We may use your personal data for different business purposes and rely on different legal bases, subject to applicable data protection laws and regulations. We do not process your personal data for purposes that are incompatible with those notified to you through this document.

We may use each category of personal data we collect on the following legal bases as set out in the GDPR Principles from Article 5 to Article 11 as well as Articles 12 to 23 on Data Subject Rights:

- **With your consent**, for all those purposes for which you specifically give your consent. When we process sensitive data about you, we additionally rely on your explicit consent obtained through your written consent. You have the right to withdraw your consent at any time.
- **To perform our contractual obligations to you**, including the management and delivery of the insurance contract.
- **To fulfil a legal obligation** to which we are subject, for example, know-your-customer checks.
- **To pursue our legitimate interests**, where they are not overridden by your own legitimate interests and/or fundamental rights and freedoms, including:

- To manage our interactions and business relationship, including by responding to requests you have submitted via our website, telephone, email or other means, and to deal with ongoing queries relating to such requests;
- Prevent or detect fraud, misrepresentation, security incidents, or crimes;
- To protect the safety, property, and rights of all persons who interact with us, including by ensuring the health and safety of all persons present on our business premises;
- To bring or defend legal claims relating to Monument Group entities;
- Investigate any complaints received from you or others about our services;
- Obtain legal advice, support, or representation in connection with legal, compliance, regulatory, and investigative claims, as necessary, as permitted by applicable laws and regulations;
- Notify you about changes to our services, if any;
- Present content on our website in the manner we believe is most effective or
- To ensure the security of our website, manage our business, provide administrative and IT services, and ensure network security.

- **For purposes that may be required or permitted by applicable data protection laws and regulations,** including for any other secondary purposes consistent with the original purposes of the processing of personal data set out herein**.**

Whenever it is necessary to process your personal data for purposes incompatible with those described above, we will contact you beforehand to ask for your explicit consent to such processing and will provide you with all relevant and necessary information relating to the necessity of such processing, as required by applicable data protection laws and regulations.

Please note that in certain circumstances, including where you have entered into or offer to enter into a contract with us (e.g. to us/provide you with products and/or services), the provision of personal data is a requirement of the contract you have entered into or are offering to enter into with us. The provision of personal data in these circumstances is necessary to enable us to carry out pre-contractual steps at your request, to conclude the contract and/or to perform our legal obligations under this contract.

5. How do we share your personal data?

Where permitted by applicable laws and regulations, we may disclose your personal data to Monument's subsidiaries and affiliates, third-party vendors, service providers and business partners, law enforcement and other government agencies, companies with whom we are involved in a corporate transaction, or any other third party on the legal bases set forth herein.

We may share your personal data with the categories of recipients described below:

- **Monument Subsidiaries and Affiliates**. We may share your personal data within our group of companies, which includes parent companies, affiliates, subsidiaries, business units, and other companies that share common ownership for the purposes, and using the legal bases, set forth herein.
- **Third-party suppliers of goods and services, partners, and other companies**. We may share your personal data with third parties working on our behalf to facilitate our interactions or to request or support our relationship.
- **Law enforcement and other government agencies**. We may share your personal data with law enforcement and/or other government agencies to comply with the law or legal requirements, to enforce or apply our terms and conditions and other agreements, and to protect our rights, property, and the safety of our employees, customers, and third parties.
- **Companies participating in a business transaction with us**. If we acquire insurance portfolios or other companies, or if we sell some or all of our assets, merge or are acquired by

another entity, or otherwise restructure our business, including through a sale or as part of bankruptcy, we may share your personal data with that entity.

6. Cross-border transfers of personal data

In some cases, we may need to transfer your personal data from their home country to another jurisdiction for processing. Where personal data may be transferred outside the territory where it was collected, we will only do so where permitted by applicable laws and regulations. We will implement appropriate legal mechanisms and safeguards to ensure that your personal data remains adequately protected once it arrives at its destination, as required by applicable data protection laws and regulations.

In some cases, it may be necessary to transfer your personal data to an entity within the Monument Group or to a third party as set out in Section 5 outside the country where it is collected. Our operations span multiple jurisdictions, including Bermuda, the United Kingdom, Singapore, Ireland, Luxembourg, Belgium, the Isle of Man, Spain and Italy.

Third-party recipients are organizations with whom we engage to provide our services to you. In doing so, we rely on a number of legal mechanisms to ensure that your data remains protected to a standard equivalent to that accorded to it in the country of origin.

Depending on the direction of the transfer of personal data and the European Commission's Standard Contractual Clauses, it includes the United Kingdom's regulations and standard contractual clauses, as well as other legally applicable safeguards (including physical safeguards) in accordance with applicable data protection laws and regulations. A copy of the relevant mechanism and information about the safeguards we have in place can be provided upon request by contacting us – see the "*Contact Us*" section below.

7. How do we protect and secure your data?

Monument Assurance Luxembourg S.A. has implemented IT and operational security procedures designed to protect your personal data against accidental or unlawful loss, disclosure, misuse, alteration or use.

We limit access to your personal data to only those employees and third parties who have a need to know. Third parties will only process your personal data on our instructions, and they are subject to a duty of confidentiality. We have put in place procedures to respond appropriately to any suspected personal data breach or security incident and will notify you and the relevant data protection authorities where we are legally required to do so.

Specifically for Luxembourg, the processing of your health data is carried out in accordance with the provisions of the law of 6 February 2025 amending the amended law of 7 December 2015 on the insurance sector. This processing is necessary for the performance of your insurance contract and provides:

1. compliance with the provisions on professional secrecy set out in Article 300 of the Law of 7 December 20215;
2. the implementation of the following appropriate measures taking into account the state of knowledge, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks, varying in likelihood and severity, to the rights and freedoms of data subjects:
   a) the appointment of a data protection officer;
   b) carrying out impact assessments in accordance with Article 35 of Regulation (EU) 2016/679;
   c) anonymisation or pseudonymisation of health data or other functional separation measures for certain health data processing operations;
   d) encryption of health data in transit, as well as state-of-the-art key management;

e) the implementation of restrictions on access to health data;
f) the establishment of log files that make it possible to establish the reason, date and time of the consultation and the identification of the person who collected, modified or deleted the health data;
g) raising staff awareness of the protection of health data and professional secrecy;
h) the regular evaluation of the effectiveness of the technical and organisational measures put in place through an independent audit;
i) the adoption of sectoral codes of conduct as provided for in Article 40 of Regulation (EU) 2016/679 and
j) the establishment of an internal policy providing in particular for how the principles laid down in Article 5 of Regulation (EU) 2016/679 are to be respected.

With regard to our subcontracting activities, we have concluded a service contract for the processing of your personal data with Monument Assurance Services Luxembourg Sà.r.l..

The processing of your data is strictly regulated within the framework of this contract and we carry out audits to ensure their compliance with the applicable contractual and regulatory rules.

8. Retention and disposal of personal data

We do not retain your personal data for longer than is necessary in accordance with legitimate legal, regulatory and business requirements.

At the end of their retention period, based on the minimum retention periods required by applicable laws and regulations, we will take steps to review your personal data. We may continue to retain your personal data if we identify another reason for doing so and there is a legal basis for that reason under applicable data protection laws and regulations. In this case, we will only retain the personal data required for the new purpose and we will implement systems and controls over this data in accordance with applicable data protection laws and regulations.

If there is no longer a purpose or legal basis for holding your personal data, we will dispose of it securely and permanently, in accordance with applicable data protection laws and regulations.

9. Individual Privacy Rights

Individuals whose personal data we process have a number of rights in relation to that data, depending on the jurisdiction in which they are located. To exercise your data protection rights, please contact us. We will respond to reasonable requests in accordance with applicable data protection laws and regulations.

The specific data protection rights applicable to you are detailed below depending on the jurisdiction in which you reside or are otherwise located. Please note that these data protection rights are not absolute and there may be circumstances in which we may legitimately refuse a request, as permitted by applicable data protection laws and regulations.

You should also note that the specific scope of the rights and associated exemptions may vary from jurisdiction to jurisdiction. You will not normally have to pay a fee to access your personal data (or to exercise any of the other rights set out below), although we may charge a reasonable fee if your request is unfounded, repetitive or excessive. In addition, we may refuse to comply with your request in these circumstances.

We may need to ask you for specific information to help us confirm your identity and ensure your right to access your personal data (or to exercise any of the other rights set out below). This is a security measure to ensure that personal data is not disclosed to an individual who does not have the right to receive it.

We may also contact you to request additional information in connection with your request in order to expedite our response. We will only collect information that is strictly necessary to ensure that we only honor requests received from the actual data subject or their authorized representative.

We strive to respond to all legitimate requests within the time limits provided by applicable data protection laws and regulations. It may happen that we take longer to respond if your request is particularly complex or if you have made several different requests. In this case, we will inform you of the estimated response times.

Your individual data protection rights

Each user has the following data protection rights in relation to our company:

The right to be informed

You have the right to receive information about how and why your personal data is processed.

The right of access

You have the right to request copies of your personal data that we have collected.

The right to rectification

You have the right to request rectification/completion of inaccurate/incomplete personal information that we have collected about you.

The right to erasure ("right to be forgotten")

You have the right to request the erasure of your personal data that we have collected, under certain legal conditions.

The right to restrict processing

You have the right to request the restriction of our processing of your personal data, under certain legal conditions.

The right to object to processing

You have the right to object to our processing of your personal data, under certain legal conditions.

The right to data portability

You have the right to request the transfer of your personal data that we have collected to a third party ("controller") or directly to you in a structured, commonly used and machine-readable format, under certain legal conditions.

Rights relating to automated decision-making and profiling

You have the right not to be subject to a decision based solely on automated processing, unless permitted by law.

The right to withdraw your consent

You have the right to withdraw the consent you have given at any time.

10. Contact us

If you have any questions, concerns and/or complaints regarding this document or if you wish to exercise your data protection rights above, please contact the Data Protection Officer of Monument Assurance Luxembourg S.A. using the following contact details:

- By email:

Luxembourg : DPO@monumentassurance.lu

- By mail:

Monument Assurance Luxembourg S.A.
Data Protection Officer
Atrium Business Park
29, rue du Puits Romain
L-8070 BERTRANGE

You also have the right to lodge a complaint with the relevant data protection authority of your country of residency such as the CNPD for Luxembourg (15 boulevard du jazz, L-4370 Esch-Belval) if your problem is still not resolved or if you are not satisfied.

However, we would appreciate it if you gave us the opportunity to resolve this issue before you contact the data protection authority.

END OF DOCUMENT