

Monument Assurance Belgium

Privacy Notice

Date of entry into force: 11.05.2026

1 INTRODUCTION

Monument Assurance Belgium is committed to maintaining and respecting its data protection obligations.

This notice contains important information about our privacy practices with respect to our clients and their representatives, visitors to our websites, external candidates, contractors and other business partners, including, but not limited to, investor firms, potential and target business partners, suppliers of goods and services, and candidate shareholders and their employees.

This notice is published by Monument Assurance Belgium. When we mention "Monument", "we", "us" or "our", we are referring to the company that processes your personal data and the third parties that do so on its behalf.

For the purposes of this notice, personal data includes any information relating to a natural person who can be identified, directly or indirectly, on the basis of data or a combination of data.

This notice tells you how we collect, process and protect your personal data when you interact with us. The categories of personal data we collect and the way we process that data depend on the nature of our relationship with you and the ways in which we interact, including when you visit our websites.

We may update this notice. We will notify you of any changes to this notice by posting an update on our websites. In specific situations where governed by applicable data protection laws and regulations, we will seek your consent before making significant changes to the way we process your personal data previously collected from you.

Third party websites that you may access through our websites are not covered by this notice. Monument Assurance Belgium accepts no responsibility for the use and protection of personal data you provide to these third party websites. You should exercise caution and read the privacy notice of the third party concerned before providing any personal data.

2 SOURCES OF PERSONAL DATA COLLECTION

We collect personal data about you from a number of sources, including directly from you, through business acquisitions and in the course of administering the insurance policy, from third parties and by automated means.

We collect personal data about you in a number of ways, including

- **Direct collection**
We collect personal data that you provide to us directly, for example, when you contact us by email, post or telephone, in which case we may save and process your data, as well as the message itself and the metadata provided we have a legal basis to do so.
- **Procurement and management of insurance policies**
When we acquire new business portfolios, we get new contracts. This means that we collect all the information related to these existing contracts. As we manage these contracts, we collect new personal data (e.g. when stakeholders wish to amend the contract or submit a claim, complete forms, report a claim, submit medical expenses, report hospitalization, enter personal data via our websites).
- **Collection by third parties**
We collect personal data about you from third parties such as persons you have authorized (e.g. insurance intermediaries, your lawyer, your notary and our partners), organisations and platforms to carry out checks we are required to carry out under anti-fraud and anti-money laundering and anti-terrorism legislation, platforms for obtaining your address and identifying your family members in order to identify the beneficiary(ies), your beneficiary(ies), by other companies when they are considering transferring (part of) their portfolios to Monument if this is necessary for the analysis prior to such acquisition or management in our systems. As part of the recruitment process, we collect personal data about you from third parties such as people you have authorised, recruitment or coaching companies.
- **Publicly available sources**
We may collect personal data from publicly available sources such as the Belgian Official Gazette and the Crossroads Bank of Enterprises, public-facing websites or professional networking platforms.
- **Automated collection**
We also collect and may allow third parties to automatically collect personal data about you through the use of cookies, plug-ins and similar tracking technologies on our websites.
You can update your automated collection preferences by accessing the cookie preference centre on our websites. For more information, please see our cookie notice at :
<https://www.monumentassurance.be>.
With respect to third party websites, we do not control them and are not responsible for their privacy and cookie policies.
- **Security cameras in and around our buildings marked with pictograms**

These images are stored for the sole purpose of ensuring the safety of property and persons and to prevent and identify abuse, fraud or other offences to which we and our customers may fall victim.

We may collect one or more categories of personal data about you depending on the nature of our relationship with you. This includes data relating to:

- **Personal identification:** surname, first name, contact details (such as e-mail and postal address, telephone numbers), date of birth, job title, name of employer or organisation, joint committee and visual image;
- **Financial information:** bank account name and number, IBAN, credit records, shareholding rights and other relevant financial data necessary for the execution of business transactions and/or certificate verifications;
- **Recruitment information:** *curriculum vitae*, including biographical information (such as work and study history), comments on professional references and recruitment, grades and related performance information, documents such as passport, ID card, driving licence and/or visa information, other information about you that you provide in a *curriculum vitae* or similar document;
- **Details of policyholders, insureds, beneficiaries, affiliates or any other parties involved in the insurance, mortgage or other contract.**

These include :

- personal identification data: first name, surname, sex, gender, date and place of birth, date of death, national register number, identity card number, contact details (e.g. telephone number, e-mail and fax), Tax Identification number ;
- location data: street and number, postal code and country of residence;
- personal data: marital status, partner identity, number of children, language;
- financial data: bank details, overall financial situation (salary, real estate, etc.), documents required for the settlement of the contract (e.g. proof of retirement, an extract of the member's death certificate, notarial deed showing the beneficiary's status, any other document enabling the identity of the beneficiary to be verified);
- customer data: audio and video recordings;
- occupational data: date of service, social status, employment rate, NISS number, employer, occupational sector, salary, employment history, retirement date;
- product data: your products and product usage; and
- special categories of health data: weight, height, illnesses and treatments, smoking and pregnancy, as well as the description of personal injuries following an accident, the medical expenses you declare in the context of your hospital insurance;
- **Detailed information about your claims or your level of satisfaction :** including personal data about policyholders, witnesses, related parties, appointed experts and third party service providers, satisfaction surveys and questionnaires and special categories of personal data such as medical reports, disability information and criminal data;
- **Surveillance and car park management information** including number plate when entering our premises, reference for parking and building access badges, and technical information collected 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 information about online activities, such as direct and social media interaction with our websites;

- **Compliance information:** results of background checks, including in relation to criminal data, sanctions, politically exposed persons or export control records, complaints or claims, investigations and other monitoring, reporting and remedial information; and
- **Contractual information:** information about existing contracts between us, between the individual and third parties;
- **Aggregate data:** this data may be derived from your personal data but is not considered personal data by law because such data, such as statistical or demographic data, will not directly or indirectly reveal your identity. However, if we combine or connect the aggregated data with your personal data, which may then directly or indirectly identify you, we treat this combined data as personal data, which will be used in accordance with this privacy notice;
- **Excluded data:** We do not collect the following special categories of personal data about you, unless it is legally required:
 - details of your race or ethnic origin ;
 - religious or philosophical beliefs ;
 - sex life ;
 - sexual orientation ;
 - political views ;
 - trade union membership; and,
 - genetic and biometric data that are not related to your contract.

We also do not collect information on criminal convictions and offences, except as part of our anti-money laundering and anti-terrorism procedures, if required by law or certain guidelines or regulations of a competent supervisory authority.

4 HOW WE USE YOUR PERSONAL DATA LEGALLY

We may use your personal data on various legal bases, subject to applicable data protection laws and regulations. We do not process your personal data for purposes incompatible with those notified to you through this notice.

Each processing operation is carried out on a single legal basis. We determine the legal basis for each individual treatment, depending on :

- the nature of the personal data we process; and
- the specific purpose for which we process personal data.

We may use each category of personal data we collect on the following legal grounds and for the following purposes:

- **With your consent (or that of your legal representative)**, your personal data is processed for the specific purpose(s) to which you have consented via contractual documents, standard forms, declarations or insurance intermediaries.

This includes:

- processing of health-related data (e.g. in the context of managing your insurance ;
- the installation of cookies or similar technologies on our websites that analyse browsing patterns in order to improve our websites;
- recording of telephone and/or video conversations for specific purposes.

You have the right to withdraw your consent at any time.

- **To perform our contractual obligations to you**

This includes:

- Management and execution of insurance contracts (including in our data collection systems or tools) comprising claims handling, monitoring of premium payments, informing customers, executing a specific customer request;
- the conclusion of an agreement ;
- pre-contractual steps taken after you have submitted an application for recruitment purposes;
- the processing of identification data for authentication purposes when you wish to log on to our IT platform;
- the technical cookies of our websites necessary for its proper functioning.

- **To fulfil a legal or regulatory obligation**

This includes:

- the preparation of legal or regulatory reports including those required to comply with our tax obligations (e.g. FATCA/CRSform);
- detecting, preventing and combating money laundering, terrorism and tax fraud;
- the application of insurance regulations and in particular the duty to provide information on products;
- the enforcement of obligations relating to financial embargoes and asset freezes.

- **To pursue our legitimate interests**, where your own legitimate interests and/or fundamental rights and freedoms do not override these and to the extent permitted by applicable laws and regulations, including :
 - to manage our interactions and business relationships with you, including responding to requests you have submitted via our websites, by telephone, e-mail or other means and to deal with any outstanding issues relating to those requests;
 - managing our insurance portfolios, carrying out business plans and risk analyses;
 - prevent or detect fraud, misrepresentation, security incidents or crime;
 - to protect the safety, property and rights of all persons who interact with us, including ensuring the health and safety of all persons on our premises, for example by means of security cameras in and around our premises;
 - to establish, exercise, defend and protect the rights of the Monument Group entities or those of persons we may represent (e.g. in litigation) and to gather evidence;
 - investigate any complaints received from you or others about our services;
 - obtain legal advice, support or representation for legal, compliance, regulatory and investigative purposes;
 - inform you of changes to our services, if any;
 - to present the content of our websites in the manner we consider most effective or to keep our websites safe and secure, to manage our business, to provide administrative and IT services, and to provide network security;
 - to draw up a global profile of our customers to best meet their needs;
 - test, evaluate, simplify, optimize and/or automate our internal processes, particularly in the management of files, our websites and platforms, and our distribution channels;
 - to become aware of the existence and content of communication (letters, telephone calls and e-mails) between our employees, customers and partners, and to store the communication and metadata for the purposes of evidence, quality control and/or training/coaching of our employees, as well as, in some cases, for use in the automation of our internal processes.
- **For such purposes as may be required or permitted by applicable data protection laws and regulations**, including any other secondary purposes consistent with the original purposes of processing personal data set out in this notice.

Whenever there is a need to process your personal data for purposes incompatible with those described above, we will inform you by updating this privacy notice and obtain your consent in accordance with applicable data protection laws and regulations before engaging in such further processing. We do not sell or intend to sell your personal data. For more information about your privacy rights, see section 9, "Your individual privacy rights", of this notice.

Please note that in certain circumstances the provision of personal data is a requirement of the contract we are administering. The provision of personal data in these circumstances is necessary to enable us to perform our legal obligations under that contract.

5 HOW WE SHARE YOUR PERSONAL DATA

In addition to our employees and advisors, we may disclose your personal data to other Monument Group entities, third party suppliers, service providers and business partners, law enforcement and other government agencies, companies with whom we are involved in a business transaction or any other third party on the legal grounds set out in this notice.

Where there is a legal basis (see section 4 of this notice), we may share your personal data with the categories of recipients described below (acting as "processor" or "controller"):

- **Other entities in the Monument group of companies.** We may share your personal data within our group of companies, which includes parents, affiliates, subsidiaries, business units and other companies whose shares are jointly owned or controlled, for the purposes and using the legal bases set out in this notice, and their advisers and consultants.
- **Third party suppliers of goods and services, partners and other businesses.** We may share your personal data with third parties working on our behalf to facilitate our interactions with you or to request or support our relationship with you. These include companies involved in contract or claims management, medical consultants, medical or technical experts or advisors, insurance intermediaries, lawyers, bailiffs, banks, external commissioners/auditors, IT service providers, document management companies (cloud, scanning, archiving, mailing, etc.), insurance companies for co-insurance or reinsurance purposes.
- **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. These include social, tax, administrative authorities as determined by law, regulatory authorities and the insurance ombudsman.
- **Companies involved in a corporate transaction with us.** If we acquire insurance portfolios or other companies, or sell some or all of our assets, merge with or are acquired by another entity, or otherwise restructure our business, including through a sale or bankruptcy, we may share your personal data with these entities only as necessary for the purposes of the relevant transaction.

6 CROSS-BORDER TRANSFERS OF PERSONAL DATA

In some cases, we may need to transfer your personal data from the country of origin to another country for processing. Where personal data is 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 when it reaches its destination, as required by applicable data protection laws and regulations.

In some cases, it may be necessary for us to transfer your personal data to a Monument group entity or third party as listed in section 5. of this notice outside the country where it was collected. Our operations extend to

a number of countries including Bermuda, the United Kingdom, Singapore, Ireland, Luxembourg, Belgium, Guernsey, Isle of Man, Spain and Italy. Third party recipients include organisations that we engage with to provide our products and services to you. In doing so, we rely on a number of legal mechanisms to ensure that your data remains protected to an equivalent level to that afforded in the country of origin. Depending on the destination of the personal data transfer, this includes European Commission adequacy decisions and standard contractual clauses, UK adequacy decisions and standard contractual clauses, and other legally binding safeguards, including binding corporate rules under applicable data protection laws and regulations. A copy of the relevant mechanism and information on the safeguards we have in place can be made available on request by contacting us (see section 10 of this notice).

7 HOW WE PROTECT AND SECURE YOUR DATA

Monument Assurance Belgium has implemented technological and operational security procedures designed to protect your personal data from loss, disclosure, misuse, alteration or accidental or unlawful use.

We restrict access to your personal data only to our employees and third parties on the basis of a business need to know for the performance of their duties, the fulfilment of a contractual/legal obligation or with regard to the legitimate interest that justifies such transfer. In accordance with the relevant legislation, the parties will only process your personal data on our instructions and are subject to a duty of confidentiality. Third parties are not permitted to use your personal data for their own purposes. We have procedures in place to respond appropriately to any suspected breach of legislation or security incident and will inform you and the relevant data protection regulators where we are legally required to do so.

With regard to our subcontractors, we systematically enter into a data processing contract with each of them. 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 legal and regulatory requirements and our legitimate interest.

Unless there are specific legal time limits, data will in principle be kept for up to 10 years after the end of the contractual relationship with the customer.

For data relating to insurance, different periods may apply depending on the type of insurance. In the case of life insurance, this period may extend to 30 years.

At the end of its retention period, which is 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 purpose for doing so and if there is a legal basis for doing so under applicable data protection laws and regulations. If this is the case, we will retain only the personal data required for the new purpose and implement systems and controls over that data in accordance with applicable data protection laws and regulations.

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

9 INDIVIDUAL RIGHTS TO PRIVACY

Individuals whose personal data we process have a number of rights in relation to that data. To exercise your data protection rights, please contact us (see section 10. Contact Us of this Notice). We will respond to requests in accordance with applicable data protection laws and regulations.

The specific data protection rights applicable to you are detailed in the table below. Please note that these data protection rights are not absolute and there may be circumstances in which we can legitimately refuse a request as permitted by applicable data protection laws and regulations.

You will not be charged a fee to access your personal data or to exercise any of the other rights set out below. However, if your request is unfounded, repetitive or excessive, we may charge a reasonable fee for providing the information or communication.

We may need to ask you for specific information to help us confirm your identity and to 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 anyone who does not have a right to receive it. We may also contact you to request further information about your request in order to expedite our response. We will only collect information that is strictly necessary to ensure that we only honour requests received from the actual person concerned or their authorised representative. We aim to respond to all legitimate requests within one month in accordance with applicable data protection regulations. Sometimes it may take us longer to respond if your request is particularly complex or if you have made a number of different requests.

In this case, we will inform you of the estimated response time.

INDIVIDUAL RIGHTS TO PRIVACY	
Right to information	The right to receive the information set out in this Notice about the processing of your personal data.
Right to object	The right to refuse the processing of your personal data in certain legal circumstances.
Right to limitation	The right to ask us to suspend the processing of your personal data in specific circumstances.
Right of deletion	The right to ask us to delete or withdraw personal data where there is no legal reason for us to continue processing it.
Right of access	The right to receive a copy of or access to the personal data we hold about you.
Right of rectification	The right to ask us to correct or complete any inaccurate personal data we may hold about you.
Right to portability	You have the right to request the transfer of your personal data collected by us to a third party controller or directly to you in a structured, commonly used and machine-readable format under certain legal conditions.
Right to complain / appeal	If you believe that the processing of your personal data constitutes a breach of the relevant legislation, you have the right to lodge a complaint with the Belgian Data Protection Authority (Contact: rue de la Presse 35, 1000 Brussels, Tel. +32 2 274 48 00). However, we thank you for giving us the opportunity to address your concerns before contacting the DPA and invite you to contact us in the first instance by e-mail or by post (see section 10. Contact us of this notice).
Right to withdraw consent	The right to withdraw, at any time, the consent you have given us to process your personal data (where the legal basis on which we rely is consent).
Rights relating to automated decision-making and profiling	You have the right not to be subject to a decision based solely on automated processing, except where permitted by law.

10 CONTACT US

If you have any questions, concerns and/or complaints about this notice or if you wish to exercise your data protection rights above, please contact the Data Protection Officer using the following means

- E-mail: dataprotection@monumentassurance.com
- Position: Monument Assurance Belgium
For the attention of the Data Protection Officer
Boulevard du Roi Albert II 19
1210 Brussels

11 MAIN CHANGES COMPARED TO THE PREVIOUS VERSION

In this new version of the Privacy Notice, you will learn more about the personal data we process and collect.