

## Privacy notice for customers of the Wesleyan Group of Companies

### WHAT IS THE PURPOSE OF THIS DOCUMENT?

The Wesleyan Group of Companies (known as “Wesleyan”, “we”, “our”, “us”) is committed to protecting the privacy and security of your personal information. You may have a relationship with one or more of our companies, including Wesleyan Assurance Society, Wesleyan Bank Ltd, Wesleyan Financial Services Ltd and Wesleyan Unit Trust Managers Ltd. Further details about our Group of Companies can be found [here \(www.wesleyan.co.uk/legal-disclaimer/\)](http://www.wesleyan.co.uk/legal-disclaimer/). Our address is Colmore Circus, Birmingham B4 6AR.

This notice applies to prospective customers, current customers and former customers to the Wesleyan Group of Companies and describes how we collect and use personal information about you in accordance with the General Data Protection Regulations (“GDPR”) and other data protection laws. Customers of Practice Plan, DPAS and Quality Plan will receive a separate privacy notice specific to the products and services they each provide.

Wesleyan is a “controller”. This means that we are responsible for deciding how we hold and use personal information about you. It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information. We may update this notice at any time.

### THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

Depending on the services and products we provide to you, we may collect, store, and use the following categories of personal information about you:

- ▶ Personal details such as name, title, addresses, telephone numbers, personal email addresses, date of birth, gender, marital status and details about dependants and next of kin
- ▶ National Insurance number and other copies of document to confirm your identity
- ▶ Passport information and information about your travel plans, dates of travel, destination(s) and planned activities
- ▶ Driving licence information and information about your vehicle(s), past claims, recent damage
- ▶ Bank account details, payroll records, tax status information and credit scores
- ▶ Details of bankruptcies
- ▶ Information about your employment records (including salary, pension and benefits information, job titles, work history, working hours, training records and professional memberships, location of employment or workplace)

We may also collect, store and use the following “special categories” of more sensitive personal information:

- ▶ Information about your race, ethnicity or sexual orientation (where any of these could be established from information you provide to us)
- ▶ Information about your health, including any medical condition, health and sickness records (where this is relevant to policies we offer, such as health insurance, as well as processing any subsequent claims)
- ▶ Information about criminal convictions and offences (as part of our fraud prevention checks and where this is relevant to policies such as motor insurance)

## HOW IS YOUR PERSONAL INFORMATION COLLECTED?

There are a number of ways in which we collect your personal information, the main way is directly from you such as:

- ▶ Enquiry, quotes, claim and application forms you submit or emails or correspondence you may send to us
- ▶ When you consider purchasing or actually purchase a product or service from us
- ▶ Telephone calls with you (which maybe recorded)
- ▶ Via cookies when you access our websites, applications, social media (such as Facebook pixels) or emails (see our cookie policy for further information)
- ▶ When you create a MyWes account

and we may also collect your information from third parties such as:

- ▶ Where you have agreed for your information to be passed onto us (e.g. by a family member when you may not be able to disclose the relevant information directly or by a third party referrer who is introducing business to us)
- ▶ Credit reference agencies or other background check agencies
- ▶ Medical professionals (where you have agreed to this)

By passing us any information about another person, you confirm you have their authority to share that information with us.

## HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you and for pre-contract administration
2. Where we need to comply with a legal obligation
3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests
4. Where you have given your consent to do so for a specific purpose

## Situations in which we will use your personal information

We need all the categories of information in the list above (see [The kind of information we hold about you](#)) primarily to allow us to perform our contract with you [\*] and to enable us to comply with legal obligations [\*\*]. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties [\*\*\*], provided your interests and fundamental rights do not override those interests and where you have given us your consent to process your information [\*\*\*\*] The situations in which we will process your personal information are listed below. We have indicated by [asterisks] the purpose or purposes for which we are processing or will process your personal information.

- ▶ Evaluating your application and providing you with a quote (this maybe provided directly by us or a preferred third party) [\*]
- ▶ Administering and servicing the contract we have entered into with you (or propose to enter into with you) and managing the product or facility, which may include any mutual benefits that you may be entitled to [\*]

- ▶ Claims management (in relation to policies you hold with us or via a third party which are managed by us) [\* , \*\* , \*\*\*]
- ▶ Claims management (in relation to policies you hold with us or via a third party which are managed by us) [\* , \*\* , \*\*\*]
- ▶ Anti-fraud and money laundering purposes (to detect and prevent fraudulent claims) [\*\* , \*\*\*]
- ▶ Providing you with information about products and services based upon any preferences you may have expressed and/or which we think might be of interest (marketing purposes) [\*\*\* , \*\*\*\*]
- ▶ Recovering debt [\*\*\*]
- ▶ Complaints management (if you are not happy with the service we have provided you) [\*\*\*]
- ▶ Business management and planning, including quality, testing, training, accounting, auditing purposes and market research [\*\*\*]
- ▶ Running events and/or competitions [\*\*\*]

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

### **If you fail to provide personal information**

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into (or are proposing to enter into) with you or we may be prevented from complying with our legal obligations (such as detecting or investigating fraud) and so we may be required to decline an application or claim.

### **Change of purpose**

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

## **HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION**

Special categories of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. With your explicit consent
2. Where it is in the substantial public interest and in line with our data protection policy

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

### **Do we need your consent?**

We may approach you for your approval to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it. Without this approval, in some circumstances, we may not be able to provide you with cover under the policy, handle claims or you may not be able to benefit from some of our services.

## INFORMATION ABOUT CRIMINAL CONVICTIONS

We envisage that we may hold information about criminal convictions you may have but we will only collect such information if it is necessary given the nature of the product you wish to purchase from us and where we are legally able to do so e.g. to assess and provide you with a quote for various insurance products and as part of our fraud prevention checks.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

## AUTOMATED DECISION-MAKING, FRAUD PREVENTION AND CREDIT REFERENCING

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.
2. Where it is necessary for entering into or to perform the contract with you and appropriate measures are in place to safeguard your rights.
3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights and freedoms and legitimate interests.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest and we must also put in place appropriate measures to safeguard your rights and freedoms and legitimate interests.

As part of the processing of your personal data, decisions may be made by automated means by putting your information into a system and the decision is calculated using automatic processes. We may make automated decisions about you in the following situations:

Where you pose a fraud or money laundering risk e.g. if:

- ▶ our processing reveals your behaviour to be consistent with that of known fraudsters or money launderers or is inconsistent with your previous submissions; or
- ▶ you appear to have deliberately hidden your true identity and/or you have provided false or inaccurate information

When deciding your premium for insurance products and assessing applications e.g.:

- ▶ depending on the type of insurance product you apply for our processing of your personal and/or sensitive information may be used to assess the price and determine whether there are any exclusions that need to be applied to the policy

The results of these checks may affect the type of products and services we can offer you. You have rights in relation to automated decision making: if you want to know more please contact our Data Protection Officer, details of which can be found at the end of this privacy notice. If we are unable to undertake the checks outlined above, it may not be possible for us to offer certain services or products to you.

When we and fraud prevention agencies process your personal data, we do so on the basis that we have a legitimate interest in preventing fraud and money laundering and to verify your identity in order to protect our business and to comply with laws that apply to us. Such processing is also a contractual requirement of the services or financing you have requested.

If we, or a fraud prevention agency, determine that you pose a fraud or money laundering risk, we may refuse to provide the products, services and/or financing you have requested or we may stop providing existing services to you.

We, and fraud prevention agencies may also enable law enforcement agencies to access and use your personal data to detect, investigate and prevent crime.

Fraud prevention agencies can hold your personal data for different periods of time, and if you are considered to pose a fraud or money laundering risk, your data can be held for up to six years and may result in others refusing to provide products, services, financing or employment to you.

A record of any fraud or money laundering risk will be retained by the fraud prevention agencies, and may result in others refusing to provide services, financing or employment to you. If you have any questions about this, please contact us on the details above.

Where you are applying for credit, we may also use credit scoring. This means existing and historic data about you may be used to determine your ability to make future payments. This allows us to make responsible lending decisions. The identities of the Credit Reference Agencies, and the ways in which they use and share personal information, are explained in more detail at [www.experian.co.uk/crain](http://www.experian.co.uk/crain)

## DATA SHARING

We will share your data with third parties, including third-party service providers and other entities in the Wesleyan Group of Companies. We require third parties to respect the security of your data and to treat it in accordance with the law. If you are a joint applicant or you have a joint product or policy, we may disclose your information where necessary to other joint applicants.

### Why might you share my personal information with third parties?

We may share your personal information with third parties where required by law, where it is necessary to administer the contracts we, or a third party may, have with you, where we have another legitimate interest in doing so or where you have asked us to pass your data to a third party e.g. lawyers, other mortgage providers etc. We also share personal data for crime and fraud prevention, credit reference and the apprehension and prosecution of offenders.

### Which third-party service providers process my personal information?

We may transfer or disclose your personal data to the following categories of recipients:

- ▶ other members of the Wesleyan Group of Companies as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data or to help us identify products and services which may be of interest to you
- ▶ third-party service providers (including IT suppliers, auditors, marketing agencies, market researchers, document management providers and underwriting services)

### How secure is your information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in our group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

## What about other third parties?

We may share your personal information with other third parties who may process your personal data and will have their own obligation to comply with Data Protection laws, such as:

- ▶ other third parties who are associated with the supply of products and services in relation to the contract we hold with you e.g. third party providers/lenders who form part of our panel(s). If you would like further information on these third parties, please contact your appointed Financial Consultant or a member of the Customer Relationship Centre.
- ▶ our regulators (Financial Conduct Authority (FCA), Prudential Regulatory Authority (PRA), Information Commissioners Office (ICO)) and the Financial Ombudsman Service (FOS)
- ▶ government agencies/ law enforcement
- ▶ fraud prevention agencies
- ▶ credit reference agencies
- ▶ third parties as part of any possible sale or restructuring of our Group of Companies
- ▶ Motor Insurance Information Centre (MIIC)

If you hold a motor insurance policy your details will be added to the Motor Insurance Database (MID), run by the Motor Insurers Information Centre (MIIC). MID data may be used by the DVLA and DVLNI for the purpose of Electronic Vehicle Licensing and by the Police for the purposes of establishing whether a driver's use of the vehicle is likely to be covered by a motor insurance policy and/or for preventing and detecting crime. If you are involved in an accident (in the UK or abroad) other UK insurers, the Motor Insurer's Bureau and MIIC may search the MID to ascertain relevant policy information. Persons with a valid claim in respect of a road traffic accident (including citizens of other countries) may also obtain relevant information which is held on the MID.

You can find out more about this from your insurer or at [www.miic.org.uk](http://www.miic.org.uk)

You should show this statement regarding MIIC to anyone insured to drive the vehicle covered under the policy.

A credit reference check will add to your record details of our searches and your application. This record (but not our name) will be seen by other organisations when you apply for credit in the future. A large number of applications within a short period of time could affect your ability to obtain credit.

## Transferring information outside the EU

Occasionally there may be circumstances where we are required to transfer your personal information to countries outside the European Economic Area (EEA). To ensure that your personal information does receive an adequate level of protection we have put in place model clauses to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the EU and UK laws on data protection. If you require further information about this protective measure you can request it from our Data Protection Officer.

## DATA SECURITY

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so. For more information about how we protect your information, please visit our security page <https://www.wesleyan.co.uk/security/>

## DATA RETENTION

### How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. We typically keep claims records for up to 12 years from the end of our relationship with you. In some circumstances we may be required to retain for longer periods such as, if there is legal action, a dispute or a requirement of a particular product, such as, a pension product or long term insurance product.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

## YOUR RIGHTS AND DUTIES

### Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your relationship with us. You can do this by using our contact us facilities which can be found at <https://www.wesleyan.co.uk/customer-services/>.

If you wish to update your marketing preferences at any time, you can do so by contacting us at [marketingpreferences@wesleyan.co.uk](mailto:marketingpreferences@wesleyan.co.uk) or via general enquiries on 0800 975 2087.

### Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- ▶ **Request access** to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- ▶ **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- ▶ **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- ▶ **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- ▶ **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- ▶ **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact our data protection officer using the details below.

## No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

## What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

## RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact our Data Protection Officer. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

## DATA PROTECTION OFFICER

We have appointed a data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact our DPO. While we hope you can discuss issues with the DPO, you also have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

## CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

**If you have any questions about this privacy notice, please contact Data Protection Officer on 0121 200 3003 or by email to [Privacy@wesleyan.co.uk](mailto:Privacy@wesleyan.co.uk)**