PRIVACY POLICY

To ensure that insurance companies are able to carry out their tasks in a more effective and secure manner, electronic data processing (**EDP**) today has become indispensable in everyday business. Data processing can be used to assist with processing contractual relationships correctly, quickly and in a cost-efficient manner. In addition, in direct comparison with manual procedures, EDP offers the insured community better protection against abusive actions.

Element Insurance AG (referred to as "we", "us", "our" or "ELEMENT" in this notice) is committed to protecting the personal data of its policyholders (referred to as "you" or "your" in this notice). Element is a controller and the processing of your personal data is subject to the General Data Protection Regulation (GDPR). You can contact us and our data protection officer by e-mail at datenschutz@element.in or by post at ELEMENT Insurance AG, Attn: Data Protection Officer, Saarbrücker Str. 37A, 10405, Berlin, Germany.

I. WHY WE PROCESS YOUR DATA

When taking out your insurance cover, as part of the application procedure, you provided us with the personal data required for the execution of the contract (**application data**).

We process this data to the extent necessary for the conclusion and performance of the insurance contract.

In addition, **actuarial data** such as customer number (partner number), insured sum, term of insurance, premium, bank details and, if necessary, the details of a third party, e.g. an intermediary or appraiser are collected (**contract data**). In the event of a claim, we will store your information on the damage and also information from third parties, such as appraisals, invoices or the amount of the payout (**benefit data**).

Automated decision making including profiling according to Art. 22 GDPR does not take place.

This data is processed to enable us to provide you with insurance cover in line with your policy.

II. LEGAL BASIS FOR PROCESSING

We process your data to enable us to provide you with insurance cover in accordance with point (b) of Article 6(1) GDPR and - in case of processing of special categories of personal data as defined in Article 9(1) GDPR (in particular, health data) - based on your consent in accordance with point (a) of Article 9(2) GDPR.

We also process your data to protect legitimate interests pursued by us or third parties (point (f) of Article 6(1) GDPR). This may especially be necessary to ensure IT security and IT operations, and to prevent and investigate criminal acts; in particular, we use data analyses to detect indications that may be indicative of insurance fraud.

In addition, we process your personal data to comply with legal obligations, e.g. regulatory requirements, retention obligations under commercial or tax law, or our obligation to provide advice.

The legal basis for the processing in this case is the respective statutory regulations in conjunction with point (c) of Article 6(1) GDPR.

III. PROCESSING OUTSIDE THE EUROPEAN UNION, WEB HOSTING, CONTACT, PAYMENT SERVICE PROVIDER

Subject to express consent or in case of transfers required by contract or law, we only process or have data processed in third countries with an adequate level of data protection, contractual obligation through the EU Commission's so-called standard data protection clauses, existing certifications or binding corporate data protection regulations (Articles 44 to 49 GDPR, EU Commission information page).

For data processing, we rely on cloud hosting services from external providers. In this respect, we have opted for the services of Amazon Web Services (AWS) and Salesforce (cloud provider). In doing so, we exclusively use European server locations in order to comply with the EU's special requirements with regard to data processing; we use data centers as the main instances we use data centers in Frankfurt am Main, and as backup instances we use data centers in Frankfurt am Main and Paris.The cloud providers meet the highest data protection and data security requirements and are ISO-27001 certified, among other things.

In the course of processing by a cloud provider, some processing activities may take place on servers in the USA, if there is specific authorization for this. For more information, please refer to AWS Security, Identity and Compliance and Salesforce Trust and Compliance.

We use Salesforce. com Inc. as a provider to manage contact requests and communication. This covers the processing of the content of all electronic communication (e.g. e-mail addresses, content, attachments). Contact requests in the context of contractual or pre-contractual relationships are answered in order to comply with our contractual obligations or to respond to (pre-) contractual inquiries and therefore on the basis of point (b) of Article 6(1) GDPR. Moreover, processing is based on our legitimate interests in responding to the requests in accordance with point (f) of Article 6(1) GDPR, so as to ensure the fast and coherent processing of incoming requests. Only servers located within the EU are used for processing. Salesforce is a certified licensee of the TRUSTe Privacy Seal. For more information, see Salesforce Privacy.

For payment processing, we use carefully selected, reliable and PSD-II certified payment service providers, currently Stripe Payments Europe, Ltd. The data required for processing - e.g. credit card number, CVV, valid dates, IBAN or payment amount - (**payment data**) is processed directly by the payment service provider. The entered credit card information is not stored by ELEMENT. ELEMENT only stores a payment token for credit card payments that has been rendered anonymous. ELEMENT uses payment service providers on the basis of legitimate interest in accordance with point (f) of Article 6(1) GDPR in order to ensure the security of payment processing. With specific authorization, processing may be carried out using servers located outside the European Union, in particular in the USA. For further details, see Stripe Global Privacy Policy available in the Stripe Privacy Center.

IV. DATA TRANSFER TO REINSURERS

In the interests of our insurance holders, we will always ensure that any risks assumed by us are balanced. This is why, in many cases, we pass on part of the risks to reinsurers in Germany and abroad. These reinsurers also require corresponding actuarial information from us, such as policy number, premium, type of insurance cover as well as risk and risk premium and - in individual cases - your personal details as well. In addition, where reinsurers are involved in the assessment of risks

and losses, they are provided with the relevant required documents. In some cases, reinsurers involve additional reinsurers and also transfer the corresponding data to them.

V. DATA TRANSFER TO OTHER INSURERS

You are obligated to answer all questions when you apply, to notify us of any changes relevant to your contract and, in the event of a claim, of all circumstances that are of significance for the assessment of the risk and the settlement of the claim. This includes, e.g., previous claims or notifications of other, similar insurance policies (applied for, existing, refused or terminated). To prevent insurance fraud, to clarify potential contradictions in the information provided by the insured person or so as to close gaps in the findings on the incurred loss, it may be necessary to request information from other insurers or to provide corresponding information in response to inquiries.

In certain other cases (double insurance, statutory subrogation as well as in the case of sharing agreements), personal data also needs to be exchanged between the insurers. In such cases, data of the data subject is disclosed, such as name and address, type of insurance cover and risk or details of the damage, such as the amount or date of the damage.

VI. DATA TRANSFER TO APPRAISERS (VALUERS)

In the context of claims assessment, it is necessary to transfer actuarial data, information on the type and scope of insurance cover as well as your information about the claim to the persons in charge of the claims assessment (valuers), in order to enable them to determine the amount of the claim.

VII. INSURANCE INTERMEDIARIES / PARTNERS

If your insurance contracts are handled by an intermediary , they process the application, contract and claims data as necessary for conclusion and performance of the contract. We also transfer this data to your intermediary if they require the information to assist and advise you with regard to your insurance and financial services matters. If you have taken out insurance through one of our sales or cooperation partners, we will transfer your application, contract and claims data if this is necessary to execute the insurance relationship or for administrative purposes, such as settlement with the partner.

VIII. EXTERNAL SERVICE PROVIDERS

In some instances, we use additional external service providers in order to comply with our contractual and legal obligations.

A current schedule of the contractors and service providers we use not merely on a temporary basis is available on our website under this link https://documents.element.in/hubfs/Legal_Files/2023-10-31%20%20WE%20IRE%20List%20of%20service%20providers.pdf

IX. OTHER RECIPIENTS

In addition, we may transfer your personal data to other recipients, such as authorities, in order to comply with statutory reporting obligations (e.g. social insurance carriers, tax authorities or law enforcement agencies), if we are required to do so.

X. CENTRAL INFORMATION SYSTEMS

When examining an application or a claim, assessing the risk, further clarifying the facts or preventing insurance fraud, it may be necessary to inquire with the relevant trade association or with other insurers or to respond to corresponding inquiries by other insurers. Central information systems are in place for this purpose that may be tracked with the respective system, thus only if certain requirements are met.

XI. FURTHER INFORMATION AND EXPLANATIONS OF YOUR RIGHTS

As a data subject, you have the right to request information about the processing by us (access right). We will explain the data processing in the context of providing information about the data being processed or provide an overview (copy) of the data processed. If any data stored by us is incorrect or no longer up to date, you have the right to have this data rectified. You may also request the erasure of such data. If, as an exception, erasure is not possible due to other legal requirements, the data will be made unavailable with the effect that it is only available for this statutory purpose. You may also have the processing of your data restricted, e.g. if you believe that the data stored by us is not accurate. You also have the right to data portability, i.e. upon request, we will provide you with a digital copy of your provided personal data.

If you have given your consent to the processing of your data, you may withdraw this consent at any time. A withdrawal does not effect the permissibility of the processing of your data carried out prior to your withdrawal.

If we base the processing of your data on a legitimate interest pursuant to point (f) of Article 6(1) GDPR, you may object to the processing. Should you object, we request that you explain the reasons why we should not process your data. In the event of your reasoned objection, we will review the facts of the case and either cease or adapt processing or notify you of our compelling legitimate interests which allow us to continue the processing.

You may contact us at any time as detailed above in order to exercise the rights described.

You also have the right to lodge a complaint with any data protection supervisory authority within the European Union, in particular in the Member State of your habitual residence, place of work or place of the alleged infringement. A list of competent authorities is available under the following link https://edpb.europa.eu/about-edpb/about-edpb/members_en#member-es

XII. DURATION OF DATA RETENTION

We will delete your personal data as soon as they are no longer required for the purposes described above. It may be the case that personal data is retained for the period of time during which claims may be asserted against our company (statutory period of limitation of three or up to thirty years). In addition, we also retain your personal data where we are required by law to do so. The relevant obligations to provide proof and retention obligations follow from the German Commercial Code, the German Fiscal Code and the German Money Laundering Act, among others to which the data controller is subject. The retention periods under these laws are up to ten years.
Data in retention before deletion will be blocked, which means that they will not be further processed, except in special cases provided for by law.