

## Privacy Statement

### 1. About us

In supplying our services, we are responsible for processing personal data. Under the General Data Protection Regulation, that makes us Controller. This responsibility is shared between us and those insurance companies that have authorised us to perform their insurance policies.

### 2. What personal data do we process?

When you, or your employer, applies for insurance or any other service from us, we will request personal data. This data is provided by you, or your employer, through your (employer's) advisor/intermediary (hereinafter: advisor). If you are a customer with us, in certain situations we may also ask you to provide personal data directly.

#### *NAP details (Name, Address, Phone number)*

The personal data we process depends on the type of contact we have had with you:

- If you visit our website and use our systems, we collect data about your visit to our website via your IP address, cookies, and cookie settings. We only use cookies to improve the functionality of our website and services.
- If you request information from us, we will ask for your contact details so as to be able to provide the information to you.
- When you become a customer, we will require, at least, your contact details (name, address, domicile, phone number, and e-mail address). This data is used by us to perform the (insurance) agreement we entered into, with you.
- When you apply for a job with us, we will request your CV, we may request copies of your diplomas, and possibly other personal data. This data is stored, with your permission, for up to 12 months after your application.

#### *Financial data*

If you are a customer of ours, we will use your bank account number to make and collect payments, and to transfer any monetary value of damages owed to you by us.

In addition, we will have access to your salary details if you, or your employer, take out one of our income insurance policies.

#### *Additional data*

For certain products we require additional information from you, for example your vehicle's licence plate number in case of a car insurance, or your profession or medical data for an income insurance. This data we use for, among other things, risk assessments, determining the terms and conditions of the product, and assessing any potential insurance claims for damages.

#### *Medical data*

To accept and perform income insurance policies, and for the processing of injury treatment claims, we require information about your health. Sometimes we may require information from your physician. In case we require information from your physician we will always request your permission, prior to obtaining such information.

Our employees only process health data they require for the performance of their work. Those employees are under a duty of confidentiality for all data they process. Processing of your health details

takes place within a special, separate unit (functional unit) of the relevant insurance company, under the responsibility of their medical advisor. The medical advisor is a BIG (Professions in Individual Healthcare) registered healthcare specialist. They adhere to the rules set out in the Professional Code for Healthcare Advisors working in Private Insurance Companies (Beroepscode voor Geneeskundig Adviseurs werkzaam in Particuliere Verzekeringszaken en/of Personenschadezaken).

Are you dealing with an injury or work disability claim? Then you will receive a separate brochure for individual insurance policies, containing an explanation of how your data is used.

For the assessment and processing of claims issued by your employer, under an insured continued payment of wages obligation, we also process your health details. In doing so, we always adhere to the guidelines set out in the most recent version of the Privacy Income Insurances Manual (Handleiding Privacy Inkomensverzekeringen), as written by the Association of Insurers (Verbond van Verzekeraars OVAL).

#### *Criminal past*

For the risk assessment of damage and income insurances we ask you to provide information about the existence or absence of a criminal past. Criminal offences committed more than 8 years prior do not need to be reported to us. Criminal data on, for example, your application form will only be processed by authorised employees.

#### *Burgerservice nummer /Social Security number (BSN)*

In some cases, we will also process your BSN. For example, for income insurance policies that fall under the Dutch Pensions Act. We will only process your BSN where we are legally required to do so.

#### *Data about your communication with us*

We process data about the contact you have had with us, in case you have asked us a question, or when you have filed a complaint with us. Your complaint is recorded in our complaints administration.

### **3. How do we acquire your personal data?**

In most cases we obtain your details from your (employer's) advisor. We may also obtain and process data from other parties, such as the DWP (UWV), valuers, damage experts, or Health and Safety services. Our processing register records the source that we obtained data from whenever we know the sources. We will keep you informed as much as possible about the sources that have provided data to us.

### **4. Why do we process personal data?**

We process personal data for the following purposes:

#### *For the performance of our services*

We use personal data to contact you, to investigate whether you are eligible to take out insurance with us, or to process changes to your policy. We may also use your data to manage your insurance policies – or the insurance policies of your employer, such as income insurance – and to process claims, declarations, and damages.

#### *Risk reduction*

We use your personal data to reduce risks, by, among other things:

- Ensuring proper security, for example through the storage of usernames, passwords, and security questions.

- Performing internal quality assessments to identify and test potential problems and risks and to test whether legislation has been implemented adequately and is complied with.
- Ensuring that we remain a solvent and healthy company (risk management).

#### *Marketing activities*

We would like to keep you informed about our services. We may keep you informed about new developments or additional services that may be relevant to you, via e-mails, newsletters, our website, and on social media. Do you prefer not to receive such information? Then you can unsubscribe via any message you receive from us.

#### *Improvement and innovation*

We use personal data for the continuous improvement of our products and services. To do this, we generate reports and analyses of our services. In writing these, we will remove the personal data that is not required where possible, we may also bundle data to certain abstraction levels (aggregating), encrypt (pseudonymisation), or anonymise data.

#### *Uncovering fraud and misuse*

In the investigation of fraud, misuse, and improper use we also record personal data. In doing so, we adhere to the instructions that insurance companies provide us with.

### **5. On what legal grounds do we process personal data?**

Processing of personal data is only permitted where we have legal grounds to do so. In doing so, we follow the following rationale:

- The processing is necessary for the performance of the agreement, for example the insurance agreement.
- The processing is necessary to comply with a legal requirement, for example in case we request a copy of a proof of identity document to identify you.
- The processing is necessary to accommodate a legitimate interest, for example, when we instigate an investigation into potential fraud. In doing so, we weigh up our, or a third party's legitimate interests against yours.

### **6. How do we secure your personal data?**

We exercise the highest degree of care in treating personal data and have taken technical and organisational measures to secure personal data against loss or illegitimate use. These measures include, for example, measures for the safety and the prevention of misuse of our website or IT systems. But also, security of physical environments where data is stored.

We have an information security policy and ensure that our employees have the required knowledge of the field of personal data protection. Only authorised personnel can view and process your data.

We also require the suppliers of our software and IT systems to implement security measures of at least an equal standard.

All of our employees have signed a confidentiality statement and sworn an oath or promise. In this oath or promise, employees promise and/or declare that they will comply with the legislation, regulations and codes of practice and will conduct themselves with integrity.

### **7. How long do we store personal data for?**

We do not store personal data any longer than necessary. In some cases, the law defines the amount of time we are required, or obliged, to store information for. In other cases, we determine the amount of time we require your data for ourselves. To this end we have written a storage duration policy.

### **8. Who do we share personal data with?**

We will share personal data with third parties where this is permitted by law and necessary for the operational management of our business. We share personal data with:

- Our employees, when they are directly involved with the service or insurance engaged by you or your employer;
- Departments, subsidiary and sister companies. This way we can efficiently process your application and retain oversight of the services you acquire from us. This allows us to provide better service, for example by changing your address in all of our systems, based on a single change of address notification;
- Your employer, where this is necessary for the processing of claims under income insurance policies;
- The government, if we have a legal obligation to do so. This could include revenue services, the DWP, the police, the justice department, or regulators, such as the Authority on Financial Markets (AFM) and the Authority on Personal data;
- Your advisor, in so far as we are legally permitted, and where necessary for providing our services;
- Businesses engaged by us to perform services related to your (employer's) insurance agreement with us. This could include debt collection agencies, independent expert firms, Health and Safety services, legal representatives, or insurance companies;
- Databank CIS; to run a responsible acceptance and risk management policy, and so as to prevent fraud, we record personal data in the Central Information System of the CIS Institute in The Hague. The CIS Institute is an institute that is able to support insurance companies in acceptance and claim processes. Between insurers connected to CIS we can, under strict conditions, exchange information via the CIS Institute. More information about this can be found on the [Stichting CIS](#) website.

We may also outsource the processing of personal data to third parties. Under the law, those third parties then become processors of personal data. For example, we make use of IT service providers for maintenance and support. Those parties are regarded as processors because they themselves have no authority over the personal data regarding our products and services. In this situation we remain responsible for the careful processing of personal data.

### **9. What are your rights?**

The General Data Protection Regulation gives you several rights, which you can exercise in regard to us. Please find below these rights, and how to exercise them in our regard.

*Access and rectification of personal data*

You have the right to ask us what personal data of yours we process and to have any incorrect data corrected or removed. Requests to view or correct your information can be sent to our Compliance Department using the contact details below:

Compliance department  
F.A.O. Data Protection Officer  
Postbus 2007  
199. AA Velsbroek  
The Netherlands

We will ask security questions or request a copy of your proof of identity document to identify you. You will receive a response from us within four weeks.

*Proof of Identity document*

When providing a copy of your proof of identity document you will need to redact your passport photo and Citizen Service/Social Security number. We also advise that you stipulate on this copy that it is intended only for use in the exercise of your rights regarding your personal data.

*The right to erasure/be forgotten*

In some cases, and under some circumstances, you have the right to have the personal data we have of you erased. This is the case if:

- The personal data are no longer required for the purposes for which they were collected or processed;
- You legitimately object against its processing;
- Your personal data have been illegitimately processed by us;
- We are legally required to erase the personal data.

The right to be forgotten is not an absolute right.

We may decide not to comply with your request, and thus not to erase your data, if your request is not based on one of the above grounds, or (i) to allow exercising of the right to freedom of expression and information; (ii) to comply with a legal requirement; or (iii) to instigate, exercise, or underpin a legal claim.

If we do not comply with your request to have your personal data erased, we will inform you accordingly about the reasons why we will not be complying with your request.

*Restriction of processing*

If you are of the opinion that we have illegitimately processed your personal data, or that the data processed by us is incorrect, you can request restriction of processing. This means that we would no longer be permitted to process that data.

*Transfer of data (data portability)*

You have the right to receive a copy of the personal data that you have provided to us for the performance of an agreement that you have entered into, with us. This only concerns the personal data we have received from you personally, not the data that we received from third parties. The aim of this right is to make it more convenient for you to supply this data to a different party.

*Right to object*

You retain the right, at all times, to object to the processing of your personal data taking place on the basis of our legitimate interest, or the legitimate interest of a third party.

In such cases we will no longer process your data, unless binding legitimate grounds for the processing of that data outweigh your personal interest, or unless the processing of that data is in connection with the institution, performance, or underpinning of a legal claim.

*Unsubscribing from offers*

We only approach business relations with offers. You have the right to unsubscribe from newsletters or offers about ours and connected services. In commercial offers we will always include an option to unsubscribe.

**10. Social Media**

You may choose to contact us via social media pages, such as Facebook and LinkedIn. To be able to respond to personal questions in your social media message, we will ask you via a private message (direct message or e-mail), to share your contact details with us. This allows us to check that we are speaking to the right person.

This Privacy Statement is applicable to the data we receive from you via these platforms. The use of social media falls under your personal responsibility. This Privacy Statement does not apply to the way the social media platforms deal with the personal data you provide. Please note that many social media platforms are based outside of the European Union and that they store data outside of the European Union. Privacy laws of the European Union is often not applicable in those circumstances.

We advise you to consult the Privacy Statements of these social media platforms for more information about the way they process personal data.

**11. Amending the Privacy Statement**

Privacy legislation is under development. For that reason, we reserve the right to amend this Privacy Statement to keep it up-to-date. We will do so to incorporate new developments, for example, if something changes within our business activities, the law, or jurisprudence. Therefore, we recommend that you regularly revisit this Privacy Statement when visiting our websites. We will also actively inform you about changes to this Privacy Statement by e-mail or newsletter.

**12. Questions or complaints**

If you have any questions about this Privacy Statement, or if you have a privacy-related complaint, please contact our Data Protection Functionary.

Compliance Department:  
F.A.O. Data Protection Officer  
Postbus 2085  
1990 AB Velsbroek  
The Netherlands

Alternatively, you can always file a complaint with the Authority on Personal data. For more information please visit [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) or call 0900-2001201.

This Privacy Statement was last updated on May 4<sup>th</sup>, 2018