

Broker Hub SaaS Data Processing Agreement

22 September 2026

Broker and Finova have entered into the Agreement under which Broker is provided access to and use of Broker Hub SaaS during the Term. This Data Processing Agreement (“**DPA**”) is incorporated into and made a part of the Agreement. Unless otherwise agreed, the terms of this DPA take precedence over any conflicting terms in the Agreement.

1. Definitions and Interpretation

The following definitions apply in this DPA.

1.1 Definitions:

Anonymisation Process: means Finova’s method of anonymising personal data by nulling applicant records and identities, disassociating user activity logs, and redacting sensitive values from system logs and models.

Commissioner, Controller, Processor, Data Subject, Personal Data, Personal Data Breach, and Processing: have the meanings given in the Data Protection Legislation.

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (“**DPA 2018**”); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications) and the mandatory guidance and codes of practice issued by the Commissioner or other relevant regulatory authority and which are applicable to a party.

Privacy Policy: means Finova’s privacy statement published at <https://www.finoa.tech/privacy>.

1.2 References to Personal Data in this DPA are references to Personal Data submitted to the Product by or on behalf of Broker. Personal Data does not include Broker’s own business contact details or account information, which are governed by Finova’s Privacy Policy.

1.3 Interpretations and defined terms in the Agreement also apply to this DPA.

2. General Provisions

2.1 Finova and Broker will comply with their respective obligations under the Data Protection Legislation.

2.2 The nature, purposes, subject matter, duration of processing, categories of Personal Data and Data Subjects, and applicable retention periods are described in Annex A.

2.3 Finova may act as Processor and Controller of Personal Data under the Agreement, each as further described in this DPA:

- a. **As Processor:** When Processing Personal Data on behalf of Broker (where Broker is Controller) to prepare, automate and submit applications to lenders using the Product.

Broker retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to Finova.

- b. **As Controller:** When producing and distributing with third parties anonymised (following the Anonymisation Process) aggregated data derived from the Personal Data, including for Finova's commercial benefit. These third parties may include regulators, trade bodies, lenders, and Finova's commercial partners that are relevant to Finova's business. Broker confirms that Finova may use the Personal Data for these purposes, and will ensure that Finova has all necessary rights, permissions, and consents from Data Subjects to do so.

2.4 Finova uses a third-party payment processor, currently Stripe, to process card payments made by the Broker to use the Product. Card data is captured and processed directly by the payment processor and is not received or stored by Finova. The payment processor acts as an independent Controller of that payment data for its own purposes (including fraud prevention and its own regulatory compliance), not as Finova's Processor, and processes it under its own terms and privacy notice. Finova reserves the right to change its payment processor from time to time.

3. Finova as Processor

3.1 Where Finova acts as Processor in respect of Personal Data, Finova will:

- a. only process the Personal Data in accordance with Broker's written instructions, unless otherwise permitted or required by Data Protection Legislation. Finova will promptly notify Broker if, in Finova's opinion, Broker's instructions do not comply with the Data Protection Legislation;
- b. maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third parties unless Broker or this DPA specifically authorises the disclosure, or as required by domestic or EU law, court or regulator (including the Commissioner);
- c. ensure that its employees and contractors are informed of the confidential nature of the Personal Data, are appropriately trained in handling Personal Data, and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;
- d. at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data, taking into account the likelihood and severity of risks to the privacy rights of Data Subjects, including, but not limited to, the security measures set out in Annex B;
- e. notify Broker of a Personal Data Breach without undue delay, unless prohibited by law or government agency; take appropriate measures designed to mitigate the cause(s) of the Personal Data Breach; and provide Broker all necessary information as required under Data Protection Legislation;

- f. comply with Broker's written instructions requiring Finova to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing;
- g. reasonably assist Broker with meeting Broker's compliance obligations under the Data Protection Legislation, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner or other relevant regulator under the Data Protection Legislation; and
- h. as directed by Broker or these terms, delete or return to Broker all Personal Data Processed in connection with the Product, and delete existing copies of the same, following termination of the Agreement, except that Finova will not be required to delete or return that Personal Data, or delete existing copies, to the extent that Finova's storage of that Personal Data or those copies is (1) required by Finova to exercise its rights and perform its obligations under this Agreement; or (2) required or authorised by Data Protection Legislation for a longer period.

3.2 Broker gives its general written authorisation for Finova to engage third party sub-processors (as listed in Annex A) in the Processing of Personal Data in accordance with Customer's instructions and the terms of the written subcontracts between the sub-processors and Finova, provided that:

- a. Finova remains liable to Broker for the acts or omissions of such sub-processors with respect to their processing of Personal Data; and
- b. each sub-processor agrees to protect the Personal Data to standards consistent with the requirements of this DPA.

3.3 Finova may engage sub-processors on a global basis, provided that any such processing complies with Data Protection Legislation and that any transfers of Personal Data outside of the UK/EEA occur under a legally valid transfer mechanism.

3.4 Finova may update the list of sub-processors at least 30 days before making a change by publishing an updated version of this DPA on its website. Broker may object to any new sub-processor by informing Finova at dataprotection@finova.tech within 30 days from the date of publication, whereupon the parties will seek to negotiate a resolution to Broker's objection. If the parties cannot resolve the objection, either party may terminate the Agreement immediately on notice to the other without liability.

3.5 Finova will make available to Broker, no more than once per year and on 30 days' written notice, information reasonably necessary to demonstrate Finova's compliance with its data protection obligations under the Agreement, which Finova may satisfy by providing a completed security questionnaire, summary audit report, or relevant third-party certification. Where such documentation does not reasonably address Broker's concerns, the parties shall discuss in good faith a proportionate alternative, which may include an on-site or system audit conducted at Broker's own cost.

4. Broker Obligations

4.1 Broker acknowledges that it controls the relationship with its clients (as Data Subjects) and that Finova has no direct agreement with them. Broker must therefore present transparent, clear and intelligible information to Data Subjects regarding Broker's and Finova's use of their Personal Data before submitting it to the Product, as required by Data Protection Legislation. Broker may achieve

this through its privacy notice, standard terms of business, or similar communication (“**Privacy Notice**”). Finova offers the following example information for Broker to adapt and include in its Privacy Notice to Data Subjects:

***"How [Broker name] uses automated tools and AI.** We use Finova's Broker Hub platform to prepare and submit decision-in-principle (DIP) and full mortgage applications (FMA) to lenders on your behalf. This includes automated processing and, in some cases, AI-assisted tools that help prepare your application and route it to lenders. We remain responsible for reviewing your information, and no credit search will be carried out without a specific action by us to initiate it. The lender you apply to makes its own, independent decision on your application; we and Finova have no role in, and no visibility of, how that decision is reached. If you have any questions about how Broker Hub processes your information, contact us at [broker contact details] or Finova at dataprotection@finova.tech.*

***Anonymised, aggregated data.** Finova, which provides the Broker Hub platform we use, may produce anonymised, aggregated data from information collected through Broker Hub - for example, average income levels by profession or general location. This data will be anonymised to ensure that no individual can be identified. Following such anonymisation, Finova may share or sell this anonymised and aggregated data to lenders and other organisations for business intelligence and commercial purposes. Finova is the controller for this specific activity and relies on its legitimate interests in producing, and where applicable commercialising this aggregate insight, having assessed that this does not override your interests. Before your information is used in this way, you have the right to object - if you would rather your information were not included, contact us at [broker contact details] or Finova at dataprotection@finova.tech and your data will be excluded from any future aggregation exercise. This will not affect your DIP or FMA application in any way."*

- 4.2 Finova will provide reasonable assistance to Broker with the interpretation of Finova's example language offered in clause 4.1 above; however, (a) Broker remains fully responsible for its compliance with Data Protection Legislation, including its Privacy Notice; and (b) except as required by Clause 3.1(a) of this DPA, Finova will not provide Broker with legal advice or confirmation of Broker's compliance with Data Protection Legislation.
- 4.3 Broker will provide Finova with a copy of Broker's Privacy Notice promptly upon Finova's request. Finova may suspend Broker's access to the Product and delete any data submitted to the Product by or on behalf of Broker if Broker fails to comply with this DPA.
- 4.4 Finova will not be liable for any claim made by a Data Subject arising from or related to Broker's or any of its affiliates' acts or omissions, to the extent that Finova was acting in accordance with Broker's Instructions.
- 4.5 Broker acknowledges that the Product is not intended as a storage repository for Personal Data and that Finova will delete Personal Data in accordance with the data storage and deletion periods stated in the Product. Broker may request changes to these deletion periods using the in-Product configuration tools (if available under Broker's account) or by submitting a support request to the Finova service desk using the contact methods stated in the Product.

ANNEX A - Personal Data processing purposes and details

Subject matter of processing: Finova will Process Personal Data as specified in the Agreement and for the purposes determined by Broker and the Agreement.

Duration of Processing: Finova will process and retain Personal Data for the period described in clause 4.5 of this DPA.

Nature of Processing: Processing activities include hosting and Processing of Personal Data as specifically instructed by Broker or as per the Agreement.

Data Subject Types: The individuals whose Personal Data is submitted to the Product by or on behalf of the Broker in connection with the preparation, processing or submission of a decision-in-principle or mortgage application, comprising: mortgage applicants and prospective borrowers; joint applicants and co-borrowers; guarantors and other security providers; and any other individual referenced in an applicant's financial, employment or affordability information (for example, an employer contact or referee named for verification purposes), in each case to the extent their Personal Data is processed through the Product.

Personal Data Categories: Personal Data processed through the Product in connection with the preparation, processing and submission of decision-in-principle and mortgage applications, in respect of each Data Subject described above, as determined by Broker and which may include: (a) identity data - full name, date of birth, marital status, number of dependants, nationality and residency status; (b) contact data - current and previous residential addresses, email address and telephone number; (c) identification data - passport, driving licence or other government-issued identification document details, used for identity verification; (d) financial and employment data - employment status, employer details, income, outgoings, existing debts, assets and bank account details; (e) credit data - credit history, credit score, existing credit commitments and details of any adverse credit history (including arrears, defaults, county court judgments or bankruptcy); (f) mortgage application data - property and loan details, deposit amount, mortgage term, product and lender selections, decision-in-principle application content, and lender responses and outcomes; (g) platform and technical data - Product account and session logs, IP address and timestamps associated with actions taken on the Product platform; and (h) derived and profiling data - any assessment, score or output generated by the Product's automated tools in preparing, assessing or routing an application (for example, affordability calculations or lender-matching outputs).

Special Personal Data Categories: Special categories of Personal Data requiring special treatment under Data Protection Legislation may be included Personal Data at the discretion of Broker. If any such data is incidentally captured - for example, through free-text fields recording vulnerable-customer information - it will be processed only to the extent necessary, and Broker is responsible for ensuring no such data is submitted other than where necessary and lawful to do so.

Approved sub-processors:

Sub-processor	Purpose	Location
Amazon Web Services	Hosting for Broker Hub and applicant data; AI services via Amazon Bedrock.	UK
Google Cloud	Processes documents uploaded by Brokers;	EEA

	Google Cloud Vertex AI.	
Resend	Email communications.	Ireland
Atlassian/Jira	Support services operated by Finova and offered to Brokers.	EEA

ANNEX B - Technical and Organisational Security Measures

Finova's technical and organisational measures to protect Personal Data are summarised in this Annex B. This Annex B is not exhaustive. During the Term, these measures may change without notice, as standards evolve or as additional controls are implemented or existing controls are modified as Finova deems reasonably necessary; provided, however, any update will not materially reduce the overall protections in this Annex B.

Information Security Program and Team: Finova maintains a formal information security programme covering administrative, technical, physical and organisational safeguards appropriate to the nature, scope, context and purposes of its processing activities, including Broker Hub and its supporting business operations.

Security Certifications: Finova holds ISO 27001:2013 certification from an independent third-party auditor. Finova's infrastructure is hosted by Amazon Web Services, whose data centres are independently certified to ISO 27001, PCI DSS Service Provider Level 1 and SOC 2.

Physical access controls: Finova operates no data centre of its own. All production infrastructure runs in Amazon Web Services facilities in the London region, and physical security is provided by Amazon Web Services: staffed secure premises, perimeter controls, camera surveillance, intrusion detection, and resilient power, cooling and fire suppression. Finova takes reasonable measures to satisfy itself that its hosting provider maintains these controls. Finova also takes reasonable measures, such as security personnel and secured buildings, to prevent unauthorised persons from gaining physical access to its own premises.

System access controls: Finova prevents unauthorized system access using OpenID Connect authentication, enforced inactive session timeouts, password hashing, rate limiting, and role-based authorization per request. Broker-provided lender credentials receive zero-knowledge protection and are encrypted using non-exportable AWS KMS keys. Credentials are write-only, bound cryptographically to specific firms, and never visible to application servers or staff. Decryption occurs strictly at the point of use with short-lived signed grants, and values are immediately wiped from memory. Automated sign-ins use execution-layer placeholder substitution, while logs and session recordings automatically mask all credential data.

Data access controls: Finova restricts data access through least-privilege principles, using narrowly scoped cloud roles. Staff administrative actions and sensitive logs are written to immutable, append-only logs. To prevent tampering, the application's database privileges strictly prohibit updating or deleting these audit records.

Transmission controls: Traffic between a Broker and the service is carried over HTTPS, requests over plain HTTP are redirected, and a minimum of TLS 1.2 is enforced at the network edge. HTTP Strict Transport Security is applied to responses.

Input controls: Finova tracks data changes through functional, append-only event tables that attribute actions to specific users. A managed web application firewall filters common exploit patterns, SQL injection attempts and known bad inputs at the network edge and applies request rate limits. Documents uploaded by Brokers are scanned for malware, and an uploaded object cannot be processed or downloaded until it has been scanned and found clean. Application logs are written in a structured form and passed through a redactor that removes personal data values while preserving correlation identifiers.

Data backups: The production database is backed up automatically and supports point-in-time recovery. Database storage is encrypted at rest. Object storage is versioned, so a previous version of an object can be recovered. Infrastructure state is stored encrypted with concurrent-change locking.

Restore procedures are documented. Finova operates in a single cloud region; there is no second region and no cross-region copy of backups.

Data segregation: Data belonging to different Brokers is logically segregated. Every record is bound to the owning firm or organisation, and all access is scoped to the requesting Broker's own firm, which is established from their membership at the point of authentication. This scoping is additionally enforced inside the database itself through row-level security policies applied to the data tables. Finova's staff administrative surfaces operate in a separate authentication realm and cannot reach Broker data through the customer interface. Outbound connections to lender portals are made from a distinct network address per organisation.