Catalina UK Privacy Policy

Catalina UK is committed to protecting the privacy of your personal information. This Privacy Policy lets you know how Catalina UK uses your personal data. In this Policy you will find information about the types of personal data we collect from you, when we collect your personal data and how long we keep it for, how your personal data is collected, the reasons for collecting and using your personal data, and information about how your personal data is shared.

The use of "we", "us", or "our" in this Privacy Policy, means Catalina UK or its subsidiaries (Catalina Worthing Insurance Limited (CWIL) and Catalina Services UK Limited (CSUK), collectively “Catalina UK”). CWIL acts as 'data controller', i.e. is responsible for decisions about how your data will be processed, for the purposes of data protection legislation, while CSUK acts as ‘processor’ on behalf of CWIL.

Please take a moment to review this Privacy Policy in detail to understand the views and practices regarding your personal data and how is treated.

Any changes to this Privacy Policy will be communicated on our website (catalinaworthing.co.uk/GDPR.html) and, unless stated otherwise, will take effect immediately once posted.

You can contact us using the following contact information:

Data Protection Compliance
Catalina UK,
99 Bishopsgate,
London,
EC2M 3XD,
United Kingdom
Email: dataprotection@catalinare.com

If you are an employee or prospective employee of Catalina UK, the processing of your personal data and your privacy rights are covered by our Employee Privacy Policy and Candidate Privacy Policy.

WHAT PERSONAL DATA DO YOU COLLECT FROM ME?

We may collect and process the following categories of personal data, depending on the nature of our relationship with you:

- Personal details such as your name, address, contact information, and information relevant to an insurance or reinsurance claim. This may include, depending on the circumstances, medical reports or information related to criminal convictions or incidents. Such data may be provided by you, your employer, an insured organisation, or another third party as part of policy administration.
- Information concerning business or commercial assets, where relevant to the servicing, provision, or administration of an insurance or reinsurance policy or related benefits.
- Details connected to requests for assistance or support—this can include your name, contact details, address, information relating to any vulnerabilities (which may involve some medical data), and financial information necessary to support the claim or service.
- Information you voluntarily provide when engaging with us directly, which may include details captured during recorded telephone calls or other communications.
- Data provided when submitting a complaint, including your name, contact details, and information relevant to the complaint. If the complaint is related to a claim, we may also process claim-specific information.
- Records of any communication you initiate with us, including written correspondence and the content of phone conversations.
- For business partners (such as consultants or service providers to Catalina UK), we may collect business contact information and other relevant commercial details.

The personal data we collect can include the following specific categories of information:

- Anti-fraud data
- Banking and payment details
- Financial background (e.g. bankruptcies, court judgments, HMRC matters)
- Policy and claim reference numbers
- Credit scores and credit history
- Date and place of birth
- Gender
- Employment details (e.g. job title, management level, department, work location)
- Family-related data, such as next-of-kin details

- Government-issued identifiers (e.g. National Insurance number, Social Security number, passport, tax ID, or driver's licence)
- Marital status
- Contact details (name, phone number, email address, postal address)
- Risk-related data

We may also process the following special category personal data, where relevant:

- Information related to criminal activity or fraud, provided either by you or by third parties such as anti-fraud agencies or other insurers
- Health-related data provided in connection with claim management
- Racial or ethnic background information
- Information from public sanctions or fraud prevention lists

Whenever we process special category personal data, we do so in line with the appropriate safeguards and in accordance with applicable data protection laws.

WHERE DO YOU COLLECT MY PERSONAL DATA FROM?

We collect your personal data from the following sources:

- Information you provide directly to us during the progression of a claim.
- Third parties authorised to assist us in managing and processing claims.
- When we take on the administration of policies or claims linked to an acquired portfolio of insurance business.
- Publicly available sources, particularly for the purposes of detecting and preventing fraud or financial crime.
- Credit reference agencies and background screening providers.

  Other insurance companies, particularly when we act in a reinsurance capacity.
- If you are a business partner, we may collect personal data when you or your organisation supplies it as part of our professional relationship.

In situations where the provision of personal data is required by law or under the terms of a contract we have or are planning on entering in with you, failure to provide that information may mean we're unable to fulfil our obligations. This could result in us being unable to offer or continue providing a service and may mean we cancel the service between us. Where applicable, we'll inform you at the relevant time.

WHY DO YOU PROCESS MY PERSONAL DATA?

We use your personal data to carry out the following Processing Activities:

- Administering insurance policies
- Assessing and handling claims
- Fulfilling legal and regulatory requirements
- Establishing, defending, or pursuing legal claims
- Detecting, investigating, or preventing fraud
- Managing and responding to complaints or other feedback
- Communicating with you
- Making and managing payments

WHAT LAWFUL BASIS DO YOU HAVE FOR PROCESSING MY PERSONAL DATA?

Our lawful basis for processing your personal data depends on the specific purpose for which it is used. These bases include:

- Performance of a contract – we need to process your personal data in order to fulfil our contract with you, such as administering your insurance policy.
- Legal obligation – we are required to process your personal data to meet legal or regulatory duties, for example, conducting background checks or reporting financial crime.
- Legitimate interests – as an insurance provider, we have a legitimate interest in using your data to protect against fraud and ensure the efficient operation of our business.

It may be necessary for us to process special category personal data (such as health or criminal conviction data) to manage the policy, provide benefits, comply with our legal responsibilities, or to obtain legal advice or defend legal claims. When we do so, we rely on one or more of the following legal bases:

- Insurance purpose - it is necessary for us to use your special category personal data for an insurance purpose, such as administering a policy benefit or for processing a claim.
- Legal claims - it is necessary for us to use your special category personal data to establish, exercise or defend legal claims.

- Fraud prevention - it is necessary for us to use your special category personal data to prevent fraud or a particular kind of fraud.
- Preventing or detecting unlawful acts - it is necessary for us to use your special category personal data to prevent or detect an unlawful act.

In some instances, we may use your personal data, including special category personal data, on the basis of your express consent. Where we rely on your consent as a legal basis for processing, we shall expressly inform you that we are doing so at the time that we request your consent. You do not have to give your consent, and you may withdraw your consent at any time. However, if you do not give your consent, or you withdraw your consent, this may affect our ability to provide you with the service. If you choose to withdraw your consent, we shall inform you of the consequences of withdrawal.

DO YOU SHARE MY PERSONAL DATA WITH THIRD PARTIES?

To help us carry out our Processing Activities, we may need to share your personal data with entities within and outside of Catalina UK as follows:

- Adjusters and other claims experts
- Anti-fraud agencies
- Courts
- Credit reference agencies
- Background checking agencies (e.g. DBS in England and Wales, or Disclosure Scotland)
- Law enforcement authorities (domestic or foreign)
- Legal counsel
- Outside legal counsel
- Ombudsmen, including Financial Services and Pensions Ombudsman Office (FSPO) and Financial Ombudsmen Service (FOS)
- Insurers (where we act as reinsurer)
- Reinsurers
- Regulators, including the Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA), or the Information Commissioners' Office (ICO)
- Service providers who supply back-office support
- Third-Party Administrators (TPA)
- Relatives, guardians or next of kin (where someone does not have capacity)
- Amongst other members of the Catalina Group of Companies

- Any entities to which we sell all or part of our business, or with which we merge

Transfers of personal data to entities within the UK and EEA are carried out with contractual safeguards in place, which incorporate the requirements of the UK GDPR and relevant guidance issued by the UK Information Commissioner's Office (ICO). We ensure that such transfers are made only where appropriate data protection measures are in place. EU and UK GDPR benefit from mutual adequacy decisions which recognise each regime offers an equivalent standard of protection for data subjects.

DO YOU TRANSFER MY PERSONAL DATA OUTSIDE THE UK / EEA?

We may transfer your personal data to other companies within our group and our suppliers in the United States and Bermuda. We do this for management purposes, reporting activities on company performance for regulatory or statutory purposes, in the context of a business reorganisation or group restructuring exercise, and for system maintenance support and hosting of data.

Whenever it is necessary to transfer your personal data to other companies of the group, agents or contractors located outside of the UK/ EEA, we shall take appropriate steps to ensure that such transfer adequately protects your rights and interests.

We shall only transfer your personal data to countries recognised as providing an adequate level of legal protection, or where we are satisfied that protections are in place to properly protect your privacy rights.

Transfers between Catalina Group companies are covered by our Intra-Group Sharing Agreement, which provides specific requirements designed to ensure your personal data receives necessary protection whenever it is transferred between Catalina Group companies. We rely on the EU-US Data Privacy Framework (DPF), and UK Extension to the DPF, as an adequate safeguard when transferring data between the UK and USA. We also rely on contractual agreements approved by the European Commission or by the UK Information Commissioner's Office (ICO) when transferring data between the UK and Bermuda.

Transfers to other service providers and business partners are also protected by contractual agreements approved by the European Commission or by the UK Information

Commissioner's Office (ICO). Before transferring your data to our service providers, we ensure they can provide adequate level of data protection.

If you would like to see a copy of these appropriate safeguards (for example, a copy of the EU Commission or ICO approved model clauses) please get in touch with us by emailing dataprotection@catalinare.com.

HOW LONG WILL YOU KEEP MY PERSONAL DATA?

We keep your personal data for no longer than is necessary for the purpose for which the information is collected and to manage our relationship with you, including for the purpose of satisfying any legal, accounting, or reporting requirements.

When deciding how long to retain personal data, we consider the amount, type, and sensitivity of the data, the potential risk of harm from any unauthorised use or disclosure, the reasons we are processing the data and whether those purposes could be achieved in other ways, as well as any relevant legal obligations.

In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) or receive anonymised personal data for research or statistical purposes, in which case we may use this information indefinitely without giving further notice to you.

DO YOU SECURELY STORE MY PERSONAL DATA?

We apply strict security standards, controls, and processes to protect your personal data from unauthorised access, loss, or accidental deletion. These include restricting who can have access to your personal data and protecting your data with security tools appropriate to the type of information e.g., encryption software.

We also require that our third-party processors who handle your personal data do the same.

WHAT ARE MY DATA PROTECTION RIGHTS?

Under the UK GDPR you have several rights, which allow you to maintain control over your personal data. These include the right to:

- **Access your personal data:** You can request a copy of the personal data we hold about you to check that we are processing it lawfully (commonly known as a "data subject access request").
- **Correct your personal data:** If you believe that any personal data we hold about you is incomplete or inaccurate, you can ask us to correct it. In some cases, we may need to verify the accuracy of the information you provide before making changes which may include asking for evidence from you.
- **Request deletion of your data:** You can ask us to delete or remove your personal data where there is no valid reason for us to continue processing it. This also applies if you have successfully objected to our processing, if your data was processed unlawfully, or if we are legally required to erase it. However, we may not always be able to comply due to specific legal obligations, which we will explain if applicable.
- **Restrict how we use your data:** You can ask us to limit the processing of your personal data in certain circumstances, such as:
  - if you contest the accuracy of the data;
  - if our use of the data is unlawful and you prefer restriction over erasure;
  - if you need us to keep the data for legal claims, even if we no longer need it; or
  - if you've objected to our processing and we are considering whether our legitimate grounds override yours.
- **Object to the processing of your data:** If we are relying on legitimate interests (ours or a third party's) as a basis for processing, you can object if you feel this impacts your fundamental rights and freedoms. In some cases, we may demonstrate that we have compelling grounds to continue processing your data despite your objection.
- **Request data portability:** You can ask us to transfer your personal data to you or a third party. We will provide it in a structured, commonly used, machine-readable format. This applies only to data processed by automated means where we relied on your consent or carried out the processing under a contract with you.
- **Withdraw your consent:** Where we rely on your consent to process your personal data, you can withdraw it at any time. This will not affect the lawfulness of any processing carried out before you withdrew consent. If withdrawing consent affects the products or services we can provide, we will inform you at the time.

Additional Information About Your Rights

- ***Timeframe for response:*** We aim to respond to all legitimate requests within one month. If your request is particularly complex or you have made several requests, it may take longer. Under the UK GDPR we can extend the response timeframe by two additional months. In that case, we will let you know and keep you informed of progress.
- ***No fee:*** You will not be charged to exercise your personal data rights. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive. In rare cases, we may refuse to comply under these circumstances.
- ***Verification of identity:*** To protect your data, we may need to ask for specific information to confirm your identity and ensure your right to access the data (or exercise any other rights). We may also contact you for additional information to help us process your request more efficiently.

You can contact us about exercising any of your rights by using the following information:

Data Protection Compliance
Catalina UK,
99 Bishopsgate,
London,
EC2M 3XD,
United Kingdom
Email: dataprotection@catalinare.com

DO YOU CARRY OUT AUTOMATED DECISION MAKING?

We do not make any decision about you which has a legal or similarly significant effect on you based solely on automated processing (i.e. without human intervention).

DO YOU USE COOKIES ON YOUR WEBSITE?

We do not use cookies on our website.

WHAT SHOULD I DO IF I AM NOT HAPPY WITH HOW MY PERSONAL DATA IS BEING USED?

If you have any concerns about our use of your personal data, you can make a complaint to us at dataprotection@catalinare.com.

You also have the right to complain to our relevant Supervisory Authority, which is the Information Commissioner's Officer (ICO) in the UK. They are responsible for ensuring we correctly follow all relevant data protection law.

You can contact the ICO at:

Information Commissioner's Office
Wycliffe House,
Water Lane Wilmslow,
Cheshire,
SK9 5AF
Tel: 0303 123 1113

You can also contact the ICO using the following link: https://ico.org.uk/make-a-complaint/data-protection-complaints.

If you are based in the European Economic Area (EEA) you can contact your national Supervisory Authority. Details of EEA Supervisory Authority members can be found here: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en.