UK Privacy Notice (re)insurance

AUK are committed to complying with data protection laws.

This Privacy Notice describes how AUK collect, use, share and secure your personal data when we provide our services as an (re)insurance business.

This Privacy Notice sets out –

- why AUK may collect personal data about you?
- what types of data may AUK collect?
- how does AUK collect your personal data?
- what is the legal basis for collecting and processing your personal data?
- for how long will my personal data be retained?
- who does AUK share your personal data with?
- how does AUK protect your personal data?
- what automated decision making may be conducted?
- what rights do you have over your personal data?
- how do I ask a question or make a complaint?
- how are international transfers dealt with?
- how do I make a data subject access request? and
- how and when will this Privacy Notice be updated?

For the purposes of the data protection legislation, the company responsible for your personal data (i.e. the Data Controller) is the Aspen Group company stated in your contract of (re)insurance and for Lloyd's syndicate 4711, Aspen Managing Agency Limited.

You may also find it useful to review the London Insurance Market Core Uses Information Notice, which explains how the various insurance market participants, including intermediaries and (re)insurers, use personal information. Our core uses and disclosures of personal information are consistent with the London Market Core Uses Information Notice. The Notice can be found here – https://www.sompo-intl.com/wp-content/uploads/Lloyds-Core-Uses-Notice-Document-28-05-24.pdf

Why AUK may collect personal data about you?

AUK collect and process your personal data in compliance with all relevant data protection laws including the UK General Data Protection Regulation (UKGDPR), the Data Protection Act 2018 (DPA) as well as other applicable legislation. Personal data, or personal information, is any information about you from which you can be identified. For example, this may include your name, your date of birth, your contact details and your email address.

AUK may collect personal data for the following reasons –

- to evaluate the risks to be covered, to ensure the policy of (re)insurance is appropriate and the premium is reflective of the risk presented;
- to provide you with a quote for an (re)insurance policy;
- to provide you with an (re)insurance policy;
- to deal with claims and other issues and complaints that arise from that (re)insurance policy;
- general client management, including communicating with you regarding administration and requested changes to your policy;
- to conduct required fraud, credit and anti-money laundering and sanctions checks;
- to fulfil legal or regulatory requirements; and
- to keep you informed of developments through marketing.

AUK may provide you with further notices highlighting certain uses of your personal information as appropriate.

What types of data may AUK collect?

The information AUK may collect depends on our relationship with you but it may include –

- personal details including name, age, gender, date of birth, photographs and marital status;
- contact information including address, telephone numbers and email address;
- financial Information including bank details, annual income and credit check details;
- information relevant to your (re)insurance policy including account name and insurance policy number;
- information relevant to your claim including claim reference number, account name and bank details;

- information obtained during telephone conversations (including recordings and transcripts of those conversations);
- marketing preferences:
- information obtained through our use of cookies;
- details of your customer experience with us; and
- information for the prevention of financial crime including verification documents such as passports and driving licences.

Some of the information collected by AUK may include special categories of personal information (sometimes referred to as 'sensitive personal information'). These may include –

- physical, or mental health conditions;
- identification information including passport details, driver's license details and national insurance number; and
- information relating to criminal offences, including alleged offences, criminal proceedings, outcomes and sentences (previous criminal convictions).

Please note that AUK do not knowingly collect personal data about children.

If you believe AUK have collected personal data about your child, you may contact Aspen's Group Data Protection Officer (dpo@aspen.co) and request that we cease processing data about your child.

How does AUK collect your personal data?

We may collect your personal data in the following ways –

- directly from you as the data subject;
- from your family members;
- from your insurer or intermediary;
- from your employer;
- from credit reference agencies, anti-fraud databases, court judgments and other publicly available databases;
- from public sources such as Companies House;
- from a range of third parties, which include –
    - other companies within the Aspen Group;
    - other companies with whom we have a business relationship;

    - insurance brokers and intermediaries;
- via Cookies;
- via our telephone calls with you, which may be recorded and this may include logging your telephone number, date, time and duration of the call;
- when you provide a service to us or our customers (as a supplier);
- from social media;
- in the event of a claim, claims handlers, witnesses, loss adjusters, medical professionals and hospitals, and counsel who are involved in adjusting and the processing of claims;
- government agencies, industry bodies, the Financial Ombudsman Service and regulators including the Financial Conduct Authority; and
- other third-party sources where necessary which may include –
    - companies who assist in investigating fraud, including obtaining information data from credit reference agencies;
    - companies who provide consumer classification and other personal data for marketing purposes;
    - companies who provide information which may be used by AUK to inform its risk selection, pricing and underwriting decisions; and
    - where we are complying with our legal obligations regarding money laundering and other anti-financial crime measures.

What is the legal basis for collecting and processing your personal data?

AUK processes your personal information in compliance with all relevant data protection laws including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA), the applicable provisions affecting or ensuring data privacy within the Insurance Act 2015, as well as all other applicable laws. The UK GDPR requires us to have a legal basis for processing your personal information. In most cases the legal basis will be one of the following –

- to fulfil our contractual obligations to you, for example to provide you with insurance cover, including the handling of claims;
- to comply with our legal obligations such as client due diligence and reporting obligations, and responding to requests from regulators, law enforcement authorities or other government authorities; and

- to meet our legitimate interests, for example, to ensure we price our products appropriately, to manage risk, to perform audits, and to maintain accurate records.

When we process personal data to meet our legitimate interests, we always balance these against your fundamental rights and freedoms and put in place robust safeguards to ensure that your privacy is protected

Generally, we do not rely on consent as a legal basis for processing your personal data in circumstances where –

- the law specifies that we have to process your personal data;
- we need to process your data to perform a contract with you;
- we have a public interest to do so; or
- we have a legitimate business reason for doing so.

Where we do rely on your consent, you have the right to withdraw it at any time in the manner indicated when your consent was provided. In addition, you can do so by contacting our Group Data Protection Officer (dpo@aspen.co).

Activity	**Legal Basis**
Quotation and inception purposes	Legitimate Interest Performance of a Contract
Conducting all required financial crime checks, including fraud, credit and anti-money laundering and sanctions checks for inception purposes;	Legal Obligation Legitimate Interest
Evaluating the risks to be covered and matching them to appropriate policies and premiums;	Legitimate Interest
Policy administration (including policy termination and renewal);	Legitimate Interest Performance of a Contract
Collection and refund of premiums;	Legitimate Interest

	Performance of a Contract
General client care management, including communicating with you regarding administration and requested changes to your policy;	Legitimate Interest Performance of a Contract
Sending you your policy documentation;	Legitimate Interest Performance of a Contract
Notification of claims;	Legitimate Interest Performance of a Contract
Managing insurance claims including evaluation of the claim and determination of compensation;	Legitimate Interest Performance of a Contract
Processing of Insurance claims – defending and prosecuting of legal claims	Legal Obligation Legitimate Interest
Processing of claims – conducting fraud checks, credit, anti-money laundering and sanctions checks	Legal Obligation
Investigating and prosecuting fraud	Legal Obligation Legitimate Interest
To carry out general risk modelling and underwriting (including calculations and determinations of policy premiums	Legitimate Interest
Complying with our legal or regulatory obligations;	Legal Obligation

Transferring books of business, company sales and reorganisations	Legitimate Interest Legal Obligation

We will only use your personal data 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 data for an unrelated purpose, we will notify you and we will explain the legal basis that allows us to do so.

If you have any queries in relation to the legal basis of processing for specific purposes, please contact our Group Data Protection Officer (dpo@aspen.co).

For how long will my personal data be retained?

The length of time for which your personal data will be retained will depend on several factors, including but not limited to –

- legislative requirements;
- Aspen's reporting requirements; and
- operational requirements (e.g. claim or pension payment processing).

Aspen seeks to minimize the time it retains data in line with the requirements of Data Protection laws, including GDPR, and any local laws applicable in your jurisdiction, and maintains a comprehensive Group Records Retention Policy to achieve this aim. This policy and associated data retention schedules pertaining to each type of information can be obtained on request from our Group Data Privacy Officer (dpo@aspen.co).

Who does AUK share your personal data with?

AUK does not sell any data to third parties for commercial purposes.

While providing services to you, AUK may disclose your data to third-parties which may include –

- other companies in the Aspen Group
- claims handlers and loss adjusters;
- intermediaries (such as brokers and coverholders);
- reinsurers;
- legal counsel, including those who are involved in adjusting and the processing of claims;
- witnesses;

- other insurers;
- banking partners;
- credit agencies;
- IT companies
- regulators;
- healthcare providers;
- fraud detection agencies and the Insurance Fraud Bureau; and
- law enforcement agencies.

Aspen requires that personal data is processed in accordance with our instructions and in circumstances which require the recipient to observe industry standard security measures in respect of personal data.

We do not allow our third parties to use your personal data for their own purpose.

How does AUK protect your personal data?

As required by applicable data protection laws, Aspen has implemented physical, electronic and technical security measures and policies and procedures to safeguard and secure the data we collect.

All AUK staff have a legal duty to respect the confidentiality of information and access to confidential information is restricted to only those who have a reasonable need to access it. Technical controls implemented may include database encryption, email encryption, identity and access management solutions, comprehensive network protection and antivirus solutions.

AUK ensures appropriate contracts and data sharing agreements are executed when sharing data with third parties, ensuring that at least an equivalent level of security is offered by our partners and suppliers. These contracts incorporate EU/UK standard contractual clauses where personal data is transferred without an 'adequacy decision' to third countries outside of the UK/EU/EEA.

What automated decision making may be conducted?

We do not make any decisions about you using automated means (without human review), and we will update our Privacy Notice if this position changes.

What rights do you have over your personal data?

You generally have the following rights under GDPR and UK GDPR, which you can usually exercise (you may have other rights subject to the jurisdiction that you are in and should look at the jurisdiction specific sections below):

Access to a copy of your personal data	The right to be provided with a copy of your personal data.
Correction (also known as rectification)	The right to require us to correct any mistakes in your personal data.
Erasure (also known as the right to be forgotten)	The right to require us to delete your personal data in certain situations (as we may have legal obligations to retain certain data).
Restriction of use	The right to require us to restrict use of your personal data in certain circumstances, e.g. if you contest the accuracy of the data.
Data portability	The right to receive the personal data you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party—in certain situations.
To object to use	The right to object – · At any time to your personal data being used for direct marketing (including profiling); · In certain other situations to our continued use of your personal data, e.g. where we use your personal data for our legitimate interests.
Not to be subject to automated decision making without human involvement	The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects. We do not make any such decisions.

If you would like to exercise any of these rights, please contact our Data Protection Officer at; 30 Fenchurch Street, London EC3M 3BD or via email (dpo@aspen.co)

What rights do you have over your personal data?

You generally have the following rights under GDPR and UK GDPR, which you can usually exercise (you may have other rights subject to the jurisdiction that you are in and should look at the jurisdiction specific sections below):

Access to a copy of your personal data	The right to be provided with a copy of your personal data.

Correction (also known as rectification)	The right to require us to correct any mistakes in your personal data.
Erasure (also known as the right to be forgotten)	The right to require us to delete your personal data in certain situations (as we may have legal obligations to retain certain data).
Restriction of use	The right to require us to restrict use of your personal data in certain circumstances, e.g. if you contest the accuracy of the data.
Data portability	The right to receive the personal data you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party—in certain situations.
To object to use	The right to object – · At any time to your personal data being used for direct marketing (including profiling); · In certain other situations to our continued use of your personal data, e.g. where we use your personal data for our legitimate interests.
Not to be subject to automated decision making without human involvement	The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects. We do not make any such decisions.

If you would like to exercise any of these rights, please contact our Data Protection Officer at; 30 Fenchurch Street, London EC3M 3BD or via email (dpo@aspen.co)

How do I ask a question or make a complaint?

For the purposes of the data protection legislation, the company responsible for your personal data (i.e. the data controller) is the Aspen Group company stated in your contract of (re)insurance or employment contract.

If you have any complaints, queries or wish to exercise your data protection rights, please contact Aspen's Group Data Protection Officer at;

30 Fenchurch Street, London EC3M 3BD or via email (dpo@aspen.co).

Where you are dissatisfied with any aspect of our handling of your personal data, you have a right to lodge a complaint with the relevant authority responsible for data protection in your jurisdiction. In the UK this is the Information Commissions Office (ICO). The ICO's contact details are set out below

Information Commissions Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, Telephone: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.

How are international transfers dealt with?

UK Residents – Transferring your data outside of the UK

The personal data that we collect about you may be transferred to, or stored at, one or more of Aspen's locations outside of the UK. Your personal data may be processed in Aspen's other offices (including the US, Bermuda, Singapore, Switzerland, Canada and Australia) and India.

Following the UK's departure from the EU, the EU authorities have made an adequacy decision in respect of the UK. This means that the UK is deemed to provide an essentially equivalent level of protection for personal data to that which exists within the EU. In turn, the UK Government has made an adequacy decision in respect of the EU. On that basis, data can flow freely between the two areas. Irrespective of this, AUK will continue to ensure that any recipient of data provides at least the same level of protection as we would ourselves.

Transfers of your personal data to jurisdictions outside of the UK will be made subject to similar safeguards and considerations to those that apply to the personal data for EU/EEA residents (see section above). However, where your personal data is transferred to a country or recipient in a country that does not offer 'adequacy', appropriate safeguards will be in place, including the use of Standard Contractual Clauses.

Additionally, where the recipient is in the USA and is certified to the EU-US Privacy Framework and UK-US Data Bridge, Aspen may also rely on this safeguard.

EU / EEA Residents – Transferring Your Data Outside of the EU

The personal data that AUK may collect about you could be transferred to, and stored in, one or more countries outside of the EEA or outside the jurisdiction in which you reside. It may also be processed by staff operating outside of the EEA (or outside the jurisdiction in which you reside) who work for Aspen or for our Third-Party Suppliers.

In such cases, AUK will take appropriate steps to ensure an adequate level of data protection is in place. This could be an "adequacy" decision, in the country of the

recipient or appropriate safeguards, such as the EU Standard Contractual Clauses required under GDPR.

If AUK cannot ensure such an adequate level of data protection, your personal data will only be transferred outside the EEA (or outside the jurisdiction in which you reside) if you have given your prior consent to such transfer, or if there are other specific exemptions that allow us to transfer the data outside the EU for example, for the establishment, exercise or defence of legal claims and any local law requirements for the transfer have been satisfied.

Your personal data may be processed in Aspen's other offices (including the US, Bermuda, Singapore, Switzerland, Canada and Australia) and India.

EU Representative Contact Details

If you are in the EU, then please make any requests via our EU Representative (The DPO Centre) (eurep@aspen.co)

How do I make a data subject access request?

If you wish to invoke any of your rights under relevant privacy regulations or to make a general enquiry regarding Aspen's approach to securing your data, please do so by contacting Aspen's Group Data Protection Officer (dpo@aspen.co).

Please note that only you or someone that you authorise to act on your behalf may submit these requests. Your request must provide sufficient information for us to reasonably verify that you are the person about whom we collected personal information and sufficient detail to allow us to properly understand, evaluate and respond to your request.

In response to such a request, we may also ask you to verify your identity or to provide additional information that helps us to understand your request better. Once we have the necessary information from you regarding proof of identity, or in the case of an agent, proof of authorisation, and your request is valid, we will respond to you as soon as possible but no later than within 30 days unless the number and complexity of the requests made are deemed to be excessively high. In this case, we may extend this time by up to two months. We will inform you if we need to make use of this additional time and why we need to do so as soon as is practicably possible.

EU / EEA Data Subject Requests

If you wish to invoke any of your rights under relevant privacy regulations or to make a general enquiry regarding Aspen's approach to securing your personal data, please do so by contacting our EU / EEA (The DPO Centre) (eurep@aspen.co).

Please note that only you or someone that you authorise to act on your behalf may submit these requests. Your request must provide sufficient information for us to

reasonably verify that you are the person about whom we collected personal information and sufficient detail to allow us to properly understand, evaluate and respond to your request.

In response to such a request, we may also ask you to verify your identity or to provide additional information that helps us to understand your request better. Once we have the necessary information from you regarding proof of identity, or in the case of an agent, proof of authorisation, and your request is valid, we will respond to you as soon as possible but no later than within 30 days unless the number and complexity of the requests made are deemed to be excessively high. In this case, we may extend this time by up to two months. We will inform you if we need to make use of this additional time and why we need to do so as soon as is practicably possible.

How and when will this Privacy Notice be updated?

Due to the nature of our business, AMAL and AIUK is unable to contact all its policyholders, beneficiaries or claimants as we do not always know who they are, particularly in the case of reinsurance policies. This means that we cannot ensure that all data subjects will be aware when our Privacy Notice changes. However, we will always ensure that it is updated to reflect any changes in legislation, our own policies or best market practices.

Any changes we may make to this Notice in the future will be posted on our website and you are advised to regularly check and review the Notice to ensure you understand how we may be processing your personal data. Any changes we may make to this Notice (which will, unless otherwise indicated, apply to any personal data already obtained before the changes were made) will be effective from the date on which those changes have been posted on this page.

This Notice was last updated on 14th March 2025.