PRIVACY POLICY

Web Portal: jupiterinsurance.in

Amica Insurance Brokers Private Limited

Effective Date: 12 May 2026 | Last Updated: 12 May 2026

This Privacy Policy (the "Policy") describes how Amica Insurance Brokers Private Limited (also operating under the consumer brand "Jupiter Insurance" at jupiterinsurance.in) collects, uses, stores, shares, discloses, retains, transfers and otherwise processes the personal data of users of the web portal jupiterinsurance.in, related mobile applications, application programming interfaces and other digital interfaces (collectively, the "Portal").

This Policy is published in accordance with (i) Rule 3(1) and Rule 4 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, (ii) Rule 4 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "SPDI Rules") to the extent applicable, (iii) the Digital Personal Data Protection Act, 2023 (the "DPDP Act") read with the Digital Personal Data Protection Rules, 2025 (the "DPDP Rules"), (iv) the Insurance Regulatory and Development Authority of India (Insurance Brokers) Regulations, 2018 (the "Brokers Regulations") read with Schedule I, Form H thereto, (v) the IRDAI Information and Cyber Security Guidelines, 2023, (vi) the IRDAI (Maintenance of Insurance Records) Regulations, 2015, (vii) the Prevention of Money Laundering Act, 2002 and the Master Guidelines on Anti Money Laundering / Counter Financing of Terrorism (AML/CFT) issued by the IRDAI from time to time, and (viii) all other Applicable Law, in each case as amended or supplemented from time to time.

Please read this Policy carefully. By accessing, browsing, registering on, or otherwise using the Portal, or by clicking "I Accept", "I Agree", "Submit", "Get Quote", or any similar button on the Portal, you confirm that you have read, understood, and consented to the collection, processing, storage, transfer and disclosure of your personal data in accordance with this Policy and the Terms and Conditions of the Portal.

Identification of the Data Fiduciary

Legal Name	Amica Insurance Brokers Private Limited
Trade Name / Web Portal	Jupiter Insurance (jupiterinsurance.in)
Category of Registration	Direct Broker (Life and General)
IRDAI Registration No.	IRDAI/INT/BRK/DB1135/2024
Certificate of Registration No.	1065
Validity of Registration	15 May 2025 to 14 May 2028

Registered Office	Office 31, 3rd Floor, Viraj Building, Plot No. 124, S.V. Road, Khar (West), Mumbai 400 052, Maharashtra, India
Principal Officer	Alpesh Kharecha
Grievance Officer	Sandeep Raj
CIN	U66220MH2022PTC393575
GSTIN	27AAXCA9084E1Z1

1. Definitions

"Amica", "we", "our", "us", "Data Fiduciary" means Amica Insurance Brokers Private Limited, an Indian private limited company holding a valid Direct Broker (Life and General) Certificate of Registration No. 1065 (IRDAI/INT/BRK/DB1135/2024) issued by the IRDAI, operating the consumer facing portal under the brand "Jupiter Insurance" at jupiterinsurance.in.

"Applicable Law" means all statutes, ordinances, rules, regulations, master circulars, guidelines, notifications, judgments, orders and directives of India, including without limitation the Insurance Act, 1938, the IRDAI Act, 1999, the Brokers Regulations, the IRDAI (Protection of Policyholders' Interests, Operations and Allied Matters of Insurers) Regulations, 2024 and the related Master Circulars, the IRDAI (Insurance Products) Regulations, 2024, the IRDAI Information and Cyber Security Guidelines, 2023, the IRDAI Master Guidelines on AML/CFT, the IRDAI (Maintenance of Insurance Records) Regulations, 2015, the Information Technology Act, 2000 and the rules thereunder, the DPDP Act, the DPDP Rules, the Prevention of Money Laundering Act, 2002 and the Consumer Protection Act, 2019.

"Consent Manager" shall have the meaning ascribed to it under Section 6(7) of the DPDP Act, namely a person registered with the Data Protection Board of India who enables a Data Principal to give, manage, review and withdraw consent through an accessible, transparent and interoperable platform.

"Cookies" means cookies, web beacons, pixels, software development kits (SDKs), local storage objects, device identifiers and other similar tracking technologies used on the Portal.

"Data Principal", "you", "your", "User" means the natural person to whom the personal data being processed relates, and includes the parent or lawful guardian of a child, and the lawful guardian of a person with disability.

"Data Processor" means any person who processes personal data on behalf of Amica.

"DPDP Act" means the Digital Personal Data Protection Act, 2023.

"DPDP Rules" means the Digital Personal Data Protection Rules, 2025 as notified by the Central Government from time to time.

"DPB" means the Data Protection Board of India established under Section 18 of the DPDP Act.

"Insurer" means any insurance company registered with the IRDAI under Section 3 of the Insurance Act, 1938 with which Amica has entered into an arrangement for solicitation, procurement or servicing of insurance products.

"Personal Data" means any data about an individual who is identifiable by or in relation to such data, as defined under Section 2(t) of the DPDP Act.

"Personal Information" / "Sensitive Personal Data or Information (SPDI)" has the meaning ascribed under the SPDI Rules, and includes information such as passwords, financial information, health information, biometric information and medical records.

"Portal" means the website hosted at jupiterinsurance.in and any subdomains, mobile applications, application programming interfaces and other digital interfaces operated by, or on behalf of, Amica from time to time.

"Processing" means a wholly or partly automated operation or set of operations performed on Personal Data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

"Services" means insurance broking, solicitation, advisory, comparison, quote generation, policy placement, premium collection, post sale servicing, claims assistance and ancillary services rendered by Amica through the Portal in accordance with the Brokers Regulations.

2. Scope and Applicability of this Policy

1. This Policy applies to all visitors, browsers, prospects, proposers, policyholders, claimants, beneficiaries, nominees, registered users and any other natural person who accesses or uses the Portal or whose Personal Data is otherwise collected, received or processed by us in connection with the Services.
2. This Policy does not apply to (a) websites, applications or services operated by Insurers, third party administrators, payment aggregators, regulators or other third parties, even where such sites are linked from or embedded in the Portal, and (b) to any non personal, anonymised or aggregated data that does not, by itself or in combination with other information available to us, identify a natural person.
3. This Policy should be read together with our Terms and Conditions, and any product specific or scheme specific notices made available to you at the time of collection of Personal Data.

3. Categories of Personal Data We Collect

We collect and process the following categories of Personal Data about you, depending on the Services availed, the product purchased, the proposal submitted, the claim filed and the Applicable Law that governs the processing:

(a) Identification and contact information: full name, salutation, gender, date of birth, age, marital status, photograph, signature, occupation, postal address, residential and correspondence address, mobile number, alternate phone number, landline number, email address and WhatsApp number.

(b) Government issued identifiers and KYC information: Permanent Account Number (PAN), Aadhaar virtual identifier (VID) or Aadhaar offline XML or other Officially Valid Documents (OVDs) such as voter identity card, driving licence, passport or NREGA job card, Form 60 (where PAN is not available), Goods and Services Tax Identification Number (GSTIN), Central KYC Records Registry (CKYCR) identifier, FATCA / CRS self certification, place of birth, country of tax residence and beneficial ownership declarations.

(c) Financial information: bank account number, IFSC code, mobile wallet identifier, UPI identifier, credit card or debit card details (collected only by the payment aggregator in tokenised or masked form), income range, source of funds, and information necessary for refund and claim payouts to be made by the Insurer.

(d) Health and medical information: current health status, pre existing diseases, medical and surgical history, family medical history, prescriptions, diagnostic reports, hospitalisation records, smoking, alcohol consumption and lifestyle disclosures, height, weight and Body Mass Index, and the reports of any pre policy medical examination conducted at the request of an Insurer.

(e) Nominee, dependant and family information: name, relationship, age, contact details, share of nomination and identification details of nominees, dependants, family floater members and beneficiaries.

(f) Vehicle and asset information: registration number, chassis number, engine number, make, model, variant, year of manufacture, fuel type, registration certificate details, previous policy details, no claim bonus details, ownership and usage particulars; and in respect of home, marine, fire and commercial cover, descriptive and valuation information about the insured property.

(g) Employment and professional information: employer name, designation, business address, nature of profession or business, and corporate group health policy details where relevant.

(h) Insurance history and claim information: details of existing and prior policies, sum insured, premium paid, claim history, claim documents and surveyor reports.

(i) Technical, device and usage information: internet protocol (IP) address, browser type and version, operating system, device type, device identifier, mobile network information, time zone setting, location data (where you have granted location permission), pages visited, time spent, click stream data, referring and exit pages, search queries and crash logs.

(j) Cookies and similar data: information collected through Cookies, including session identifiers, authentication tokens, preferences, marketing attribution parameters and conversion data.

(k) Communication and call recording data: the content and metadata of calls, SMS, emails, WhatsApp and chat conversations between you and us, including telephonic conversation recordings retained for quality assurance, training, regulatory compliance, fraud prevention, dispute resolution and audit purposes.

(l) Marketing and consent records: consent given or withdrawn, marketing preferences, opt out elections, response to surveys and feedback.

(m) Information from third parties: information received from Insurers, third party administrators, hospitals, surveyors, payment aggregators, banks, KYC service providers, Central KYC Records Registry, credit information companies (where permitted), aggregators, employers (for corporate group policies) and from publicly available sources, in each case for the purposes set out in this Policy.

We collect only such Personal Data as is necessary for the lawful purposes set out in Section 6 below, and we endeavour to ensure that the data we collect and process is accurate, complete and up to date.

4. How We Collect Personal Data

We may collect Personal Data through the following means:

- Directly from you when you visit, register, request a quote, fill a proposal form, upload a document, take part in a survey, participate in a campaign or contact us through any channel.
- Automatically through your device, browser and the Cookies and similar technologies deployed on the Portal, as more particularly described in Section 8 of this Policy.
- From third parties such as Insurers, third party administrators, hospitals, surveyors, payment aggregators, banks, KYC service providers, Central KYC Records Registry, employers (in case of group insurance), and from publicly available registries and sources.
- From you when you respond to or interact with our marketing and service communications by call, SMS, email, WhatsApp, Rich Communication Services (RCS), in app or push notifications.
- From a Consent Manager registered with the DPB through whom you have chosen to share your Personal Data with us.

5. Lawful Basis for Processing

We process your Personal Data only on one or more of the following lawful bases, in accordance with Sections 4, 6 and 7 of the DPDP Act:

4. Your free, specific, informed, unconditional and unambiguous consent given by a clear affirmative action through the Portal, including through click wrap acceptance of this Policy and the Terms and Conditions, or through a Consent Manager.
5. Certain legitimate uses where consent is not required under Section 7 of the DPDP Act, including (a) for the specified purpose for which you have voluntarily provided the data, (b) for the performance of any function under any law, (c) for compliance with any judgment, decree or order, (d) for responding to a medical emergency involving a threat to your life or health, (e) for the purpose of employment, (f) for the safety of, or assistance or services to,

any individual during a disaster or breakdown of public order, and (g) for compliance with obligations under Applicable Law.

6. To comply with mandatory legal obligations imposed on us as an IRDAI registered insurance broker, including obligations relating to Know Your Customer (KYC), Anti Money Laundering, record maintenance, regulatory reporting, audit, tax filings and grievance redressal.
7. For the conclusion or performance of a contract to which you are a party, including the insurance contract entered into between you and the Insurer through our facilitation, and the User Broker relationship constituted by your acceptance of our Terms and Conditions.

6. Purposes for Which We Process Personal Data

We process your Personal Data for one or more of the following purposes, each of which constitutes a specific and lawful purpose under Section 6 of the DPDP Act:

- To provide, operate, maintain and improve the Portal and the Services;
- To verify your identity, age, address and other particulars, and to comply with KYC, re KYC, Customer Due Diligence, Enhanced Due Diligence and beneficial ownership requirements under the Prevention of Money Laundering Act, 2002, the IRDAI Master Guidelines on AML/CFT and rules made thereunder;
- To generate quotes, compare products, undertake need analysis and suitability assessment, and to facilitate the issuance, renewal, endorsement, cancellation, portability and migration of insurance Policies;
- To submit and process proposals on your behalf with Insurers, to facilitate underwriting, financial underwriting and medical examination, and to communicate underwriting decisions to you;
- To collect premium and to remit premium to the Insurer in a duly designated Insurance Banking Account in compliance with Section 64VB of the Insurance Act, 1938 and the Brokers Regulations;
- To process refunds (including free look refunds), and to coordinate with the Insurer for claim payouts to the original payment instrument and bank account of the proposer;
- To provide claims assistance, including intimation, document collation, liaison with surveyors, loss adjusters and Third Party Administrators (TPAs), and follow up with the Insurer;
- To send service and transactional communications such as one time passwords, policy and renewal alerts, premium due reminders, claim status updates, KYC reminders and grievance status, by call, SMS, email, WhatsApp, RCS, in app notification and push notification;
- To send promotional and marketing communications relating to insurance and other ancillary products and services offered by us, our affiliates, our Insurer partners and our authorised representatives, subject to your right to withdraw consent for marketing communications;

- To carry out fraud prevention, anti money laundering, sanctions screening, politically exposed person screening, watch list screening and risk management activities;
- To detect, prevent and respond to security incidents, technical issues, abuse, unauthorised use of the Portal or any other unlawful activity;
- To analyse usage patterns, conduct research, measure marketing effectiveness, perform analytics and improve the design and content of the Portal and the Services;
- To handle grievances received from you, in accordance with Schedule I, Form H of the Brokers Regulations, the IRDAI Master Circular on Protection of Policyholders' Interests, 2024, Rule 3(2) of the Information Technology (Intermediary Guidelines) Rules, 2021 and the DPDP Act;
- To comply with reporting, record keeping, audit and regulatory inspection obligations imposed on us by the IRDAI, the DPB, the Reserve Bank of India, the Income Tax Department, the Goods and Services Tax authorities, the Financial Intelligence Unit India and other lawful authorities;
- To establish, exercise or defend legal claims, including in connection with judicial, regulatory or arbitral proceedings;
- To facilitate any actual or proposed merger, demerger, acquisition, restructuring, sale of business or transfer of assets, subject to the safeguards prescribed under the DPDP Act.

We will not use your Personal Data for any new purpose that is materially different from the purpose for which it was collected, unless we obtain your fresh consent or such other lawful basis is available.

7. Special Categories and Sensitive Personal Data

8. Certain Personal Data we collect, in particular health and medical information, financial information, biometric information and Aadhaar related information, constitutes "Sensitive Personal Data or Information" under the SPDI Rules and is also subject to enhanced safeguards under the DPDP Act, the IRDAI Information and Cyber Security Guidelines, 2023 and Section 33B of the Insurance Act, 1938 (relating to client secrecy).
9. By submitting such information through the Portal, by undergoing a pre policy medical examination, or by authorising hospitals, TPAs, laboratories or your existing Insurer to share such information with us, you provide your specific, informed and unambiguous consent to the collection, processing, storage, transfer and disclosure of such Sensitive Personal Data for the purposes set out in this Policy.
10. Aadhaar number, where collected, shall be handled in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, the rules and regulations thereunder, and the directions of the Unique Identification Authority of India (UIDAI). We do not store full Aadhaar numbers unless permitted by law, and we mask Aadhaar numbers wherever feasible.

8. Cookies and Similar Technologies

11. The Portal uses Cookies to (a) enable basic functionality such as security, session management, network management and accessibility; (b) authenticate users and maintain sessions; (c) remember your preferences, language and last accessed page; (d) understand how the Portal is used and measure performance; (e) measure the effectiveness of marketing campaigns and serve more relevant content; and (f) detect and prevent fraudulent activity.
12. We may permit selected third parties to set Cookies on the Portal for analytics, advertising, attribution and fraud prevention purposes, including providers such as Google Analytics, Google Ads, Meta Pixel and similar services. Information collected by these third parties is governed by their respective privacy policies.
13. You can control or disable Cookies through your browser or device settings. Disabling Cookies may impair certain functionality of the Portal. Further details, including the categories of Cookies used, their purpose and retention period, are set out in our Cookie Policy available at jupiterinsurance.in/cookie-policy.

9. Sharing and Disclosure of Personal Data

We share your Personal Data only with categories of recipients listed below and only to the extent reasonably necessary for the purposes set out in this Policy or as required by Applicable Law:

- Insurers and their group entities, for the solicitation, underwriting, issuance, renewal, endorsement, cancellation and servicing of insurance Policies, and for processing of claims and payment of refunds;
- Third Party Administrators (TPAs), hospitals, network providers, surveyors, loss adjusters, investigators and panel doctors empanelled by Insurers, for the processing and settlement of health and other insurance claims;
- KYC service providers, Central KYC Records Registry (CKYCR), Aadhaar authentication service providers and authorised verification agencies, for identity and address verification;
- Payment aggregators and payment gateway service providers authorised by the Reserve Bank of India, for collection of premium and processing of refunds;
- Information technology, cloud, customer relationship management, telephony, communication, analytics, marketing, cybersecurity, fraud detection, document storage, e-sign and email service providers acting as our Data Processors under written contracts that require them to process your Personal Data strictly in accordance with our instructions and in compliance with the DPDP Act;
- Our affiliates, group companies and authorised representatives (including Point of Sales Persons engaged in accordance with Applicable Law), strictly for the purposes set out in this Policy;

- Professional advisers, including legal counsel, auditors, accountants and consultants, under appropriate confidentiality obligations;
- Regulators and government authorities, including the IRDAI, the Data Protection Board of India, the Reserve Bank of India, the Income Tax Department, the Goods and Services Tax authorities, the Financial Intelligence Unit India, the Ministry of Home Affairs, the Insurance Information Bureau of India, the Indian Computer Emergency Response Team (CERT-In), the Unique Identification Authority of India, the Ombudsman, the police, any other statutory authority and any court or tribunal, where required by Applicable Law or pursuant to a lawful request;
- Acquirers, successors, transferees and other relevant parties in connection with any actual or proposed merger, demerger, acquisition, restructuring, sale of business or transfer of assets of Amica;
- Any other recipient with your prior express consent.

We do not sell, rent or trade your Personal Data to any third party for monetary consideration. Where we share Personal Data with Data Processors, we put in place contractual safeguards in accordance with Section 8(2) of the DPDP Act so that such Data Processors process your Personal Data only on documented instructions and in accordance with Applicable Law.

10. Cross Border Transfer of Personal Data

14. Your Personal Data is primarily stored in data centres located in India, in line with the IRDAI Information and Cyber Security Guidelines, 2023 and the IRDAI (Maintenance of Insurance Records) Regulations, 2015 (which require that records of policies and claims are held in data centres situated and maintained in India).
15. Where we engage Data Processors or service providers that operate outside India (for example, certain cloud service providers, email delivery providers and analytics providers), Personal Data may be transferred to and processed in countries other than India. Such transfers are made in accordance with Section 16 of the DPDP Act read with Rule 15 of the DPDP Rules, and are subject to the negative list of countries notified by the Central Government from time to time, and to any sectoral restrictions imposed by the IRDAI or other regulators.
16. Where any data localisation or restriction applies to specific categories of data (such as policyholder claim records, medical records or wellness information), we shall store such data in India and shall not transfer it outside India otherwise than as permitted by Applicable Law.
17. In all cases where Personal Data is transferred outside India, we ensure that the transferee is bound by appropriate contractual obligations to process such data in compliance with the DPDP Act and with no less protection than would be available under Applicable Law in India.

11. Retention of Personal Data

18. We retain your Personal Data only for so long as is necessary for the purposes for which it was collected and as required under Applicable Law, after which it is securely deleted, anonymised or destroyed.
19. Without limiting the foregoing, indicative retention periods are as follows:

- Proposal forms and policy records: for a period of not less than 10 years from the end of the policy term, in accordance with the IRDAI (Maintenance of Insurance Records) Regulations, 2015;
- Claims records, including health records and surveyor reports: for a period of not less than 10 years from the date of full and final settlement or repudiation of the claim, or as required under the IRDAI Master Circular on Health Insurance Business dated 29 May 2024 and the IRDAI (Maintenance of Insurance Records) Regulations, 2015;
- KYC and AML records: for a period of 5 years from the date of cessation of the business relationship or the date of the transaction, as required under Rule 9 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and the IRDAI Master Guidelines on AML/CFT;
- Telephonic call recordings and chat / WhatsApp transcripts: for a minimum period required for regulatory and dispute resolution purposes, typically not less than 5 years;
- Information and communication technology and application log data: rolling 180 days, in accordance with the IRDAI Information and Cyber Security Guidelines, 2023;
- Marketing consent records, withdrawal records and Do Not Disturb (DND) preferences: for as long as you remain a User of the Portal and for a period after that as required for regulatory and dispute resolution purposes.

Following expiry of the applicable retention period, Personal Data is either securely erased, anonymised so that it can no longer be associated with you, or, where Applicable Law so requires, archived for the prescribed period.

12. Your Rights as a Data Principal under the DPDP Act

Subject to the conditions and exceptions specified under the DPDP Act and the DPDP Rules, you have the following rights in respect of your Personal Data:

20. Right to information about Personal Data (Section 11 of the DPDP Act): to obtain a summary of the Personal Data being processed and the processing activities, and the identities of all other Data Fiduciaries and Data Processors with whom the Personal Data has been shared, along with a description of the Personal Data so shared.
21. Right to correction, completion, updation and erasure (Section 12 of the DPDP Act): to request correction of inaccurate or misleading Personal Data, completion of incomplete Personal Data, updation of Personal Data, and erasure of Personal Data that is no longer

necessary for the purpose for which it was processed, except where retention is required for compliance with Applicable Law.

22. Right of grievance redressal (Section 13 of the DPDP Act): to have a readily available means of grievance redressal in respect of any act or omission of Amica regarding the performance of its obligations under the DPDP Act.
23. Right to nominate (Section 14 of the DPDP Act): to nominate any other individual who shall, in the event of your death or incapacity, exercise these rights in accordance with Applicable Law.
24. Right to withdraw consent: to withdraw at any time the consent you have given for the processing of your Personal Data, with the consequence that we may no longer be in a position to provide certain Services to you. Withdrawal of consent will not affect the lawfulness of processing carried out on the basis of consent before its withdrawal, nor will it affect processing required to be carried out under Applicable Law.
25. You may also have additional rights under the SPDI Rules in respect of Sensitive Personal Data or Information collected by us.

To exercise any of the above rights, please write to our Data Protection Officer / Grievance Officer at the contact address set out in Section 17 below. We will respond to your request within the timeline prescribed under the DPDP Act and the DPDP Rules. We may need to verify your identity before we act on your request, and we may decline a request that is manifestly unfounded, excessive or repetitive or that would adversely affect the rights or freedoms of any other person.

You also have the right to register a complaint with the Data Protection Board of India under Section 28 of the DPDP Act if you are dissatisfied with our response to your grievance.

13. Consent, Withdrawal and Consent Manager

26. Wherever processing is based on consent, your consent is requested in clear and plain language and is given by way of a clear affirmative action, such as ticking the consent check box, clicking "I Accept" or "I Agree", entering an OTP, e-signing a proposal or otherwise positively confirming your acceptance through the Portal.
27. Wherever practicable, the consent notice is also made available in any of the languages specified in the Eighth Schedule to the Constitution of India, in accordance with Section 6(3) of the DPDP Act.
28. You may withdraw your consent at any time by writing to us at contact@jupiterinsurance.in, by using the unsubscribe link in any marketing email, or by replying "STOP" or similar keyword to any SMS or WhatsApp marketing message we send to you. Withdrawal of consent shall be subject to the consequences set out in Section 12(5) above.

14. Children and Persons with Disabilities

29. We do not knowingly process Personal Data of children (i.e., individuals under the age of 18 years) for the purpose of profiling, behavioural monitoring, targeted advertising or similar activities.
30. Where insurance cover is sought for a minor as the life or property insured, the proposal must be submitted by a parent or lawful guardian who has insurable interest in the minor and who has the capacity to contract. The Personal Data of the minor shall be processed only on the verifiable consent of the parent or lawful guardian, as required under Section 9 of the DPDP Act.
31. Personal Data of persons with disability who have a lawful guardian shall be processed only on the consent of the lawful guardian, in accordance with Section 9(2) of the DPDP Act.
32. If you believe that we have collected Personal Data of a child or a person with disability without the verifiable consent of the parent or lawful guardian, please contact us so that we can take appropriate action.

15. Marketing and Service Communications

33. By providing your mobile number, email, WhatsApp number and other contact details and accepting this Policy and our Terms and Conditions, you consent to receive (a) service and transactional communications, and (b) promotional and marketing communications from us and our Authorised Recipients (including Insurers, TPAs, payment aggregators, KYC service providers, sub brokers and POSPs) by voice call (manual or auto dialled), SMS, email, WhatsApp (including the WhatsApp Business platform), RCS, push notifications, in app notifications and postal mail.
34. Your consent shall extend to all such communications notwithstanding your registration on the National Customer Preference Register (NCPR) / Do Not Call / Do Not Disturb registries, and notwithstanding the Telecom Commercial Communications Customer Preference Regulations, 2018 and the Distributed Ledger Technology (DLT) framework. You may withdraw consent for marketing communications at any time by writing to contact@jupiterinsurance.in; however, service and transactional communications relating to a Policy procured by you, or required to be sent under Applicable Law, shall continue.
35. Telephonic conversations between you and us may be recorded, stored and transcribed for quality assurance, training, regulatory compliance, fraud prevention, dispute resolution and audit purposes, in accordance with Applicable Law.

16. Security Practices and Procedures

36. We have implemented reasonable security practices and procedures in accordance with the IRDAI Information and Cyber Security Guidelines, 2023, the SPDI Rules, the DPDP Act read with Rule 6 of the DPDP Rules, and prevailing industry standards such as ISO/IEC 27001.

37. Our technical and organisational measures include: (a) administrative controls such as policies, role based access, segregation of duties, periodic training and awareness, background checks of employees and contractors, and confidentiality undertakings; (b) technical controls such as encryption of data in transit and (where appropriate) at rest, multi factor authentication, network segmentation, intrusion detection and prevention systems, firewalls, vulnerability assessments, penetration testing, security operations centre monitoring, data loss prevention and patch management; and (c) physical controls such as secured premises, restricted access, surveillance and visitor management.
38. While we take security seriously, no method of transmission over the internet or method of electronic storage is 100% secure, and we cannot guarantee the absolute security of your Personal Data. You agree to maintain the confidentiality of your Account credentials and OTPs and to promptly notify us of any unauthorised use of your Account.

17. Personal Data Breach Notification

39. In the event of a personal data breach within the meaning of Section 8(6) of the DPDP Act, we shall, in accordance with Rule 7 of the DPDP Rules, intimate the Data Protection Board of India and each affected Data Principal in the manner and within the timelines prescribed under Applicable Law.
40. We shall also report cyber security incidents to the Indian Computer Emergency Response Team (CERT-In) within six hours of becoming aware of such incident, in accordance with Section 70B of the Information Technology Act, 2000 read with the CERT-In Directions dated 28 April 2022, and shall comply with all incident reporting obligations applicable to insurance intermediaries under the IRDAI Information and Cyber Security Guidelines, 2023.

18. Third Party Websites and Links

The Portal may contain links to, or embed content from, websites and applications operated by Insurers, payment aggregators, regulators and other third parties. We do not control such third party websites, and we are not responsible for their privacy practices or the content available on them. We encourage you to read the privacy policies of such third parties before sharing your Personal Data with them.

19. Automated Decision Making and Profiling

41. Certain aspects of the Services, such as automated quote generation, comparison, suitability scoring, fraud detection and risk scoring, may involve automated processing of your Personal Data. We use such automated processing only to support and improve the Services and the decisions taken by Insurers.
42. Where any decision that produces a significant effect on you (such as denial of cover, declining a claim or repudiating a policy) is taken by an Insurer, that decision is taken by the

Insurer based on the underwriting and claim standards adopted by the Insurer, and not by Amica.

20. Updates to this Policy

We may amend, supplement or replace this Policy from time to time, including in order to give effect to changes in Applicable Law or our business practices. The updated Policy shall be published on the Portal with a revised "Last Updated" date and shall take effect upon publication. Where the change is material, we shall make reasonable efforts to notify you (for example, by email, SMS, in app notification or banner on the Portal). Your continued use of the Portal after the publication of the updated Policy shall constitute deemed acceptance of the updated Policy, subject always to your right to withdraw consent.

21. Grievance Officer and Contact Details

For any query, request or complaint relating to this Policy, your Personal Data or your rights as a Data Principal, please contact our Data Protection Officer / Grievance Officer:

Grievance Officer

Name: Sandeep Raj

Designation: Grievance Redressal Officer

Address: Amica Insurance Brokers Private Limited, Office 31, 3rd Floor, Viraj Building, Plot No. 124, S.V. Road, Khar (West), Mumbai 400 052, Maharashtra, India

Email: grievance@jupiterinsurance.in

Phone: +91 8655055086

Resolution timeline: We endeavour to acknowledge all communications within 48 hours of receipt and to provide a substantive response within 14 (fourteen) days, or such other timeline as may be prescribed under the DPDP Act, the DPDP Rules and other Applicable Law.

Escalation: If you are not satisfied with the resolution provided by us, you may escalate your grievance to (a) the Insurance Regulatory and Development Authority of India through the Bima Bharosa Portal at https://bimabharosa.irdai.gov.in/, by toll free number 155255 or 1800 425 4732, or by email at complaints@irdai.gov.in, (b) the Office of the Insurance Ombudsman in accordance with the Insurance Ombudsman Rules, 2017, the list of which is available at https://www.cioins.co.in/, and/or (c) the Data Protection Board of India in accordance with Section 28 of the DPDP Act.

22. Governing Law and Jurisdiction

This Policy shall be governed by and construed in accordance with the laws of India. Subject to the dispute resolution and arbitration provisions set out in our Terms and Conditions, the courts at

Mumbai, Maharashtra shall have exclusive jurisdiction in respect of all matters arising out of or in connection with this Policy.

23. Miscellaneous

43. Severability: If any provision of this Policy is held by any court or competent authority to be invalid, illegal or unenforceable, the remaining provisions shall continue in full force and effect.
44. Waiver: No failure or delay by us in exercising any right under this Policy shall operate as a waiver thereof.
45. Language: This Policy is published in English. Any translation is for convenience only; in the event of any inconsistency, the English version shall prevail.
46. Reading with other documents: This Policy is to be read together with our Terms and Conditions, our Cookie Policy and any product or service specific privacy notices that may be displayed on the Portal.
47. Headings: Headings in this Policy are for convenience only and shall not affect the interpretation of any provision.

By using the Portal, you confirm that you have read, understood and consented to this Privacy Policy.