

Company Name/Data Controller: The Baldwin Group Specialty UK, Ltd trading as CAC Specialty UK (and referred to as the Company in this privacy notice)

Company Address: 4211 W. Boy Scout Blvd Suite 800 Tampa, FL 33607

Data Protection Officer / GDPR Compliance Manager Contact

Details: DataPrivacyOfficer@baldwin.com

In this Privacy Notice, we identify the personal data that we collect about you and how we use that data. It applies to any personal data you provide to the Company and any personal data we collect from other sources. If you provide personal data to us about other people, you must provide them with a copy of this Privacy Notice and obtain any necessary consent from them for the processing of their personal data. This notice is applicable to those residing in the UK.

We do not process biometric data or use automated decision-making technology. You do not have to provide us with personal data, but, if you do not, we may not be able to interact with you for the relevant purpose.

The Company is committed to being transparent about how it collects and uses data and to meeting its data protection obligations. This Privacy Notice summarises your rights and our responsibilities to you. It should be read in conjunction with our website privacy notice which can be accessed at <https://baldwin.com/privacy-policy/>.

Nothing in this Privacy Notice forms part of any contract and may be amended at any time. Please check back regularly for any changes.

1. Who do we collect data about?

The Company collects and processes a range of information about you where you fall into one of the following categories:

- Business contacts, such as insurers, brokers/intermediaries, (re)insurers, managing general agents, claims and loss adjusters, service providers/suppliers/vendors, professional advisors, experts, office visitors, governmental bodies, authorities and regulators.
- Insureds and those involved with our insurance business activities (e.g., parties covered under a policy, beneficiaries of a policy or other third party interests, other parties involved in claims in respect of the policies).
- Other individuals, such as those making general inquiries to us or whose images we capture on CCTV/surveillance cameras.

2. What data do we collect?

- Contact information, such as your email, telephone number, and physical address.
- Beneficiary and third-party information.
- Financial information such as your bank account, tax details and any assets relevant to an insurance policy.
- Policy information, such as your policy number, policy period and applicable dates, premia, policy terms and benefits, underwriting information, claims record and related data claims history, credit scoring.
- Details about your visits to our office (including CCTV, audio and still images).
- Criminal record information such as charges or convictions.
- Background checks (including anti-money laundering and know your client verification documents) and sanctions screenings.
- Commercial information such as prior business dealings and personal preferences for entertainment and marketing purposes.

- Regulatory information and status.
- Special category personal data, such as data relating to your health, genetic or biometric data, sex life, sexual orientation, gender identity, racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership.
- Marketing and promotional information such as marketing preferences and interactions with our marketing campaigns including any response to emails we send.

3. Where do we collect data from?

This depends on how you interact with us. In most cases, it will be collected from the following sources:

- Direct from you where you interact with , for example as a service provider to us.
- From our clients or others involved in the course of our professional activities. This may include insurers, brokers/intermediaries, (re)insurers, managing general agents, claims and loss adjusters, service providers/suppliers/vendors, professional advisors, experts, office visitors, governmental bodies, authorities and regulators.
- Background checking providers and agencies. This may include the DBS, from fraud databases, credit agencies and commercial screening providers.
- Publicly available information. This may include social media, court records, and public registers (e.g., Land Registry).
- Governmental authorities. This may include law enforcement and regulators.
- Group companies being any direct or indirect subsidiary of The Baldwin Insurance Group, Inc.

4. How do we use your data?

- To provide our professional services to our clients. This may include the brokering of (re)insurance, placement of policies, ongoing management of policies and claims management.
- To comply with our legal obligations. This may include to comply with anti-money laundering and counter-terrorist financing laws, sanctions obligations and to comply with law enforcement requests, court orders and regulatory requirements.
- To establish, exercise or defend legal rights and obligations. For example, in connection with a legal dispute about a policy.
- To prevent and detect crime.
- To monitor the safety and security of our office premises and IT systems.
- To manage our business. This may include establishing and managing business relationships, within our IT and network infrastructure, to model and analyse risks and for business and regulatory reporting, to market and communicate with clients and prospects, to take professional advice (e.g., legal, audit, financial, insurance).
- Corporate transactions. If we seek to sell or dispose of our business or any part of it.

5. Who do we share data with?

- Professional advisers, such as underwriters, other insurance intermediaries, lawyers, accountants, tax advisers, financial advisers, auditors, actuaries, claims handlers, investigators, loss adjusters/assessors, experts and consultants.
- IT service providers and those involved in managing our IT infrastructure.
- Fraud and credit reference agencies.
- Parties to a proposed corporate transaction.
- Governmental and law enforcement bodies.
- Our insurers and risk advisers.
- Group companies.
- Other third parties where required or permitted by law or with your agreement.

6. Legal basis for processing.

- Legitimate interest. This may include performing our professional duties for clients and managing our business and its operations.

- For the performance of a contract with you or for preparatory steps taken at your request prior to entering into a contract.
- Compliance with legal obligations. For example, to comply with anti-money laundering and counter-terrorist financing laws and sanctions obligations, to comply with law enforcement requests, court orders, and regulatory requirements and to establish, exercise or defend legal claims.
- Consent, where that is obtained. In most cases, we rely on other reasons.

7. Transfer

As is common within a group of companies, personal data is shared between group entities for, amongst others, operational purposes and group-wide functions. It may also be shared with other parties outside the UK/EEA for the purposes stated. If that occurs, it is subject to an Information Commissioner-approved International Data Transfer Agreement that any third party is required to apply the same standards and protections, which affords you the same data rights as you have here. Personal data transferred is encrypted both on transmission and when stored by third parties.

8. How does the Company protect data?

The Company takes the security of personal data seriously. The Company has internal policies, procedures, technologies and controls in place, from the point of collection to the point of destruction, to protect personal data against loss, malicious or accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by individuals in the proper performance of their duties.

9. How long does the Company keep data for?

The Company shall not retain any personal data for any longer than is necessary considering the purpose(s) for which that data is collected, held, and processed. At the end of that period, or if you withdraw your consent earlier (if consent is the basis for processing), your data will be deleted or destroyed. For details of our records retention periods, please contact DataPrivacyOfficer@baldwin.com

10. What are your rights?

As a data subject, you have a number of rights. You can:

- Know what data we hold about you, why we hold it, the lawful basis for processing it basis and who we share it with.
- Access and obtain a copy of your data on request, and to request a transfer of data to another data controller.
- Require the Company to change incorrect or incomplete data.
- Require the Company to delete or stop processing your data, for example, where the data is no longer necessary for the purposes of processing.
- Object to the processing of your data where the Company is relying on its legitimate interests as the legal ground for processing.
- Not to be subject to automated decision making (with some exceptions).
- To be notified of a data security breach in some circumstances.
- To withdraw consent processing where this was the legal basis relied upon for any such processing.
- To complain to the Information Commissioner's Office <https://ico.org.uk/concerns/>.

Not all of these rights are absolute, and in some cases we may be entitled to charge a fee. If you wish to exercise any of these rights, please contact DataPrivacyOfficer@baldwin.com

Effective date: May 5, 2026