Data Processing Agreement

Last Updated: July 10th, 2026

This Data Processing Agreement ("Agreement") is a legally binding contract between **Nuworks Ltd**, a company incorporated and registered in England, trading as **BrokerCentral** ("BrokerCentral", "Provider", "we", "our", or "us"), and the individual or entity ("Customer", "you", or "your") that accesses, installs, or uses the BrokerCentral software and related services (the "Services").

This Agreement governs the Provider's processing of Personal Data on behalf of the Customer in connection with the provision of the Services as detailed in the Agreement. In the context of this Agreement, the Customer shall be the "**Data Controller**" and the Provider shall be the "**Data Processor**."

1. DEFINITIONS AND INTERPRETATION

In this Agreement, the following definitions apply:

- “AI Functionality” means any artificial intelligence, machine-learning, generative AI, large language model, automated recommendation, prediction, ranking, classification, summarisation, conversational, or other AI-enabled functionality made available as part of the Services.
- “Customer Data” means any data, content, materials, records, prompts, inputs, outputs, Personal Data, or other information submitted to, stored within, or processed through the Services by or on behalf of the Customer.
- "Data Controller": The entity that determines the purposes and means of processing Personal Data.
- "Data Processor": The entity that processes Personal Data on behalf of the Data Controller.
- “Data Protection Laws” means all applicable laws, regulations, regulatory requirements, statutory guidance, and codes of practice relating to Personal Data, privacy, electronic communications, direct marketing, cookies, similar tracking technologies, or AI-enabled processing, in each case to the extent applicable to Personal Data, privacy, electronic communications, or AI-enabled processing, including:
- (a) the UK General Data Protection Regulation (“UK GDPR”);
- (b) the Data Protection Act 2018;
- (c) the Privacy and Electronic Communications Regulations 2003 (“PECR”);
- (d) the Data (Use and Access) Act 2025 (“DUAA 2025”);
- (e) any legislation by which the foregoing is amended, replaced, supplemented or re-enacted; and
- (f) any binding guidance, statutory codes, or regulatory requirements issued by the Information Commissioner’s Office (“ICO”) or other competent supervisory authority.
- “Personal Data” means any information relating to an identified or identifiable natural person as defined under applicable Data Protection Laws.
- “Personal Data Breach” shall have the meaning given under applicable Data Protection Laws.
- "Processing": Any operation performed on Personal Data, including collection, storage, modification, transfer, or deletion.
- “Restricted Transfer” means any transfer of Personal Data that is subject to restrictions under applicable Data Protection Laws relating to international transfers of Personal Data.
- "Sub-Processor": Any third party engaged by the Provider to process Personal Data on behalf of the Customer.
- “Supervisory Authority” means the Information Commissioner’s Office (“ICO”) or any other competent regulatory authority with jurisdiction under applicable Data Protection Laws.
- "Standard Contractual Clauses (SCCs)": The clauses approved by the European Commission or UK authorities for ensuring adequate data protection in international transfers.
- “Tracking Technologies” means cookies, pixels, SDKs, scripts, tags, analytics technologies, telemetry technologies, local storage objects, session technologies, and similar tracking or electronic communications technologies, where used by or on behalf of the Customer through the Services or otherwise used in connection with the provision, security, operation, or support of the Services.

2. ROLES AND RESPONSIBILITIES

2.1 Customer’s Responsibilities

The Customer shall:

(a) comply with all applicable Data Protection Laws in connection with its collection, use, disclosure, storage, transfer, and other processing of Personal Data in connection with the Services;

(b) ensure that it has all necessary rights, permissions, lawful bases, notices, transparency measures, cookie controls, consent mechanisms, consents, and authorisations required to:

- disclose Personal Data to the Provider;
- permit the Provider to process Personal Data in accordance with this Agreement, including where relevant through analytics technologies, telemetry systems, communications systems, AI Functionality, or Tracking Technologies used by or on behalf of the Customer through the Services; and
- use the Services and any AI Functionality lawfully;

(c) ensure that its instructions to the Provider regarding the processing of Personal Data comply with applicable Data Protection Laws and do not place the Provider in breach of applicable law;

(d) remain responsible for the accuracy, quality, legality, and lawfulness of the Personal Data and Customer Data submitted to the Services;

(e) ensure that it does not use the Services:

- for solely automated decision-making or profiling activities producing legal effects or similarly significant effects concerning individuals without appropriate lawful basis, safeguards, and meaningful human oversight;
- in a manner that breaches privacy laws, PECR, Tracking Technologies requirements, electronic communications laws, discrimination laws, insurance regulations, financial services regulations, or consumer protection laws; or
- in connection with prohibited activities identified in the Acceptable Use Policy;

(f) implement and maintain appropriate technical and organisational measures, access controls, authentication measures, and security practices appropriate to the nature of the Personal Data processed by the Customer through the Services; and

(g) cooperate reasonably with the Provider in relation to compliance activities, regulatory enquiries, Data Subject requests, security investigations, audits, and incident response activities where required under applicable Data Protection Laws.

(h) Where applicable, the Customer remains responsible for ensuring that any required notices, transparency measures, consent mechanisms, cookie controls, or permissions relating to Tracking Technologies, electronic communications, or electronic marketing activities are appropriately implemented in accordance with PECR and applicable law.

2.2 Provider's Responsibilities

Taking into account the nature of the processing and the information available to the Provider, the Provider shall provide reasonable assistance to the Customer in relation to:

- responding to Data Subject requests;
- compliance with obligations relating to security of processing;
- Personal Data Breach investigation, mitigation, and notification obligations;
- data protection impact assessments ("DPIAs"); and
- consultations, enquiries, or engagement with supervisory authorities where required under applicable Data Protection Laws.

Standard assistance reasonably required to comply with the Provider's mandatory obligations under applicable Data Protection Laws and this Agreement shall be provided without additional charge.

Where the Customer requests extraordinary, bespoke, excessive, repeated, customer-specific, or disproportionately burdensome assistance, including detailed technical analysis, bespoke reporting, custom data extraction, extended consultancy, significant engineering work, extensive audit support, or support required because of the Customer's own acts, omissions, systems, instructions, or non-compliance, the Provider may charge reasonable fees at its then-current professional services rates or other rates agreed with the Customer, unless prohibited by applicable law.

The Customer acknowledges that it remains responsible for:

(a) determining whether a DPIA, prior consultation, regulatory notification, or other compliance step is legally required; and

(b) ensuring that its use of the Services complies with applicable Data Protection Laws.

2.3 Confidentiality

The Provider shall ensure that persons authorised to process Personal Data:

- are subject to appropriate confidentiality obligations, whether contractual or statutory;
- receive appropriate training relating to data protection and security obligations; and
- access Personal Data only where necessary for the provision of the Services.

2.4 Unlawful Instructions

The Provider shall promptly inform the Customer if, in the Provider's opinion, an instruction infringes applicable Data Protection Laws, unless prohibited from doing so by law.

3. SECURITY MEASURES

3.1 Security Obligations

The Provider shall implement appropriate technical and organisational measures to protect Personal Data from unauthorised access, loss, alteration, or disclosure. These measures include, but are not limited to:

- Encryption: Personal Data shall be encrypted at rest and in transit where applicable.
- Access Control: The Provider will implement secure access controls and authentication mechanisms.
- Regular Security Audits: The Provider shall conduct regular security audits and vulnerability assessments.
- Data Minimisation: The Provider will practice data minimisation, ensuring that Personal Data is retained only as necessary for the provision of services.

3.2 Audit and Review

- The Provider will perform periodic reviews to ensure that security measures remain effective and in line with best practices.

3.3 Information and Audit Rights

The Provider shall make available to the Customer information reasonably necessary to demonstrate compliance with this Agreement and applicable Data Protection Laws.

The parties shall initially seek to satisfy audit and assurance requests through:

- responses to reasonable written questionnaires;
- security documentation and policies;
- summaries of technical and organisational measures;
- third-party audit reports, certifications, penetration testing summaries, or comparable independent verification materials; and
- other information reasonably sufficient to demonstrate compliance.

Where such information is insufficient to reasonably demonstrate compliance, the Customer may request a further audit or inspection relating to the Provider's processing of Personal Data.

Any audit or inspection:

- must be reasonable, proportionate, and limited to matters relevant to the Services and the Customer's Personal Data;
- must be conducted during normal business hours upon reasonable prior written notice;
- must not occur more than once in any twelve (12) month period except following a Personal Data Breach or material security incident affecting the Customer;
- must not unreasonably interfere with the Provider's business operations or compromise the security, confidentiality, or legal obligations owed to other customers; and
- shall be conducted at the Customer's expense unless otherwise required by applicable law.

The Provider may satisfy audit obligations through the provision of independent third-party assurance materials where appropriate.

Nothing in this Clause requires the Provider to disclose:

- confidential information relating to other customers;
- information that would compromise the security of the Services or systems;
- privileged information; or
- information prohibited from disclosure by applicable law or contractual obligation.

4. DATA SUBJECT RIGHTS ASSISTANCE

4.1 Assistance with Data Subject Requests

The Provider shall assist the Customer in responding to Data Subject requests, including:

- The right to access, rectify, and erase Personal Data.
- The right to restrict or object to processing.
- The right to data portability where applicable.

4.2 Notification of Data Subject Requests

- The Provider shall notify the Customer if it receives a Data Subject request directly, without responding unless authorised by the Customer.

4.3 Complaints and Regulatory Cooperation

The Provider shall notify the Customer without undue delay if it receives:

- a complaint relating to the processing of Personal Data on behalf of the Customer;
- correspondence from a supervisory authority relating to such processing; or
- a request relating to Data Subject rights.

Except where required by applicable law, the Provider shall not respond substantively to such complaints or requests without the Customer's prior authorisation and shall provide reasonable cooperation and assistance to the Customer in managing and resolving such matters.

5. DATA BREACH NOTIFICATION

5.1 Notification of Data Breach

In the event of a Personal Data Breach, the Provider shall notify the Customer without undue delay after becoming aware of the breach.

Such notification shall, to the extent reasonably available at the time, include:

- the nature of the Personal Data Breach;
- the categories of affected Personal Data and Data Subjects;
- the likely consequences of the breach;
- the measures taken or proposed to mitigate, investigate, contain, remediate, or prevent further breaches; and
- relevant contact details for follow-up information.

The Provider may provide information in phases or through supplemental notifications where complete information is not immediately available and shall use commercially reasonable efforts to keep the Customer informed of material developments relating to the Personal Data Breach.

5.2 Customer's Breach Obligations

Upon receiving notification of a Personal Data Breach, the Customer shall take reasonable steps to mitigate potential harm, including notifying affected data subjects and relevant authorities where required under Applicable Data Protection Laws. The Provider shall assist the Customer in fulfilling these obligations.

6. INTERNATIONAL DATA TRANSFERS

6.1 Restricted Transfers

The Provider shall not transfer, access, process, store, or otherwise make available Personal Data outside the United Kingdom or any other jurisdiction subject to applicable transfer restrictions unless such transfer complies with applicable Data Protection Laws and this DPA.

6.2 Lawful Transfer Mechanisms

Where a Restricted Transfer occurs, the Provider shall implement lawful transfer mechanisms and appropriate safeguards recognised under applicable Data Protection Laws, which may include:

- adequacy regulations or adequacy decisions;
- the International Data Transfer Agreement ("IDTA");
- the UK Addendum to the EU Standard Contractual Clauses;
- EU Standard Contractual Clauses ("EU SCCs");
- Binding Corporate Rules ("BCRs");
- recognised certification or transfer frameworks, including the UK-US Data Bridge where applicable; or
- other lawful transfer mechanisms, derogations, or safeguards permitted under applicable Data Protection Laws.

6.3 Supplementary Safeguards

Where reasonably required under applicable Data Protection Laws, the Provider may implement supplementary technical, organisational, or contractual safeguards relating to Restricted Transfers, including:

- encryption;
- pseudonymisation;
- access controls;
- data minimisation;
- transfer risk assessments ("TRAs");
- vendor due diligence procedures; and
- contractual security obligations.

6.4 Changes to Transfer Mechanisms

The Provider may update, replace, adopt, or transition to alternative transfer mechanisms or safeguards where reasonably necessary to:

- comply with applicable law or regulatory guidance;
- reflect changes in recognised transfer mechanisms or adequacy decisions;
- address operational, security, or technical requirements;
- support international service providers or Sub-Processors; or
- maintain lawful international transfer arrangements.

6.5 Sub-Processors and International Transfers

The Customer acknowledges that Sub-Processors, including AI service providers, cloud infrastructure providers, support providers, analytics providers, and integration providers, may process Personal Data in jurisdictions outside the United Kingdom where lawful transfer mechanisms and safeguards are maintained in accordance with this DPA.

6.6 Transfer Governance and Cooperation

The Provider may maintain transfer governance documentation, including transfer risk assessments, Sub-Processor records, transfer registers, security assessments, and supporting compliance materials relating to Restricted Transfers.

Upon reasonable written request and subject to confidentiality, security, legal, and operational limitations, the Provider may make available information reasonably necessary to demonstrate compliance with this Clause 6.

7. USE OF SUB-PROCESSORS

7.1 Sub-Processor Engagement

- The Customer provides a general authorisation for the Provider to engage Sub-Processors to process Personal Data. The Provider shall ensure that Sub-Processors are bound by data protection obligations no less stringent than those in this Agreement.

7.2 Sub-Processor Notification

The Provider shall maintain an up-to-date list of Sub-Processors used in connection with the Services and make such list available to Customers through a website, customer portal, or upon written request.

The Sub-Processor list may include:

- the Sub-Processor name;
- the nature of the services provided;
- the general categories of processing performed;
- the primary processing location or region; and
- the applicable international transfer mechanism where relevant.

The Provider shall provide reasonable advance notice of the appointment or replacement of any Sub-Processor that will process Personal Data on behalf of the Customer.

The Customer may object to a new or replacement Sub-Processor on reasonable data protection or security grounds within thirty (30) days of notice.

If the Customer objects to a new or replacement Sub-Processor, the parties shall work together in good faith to seek to resolve the objection, which may include providing additional information, implementing reasonable safeguards, limiting the affected processing activity, or identifying an alternative approach where commercially and technically feasible.

If the parties cannot reasonably resolve the objection, the Customer may terminate the affected Services on written notice without penalty to the extent directly impacted by the relevant Sub-Processor change.

The Provider shall not knowingly permit a new or replacement Sub-Processor to process Customer Personal Data unless the Sub-Processor is subject to written data protection obligations consistent with this Agreement and applicable Data Protection Laws.

The Provider remains responsible for the acts and omissions of its Sub-Processors in relation to their processing of Customer Personal Data to the same extent that the Provider would be responsible if it performed the relevant processing itself.

The Provider shall ensure that Sub-Processors are subject to written data protection obligations that are no less protective than those set out in this Agreement, to the extent applicable to the relevant Sub-Processor's processing activities.

For the avoidance of doubt, the Provider's responsibility for Sub-Processors under this Clause 7.3 is subject to the exclusions, limitations, and liability caps set out in the Agreement, including the Terms of Service, except to the extent such exclusions, limitations, or caps are prohibited by applicable law.

Where a Sub-Processor causes or contributes to a breach, the Provider may seek recovery, indemnity, contribution, damages, or other contractual remedies from that Sub-Processor, but this shall not affect the Customer's rights against the Provider under this Agreement, subject to the exclusions, limitations, and liability caps referred to above.

7.4 AI Sub-Processors and AI Functionality

AI Functionality is live and forms part of the Services.

The Customer acknowledges that, unless expressly agreed otherwise in writing by Provider, the Customer's documented instructions include the processing of Customer Data, prompts, inputs, outputs, metadata, operational data, telemetry data, and Personal Data through AI Functionality to the extent such processing is necessary to provide, operate, secure, support, maintain, monitor, and improve the Services in accordance with this DPA and the Agreement.

AI Functionality is not a separately disableable processing feature at Customer level unless Provider agrees otherwise in writing. The Customer remains responsible for ensuring that its use of the Services, including AI Functionality, is lawful and that relevant individuals receive appropriate transparency information where required under applicable Data Protection Laws.

AI Functionality provides AI-assisted workflow support, including functionality designed to assist with drafting, summarisation, recommendations, operational workflows, and other user-support activities made available within the Services from time to time.

Where the Provider uses artificial intelligence, machine-learning, generative AI, large language model, automated recommendation, prediction, ranking, classification, summarisation, conversational, or similar AI-enabled service providers in connection with the Services or AI Functionality, such providers shall be treated as Sub-Processors where they process Personal Data on behalf of the Customer.

AI Functionality may process Customer Data, prompts, inputs, outputs, metadata, operational data, and Personal Data where such information is submitted to, generated by, or processed through the AI-enabled features of the Services.

AI Functionality is intended to support, and not replace, human decision-making. AI-generated outputs may be inaccurate, incomplete, unreliable, outdated, biased, unexpected, or unsuitable for the Customer's intended use. The Customer must ensure that appropriately qualified personnel apply meaningful human review, verification, and professional judgment before using or relying on AI-generated outputs.

AI-generated outputs must not be used as the sole basis for regulated, legal, financial, insurance, employment, customer-facing, compliance, or similarly significant decisions.

The Provider shall use commercially reasonable efforts to ensure that AI-related Sub-Processors are subject to appropriate contractual, technical, organisational, confidentiality, security, and data protection obligations consistent with this DPA and applicable Data Protection Laws.

The Provider shall use commercially reasonable efforts to ensure that AI Sub-Processors are contractually restricted from unauthorised disclosure, retention, or use of Customer Personal Data or Customer Data outside the provision of the Services.

The Provider does not use Customer Data, Customer Personal Data, prompts or outputs to train public or shared AI models, and contractually restricts relevant AI providers from doing so, unless expressly agreed in writing.

Where applicable, the Provider may implement governance measures relating to AI-enabled processing activities, including:

- vendor due diligence procedures;
- transfer risk assessments;
- security and privacy reviews;
- contractual restrictions relating to AI training or model usage;
- access controls and logging;
- restrictions on the use of Customer Personal Data for public or shared model training;
- supplementary safeguards relating to Restricted Transfers; and
- operational procedures for identifying, investigating, restricting, mitigating, or responding to material security, safety, misuse, or compliance risks relating to AI Functionality.

The Customer acknowledges and agrees that:

- AI-enabled Sub-Processors may process prompts, inputs, outputs, metadata, telemetry, analytics data, operational information, communications metadata, or related Personal Data in connection with AI Functionality;
- AI-enabled processing activities may involve international transfers of Personal Data;
- AI-generated outputs may be probabilistic in nature and may contain inaccuracies, incomplete information, unintended results, or biased outcomes;
- AI Functionality is intended to support human decision-making and is not designed to operate as a solely automated decision-making system unless expressly agreed otherwise in writing;
- Customers remain responsible for applying meaningful human review and oversight where AI-generated outputs may materially affect individuals, insurance decisions, financial outcomes, regulatory obligations, legal rights, or similarly significant outcomes; and
- the Customer remains responsible for ensuring that its use of AI Functionality complies with applicable laws and regulatory requirements relating to automated decision-making, profiling, discrimination, insurance regulation, financial services, consumer protection, and Data Protection Laws.

The Provider may update, replace, suspend, restrict, or discontinue AI-enabled Sub-Processors or AI Functionality where reasonably necessary for legal, regulatory, security, operational, technical, ethical, or third-party dependency reasons.

8. DATA RETENTION AND DELETION

8.1 Retention Period

Upon termination or expiry of the Services, the Provider shall, at the Customer's choice and subject to applicable law, delete or return Personal Data processed on behalf of the Customer within a reasonable period.

The Provider may retain Personal Data where retention is required or permitted for legal, regulatory, security, audit, complaint-handling, insurance, professional indemnity, dispute-resolution, business continuity, backup, archive, or legitimate operational purposes.

Where Personal Data is deleted or returned following termination or expiry of the Services, residual copies may remain in routine operational backups, disaster recovery copies, restricted archive snapshots, logs, or archival systems until those copies expire or are overwritten in accordance with the Provider's standard backup, archive, and retention procedures, unless longer retention is required or permitted under this Agreement, applicable law, or applicable legal, regulatory, security, audit, complaint-handling, insurance, professional indemnity, dispute-resolution, or operational requirements.

8.2 Post-Termination Data Retrieval

Upon the Customer's written request prior to termination, the Provider shall provide a copy of the Customer's data in a commonly used, structured, and machine-readable format, including but not limited to CSV or JSON. Such data migration assistance will be provided at the Provider's standard professional service rates.

8.3 Retention Categories and Operational Retention

The Provider may retain different categories of Personal Data for different periods depending on the nature of the Personal Data, the purpose of processing, the Customer's instructions, the Services used, applicable legal and regulatory requirements, and the Provider's security, audit, backup, archive, and operational requirements.

The table below summarises the Provider's standard retention approach for Personal Data processed in connection with the Services.

Category	Retention Approach
Customer Data processed through the Platform	Retained for the duration of the Services and any applicable post-termination retrieval, deletion, backup, archive, legal, regulatory, security, or operational period described in this Agreement, the Terms of Service, or the Customer's documented instructions.
Account, user administration, and access management records	Retained for as long as necessary to administer user access, support the Services, maintain security, investigate misuse, comply with legal or regulatory obligations, and support audit or dispute-resolution requirements.
Billing, invoicing, subscription, contract, and payment-related records	Retained for as long as necessary for contract administration, tax, accounting, audit, legal, insurance, regulatory, and dispute-resolution purposes.
Customer support records, service communications, complaints, and correspondence	Retained for as long as reasonably necessary to provide support, manage the customer relationship, investigate issues, resolve complaints, evidence communications, and comply with legal, regulatory, audit, or dispute-resolution requirements.
OAuth tokens, authentication tokens, integration tokens, and connected account credentials	Retained only for as long as necessary to provide the relevant integration, authentication, account connection, or security function, unless earlier revoked, disconnected, expired, or deleted.
Audit logs, access logs, security logs, operational telemetry, diagnostics, and monitoring records	Retained for a reasonable period for security, fraud prevention, abuse detection, incident response, troubleshooting, operational resilience, audit, legal, regulatory, and compliance purposes.
Routine operational backups	Retained for up to ninety (90) days.
Monthly archive snapshots	May be retained for up to twelve (12) months where reasonably necessary for regulatory compliance, FCA-related record keeping, complaint handling, audit, tax/accounting, insurance, professional indemnity, dispute resolution, security investigation, legal preservation, or business continuity purposes.
Annual archive snapshots	May be retained for up to seven (7) years where reasonably necessary for regulatory compliance, FCA-related record keeping, complaint handling, audit, tax/accounting, insurance, professional indemnity, dispute resolution, security investigation, legal preservation, or business continuity purposes.
Legal, regulatory, audit, complaint-handling, insurance, professional indemnity, dispute-resolution, or litigation-hold records	Retained for as long as reasonably necessary to comply with applicable legal, regulatory, audit, complaint-handling, insurance, professional indemnity, dispute-resolution, legal preservation, or enforcement requirements.

Personal Data retained in backups, archive snapshots, logs, or restricted archival systems shall remain subject to appropriate technical and organisational measures.

Such Personal Data shall not be actively accessed, restored, searched, or otherwise processed except where reasonably necessary for disaster recovery, service restoration, security investigation, incident response, legal or regulatory compliance, audit, complaint handling, dispute preservation, insurance, professional indemnity, business continuity, or other legitimate operational purposes.

9. LIABILITY AND INDEMNIFICATION

9.1 Customer Indemnity

The Customer shall indemnify the Provider against third-party claims, regulatory claims, losses, damages, liabilities, fines, penalties, costs, and reasonable legal expenses arising directly from:

(a) the Customer's breach of Applicable Data Protection Laws;

(b) unlawful instructions provided by the Customer; or

(c) the Customer's failure to obtain required consents or provide lawful processing notices.

9.2 Provider Indemnity

The Provider shall indemnify the Customer against third-party claims and regulatory claims arising directly from the Provider's material breach of this Agreement or Applicable Data Protection Laws to the extent caused by the Provider's negligence, wilful misconduct, or unlawful processing of Personal Data.

9.3 Exclusions

Neither party shall be liable under this Clause to the extent the relevant claim arises from:

(a) the acts or omissions of the other party;

(b) compliance with the other party's instructions;

(c) modifications made by the other party; or

(d) circumstances outside the indemnifying party's reasonable control.

9.4 Liability Limits

The indemnities in this Clause are subject to the limitations and exclusions of liability set out in the Terms of Service unless otherwise prohibited by applicable law.

10. GOVERNING LAW AND DISPUTE RESOLUTION

10.1 Governing Law

This Agreement shall be governed by and construed in accordance with the laws of England and Wales. Any disputes arising out of or in connection with this Agreement, including any question regarding its existence, validity, or termination, shall be subject to the exclusive jurisdiction of the courts of England and Wales.

10.2 Dispute Resolution

Disputes under this Agreement shall be governed by the dispute resolution provisions of the Terms of Service.

11. MISCELLANEOUS

11.1 Conflict with Main Agreement

In the event of any conflict between this Agreement and the main Agreement, this Agreement shall prevail with respect to data protection matters.

11.2 Severability

If any provision of this Agreement is deemed invalid or unenforceable, the remaining provisions shall remain in full force and effect.

11.3 Interpretation

This Agreement shall be interpreted in a manner intended to satisfy the requirements of Article 28 of the UK GDPR and applicable Data Protection Laws.

ANNEX 1 - TECHNICAL AND ORGANISATIONAL MEASURES

The Provider shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing Personal Data. These measures are designed to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services. The following outlines the key technical and organisational measures that the Provider has in place:

1. Data Security Measures

1.1 Encryption

- Data at Rest: Personal Data stored by the Provider is encrypted using encryption mechanisms including AES-256 where applicable.
- Data in Transit: Personal Data transmitted over the network is encrypted using HTTPS with Transport Layer Security (TLS).

1.2 Access Control

- The Provider implements role-based access control (RBAC) to ensure that only authorised personnel can access Personal Data.
- Access is restricted to only those employees or systems that require it for the provision of the Services.
- All access to Personal Data is logged for auditing purposes.

1.3 Authentication and Identity Management

- The Provider supports configurable multi-factor authentication (MFA), strong password policies, and identity and access management controls designed to help secure systems processing Personal Data.
- MFA is supported and customer-configurable but is not currently mandatory. Customers are responsible for deciding whether to enable MFA for their authorised users, taking into account the nature of their use of the Services, the sensitivity of the Personal Data processed, and their own security and compliance obligations.
- The Provider applies identity and access management controls designed to restrict access to systems processing Personal Data to authorised personnel, users, or systems with a legitimate need for such access.
- The Provider applies the principle of least privilege, so that personnel and systems are granted access only to the data and functionality reasonably required for their role or function.

2. Incident Management and Response

2.1 Incident Detection

The Provider maintains operational monitoring, telemetry, alerting, logging, and incident response procedures designed to support the security, availability, reliability, and integrity of the Services.

The Provider may use infrastructure, security, logging, monitoring, and operational telemetry tools where appropriate for service security, incident detection, troubleshooting, abuse prevention, and platform reliability.

2.2 Incident Response and Mitigation

- The Provider has procedures for managing security incidents, including procedures for containing the incident, investigating the cause, and remediating any weaknesses.
- A post-incident review is conducted after every security event to ensure that appropriate actions are taken to improve systems and prevent future incidents.

2.3 Security Breach Notification

- The Provider commits to notifying the Customer without undue delay after becoming aware of a Personal Data Breach, including details about the breach and the steps taken to mitigate the impact.

3. Data Retention and Minimisation

3.1 Data Retention

- The Provider retains Personal Data only for as long as necessary to provide the Services or as otherwise required or permitted for legal, regulatory, security, audit, complaint-handling, insurance, professional indemnity, dispute-resolution, business continuity, backup, archive, or legitimate operational purposes.
- Personal Data will be deleted, returned, or anonymised upon termination of the Agreement or when it is no longer required for processing, subject to the backup, archive, legal, regulatory, security, and operational retention exceptions set out in this Agreement.

3.2 Data Minimisation

- The Provider follows a data minimisation approach, ensuring that only the minimum amount of Personal Data necessary for the provision of the Services is collected, stored, or processed.

3.3 Data Destruction

- Upon the expiration or termination of the Agreement, the Provider will either return or securely destroy all Personal Data according to the Customer's instructions, unless the Provider is legally required to retain the data.

4. System and Network Security

4.1 Firewalls and Perimeter Security

- The Provider's hosting service employs firewalls and other perimeter security measures to prevent unauthorised access to systems processing Personal Data. These are regularly updated to mitigate vulnerabilities.

4.2 Network Segmentation

- The Provider's hosting service uses network segmentation to isolate sensitive data processing systems from general network traffic, reducing the impact of potential breaches.

4.3 Vulnerability Management

- The Provider maintains vulnerability management processes designed to identify, assess, and address security weaknesses affecting systems used to provide the Services.
- The Provider may conduct vulnerability assessments, security reviews, patching, remediation tracking, and related security testing activities on a risk-based basis.
- External vulnerability assessment and penetration testing are currently being trialled using AppCheck. No final independent penetration test report is currently available.
- The Provider may update its vulnerability management and security testing arrangements from time to time to reflect changes in the Services, security risks, operational requirements, vendor arrangements, and industry practices.

5. Personnel and Organisational Measures

5.1 Employee Training

- The Provider provides training to its employees on data protection, security best practices, and the handling of Personal Data. All employees with access to Personal Data are made aware of their responsibilities and obligations under the Applicable Data Protection Laws.

5.2 Confidentiality and Non-Disclosure Agreements (NDAs)

- All employees and contractors involved in processing Personal Data are required to sign confidentiality agreements to ensure the protection of Personal Data and adherence to security protocols.

5.3 Audits and Compliance

- The Provider conducts regular internal audits to verify compliance with its security policies, including the protection of Personal Data.
- The Provider ensures that all subcontractors and Sub-Processors comply with these measures through contractual agreements.

6. Business Continuity and Disaster Recovery

6.1 Backup and Data Recovery

The Provider maintains backup procedures designed to support the availability and recoverability of Personal Data processed through the Services.

The Provider performs regular backups and conducts daily backup restoration/load checks designed to confirm that backups load correctly.

Routine operational backups are retained for up to ninety (90) days. The Provider may also retain restricted monthly and annual archive snapshots in accordance with Clause 8.1.

Restoration timing depends on the nature, severity, and scope of the relevant incident, the affected systems or data, and any applicable operational, legal, security, or regulatory constraints. Formal Recovery Time Objective (RTO) and Recovery Point Objective (RPO) commitments are not provided unless expressly agreed in an Order Form or applicable service schedule.

6.2 Disaster Recovery Procedures

The Provider maintains operational recovery procedures designed to support service continuity and recovery following material disruption.

Formal disaster recovery testing commitments, RTOs, and RPOs are not provided unless expressly agreed in an Order Form or applicable service schedule.

7. Sub-Processor Security Measures

7.1 Sub-Processor Monitoring

- The Provider ensures that any Sub-Processor it engages implements appropriate security measures to protect Personal Data.

7.2 Contractual Safeguards

- The Provider enters into written agreements with all Sub-Processors to ensure they adhere to industry-recognised security and compliance standards, including breach notification protocols and data protection obligations.

ANNEX 2 – PROCESSING DESCRIPTION AND DATA PROCESSING DETAILS

1. Subject Matter of Processing

The Provider processes Personal Data for the purpose of providing the BrokerCentral software platform, related support services, hosting, maintenance, integrations, analytics, security, and associated operational services under the Agreement.

2. Duration of Processing

Personal Data shall be processed for the duration of the Agreement and any applicable post-termination retention, backup, transition, legal, regulatory, security, or disaster recovery periods described in the Agreement and this Data Processing Agreement.

3. Nature of Processing

Processing activities may include:

- collection;
- storage;
- organisation;
- hosting;
- retrieval;
- consultation;
- use;
- transmission;
- export;
- backup;
- deletion;
- anonymisation;
- support and maintenance;
- security monitoring;
- troubleshooting;
- analytics, operational telemetry, communications processing, security monitoring, troubleshooting, and operational monitoring; and
- other processing activities reasonably necessary to provide the Services.

4. Purpose of Processing

Personal Data is processed solely for the purposes of:

- providing the Platform and Services;
- user authentication and access management;
- customer support and service administration;
- communications and notifications initiated by the Customer;
- platform security, monitoring, fraud prevention, and incident response;
- regulatory and legal compliance;
- service analytics, operational telemetry, communications management, security monitoring, fraud prevention, troubleshooting, and operational improvement in accordance with the Agreement; and
- other documented instructions of the Customer consistent with the Services.

5. Categories of Personal Data

Categories of Personal Data processed may include:

- names;
- business contact details;
- email addresses;
- telephone numbers;
- account credentials and authentication identifiers;
- insurance policy information;
- claims information;
- customer/client records;
- communications data;
- transaction records;
- audit logs;
- technical usage data, operational telemetry data, communications metadata;
- IP addresses;
- device and browser information; and
- any other Personal Data uploaded or submitted by the Customer through the Platform.

6. Categories of Data Subjects

Categories of Data Subjects may include:

- the Customer's employees, contractors, and authorised users;
- the Customer's clients, customers, policyholders, claimants, prospects, and brokers;
- third parties whose information is submitted by the Customer through the Platform;
- suppliers, advisers, and business contacts; and
- Website or Platform users.

7. Special Category Data, Criminal Offence Data, and Sensitive Processing

The parties acknowledge that the Services are used in connection with insurance broking, insurance administration, compliance, customer onboarding, claims, underwriting support, fraud prevention, and related workflow activities.

Depending on the Customer's use of the Services and the Personal Data submitted by or on behalf of the Customer, Personal Data processed through the Services may include Special Category Data and/or criminal offence data where such data is uploaded, submitted, generated, stored, or otherwise processed through the Platform by or on behalf of the Customer.

Special Category Data may include, for example, health information, medical information, vulnerability information, disability information, or other sensitive information relevant to insurance broking, claims, underwriting, compliance, or customer support activities.

Criminal offence data may include information relating to criminal convictions, offences, allegations, fraud indicators, sanctions, adverse checks, or related information where submitted by or on behalf of the Customer.

The Customer is responsible for determining whether Special Category Data and/or criminal offence data is processed through the Services and for ensuring that:

(a) an appropriate lawful basis under Article 6 UK GDPR has been identified and documented;

(b) where Special Category Data is processed, an appropriate condition under Article 9 UK GDPR and any applicable condition under the Data Protection Act 2018 has been identified and documented;

(c) where criminal offence data is processed, an appropriate condition under Article 10 UK GDPR and Schedule 1 of the Data Protection Act 2018 has been identified and documented;

(d) all necessary notices, consents, permissions, authorisations, transparency information, policy documents, appropriate policy documents where required, and regulatory requirements have been satisfied;

(e) the processing instructions provided to the Provider are lawful, fair, transparent, proportionate, and compliant with applicable Data Protection Laws;

(f) the Special Category Data and/or criminal offence data submitted to the Services is relevant, adequate, limited to what is necessary, and not excessive for the Customer's processing purposes; and

(g) appropriate Customer-side safeguards, access controls, retention controls, staff training, and governance measures are implemented.

The Provider shall process Special Category Data and/or criminal offence data solely:

- in accordance with the Customer's documented instructions;
- as necessary to provide, secure, support, maintain, or improve the Services;
- in accordance with this DPA and the Agreement; and
- subject to appropriate technical and organisational measures.

Where applicable, the parties acknowledge that processing of Special Category Data and/or criminal offence data may require additional safeguards, security measures, transfer mechanisms, access restrictions, retention controls, appropriate policy documents, regulatory assessments, or data protection impact assessments under applicable Data Protection Laws.

The Customer remains responsible for ensuring that its use of the Services in connection with insurance, claims, underwriting, compliance, fraud prevention, customer onboarding, vulnerability assessment, or other regulated activities complies with applicable Data Protection Laws and any applicable insurance, financial services, consumer protection, anti-discrimination, or regulatory requirements.

8. International Transfers

International transfers of Personal Data shall be governed by Clause 6 of this Agreement and applicable lawful transfer mechanisms.

9. Sub-Processors

The Provider may engage Sub-Processors in accordance with Clause 7 of this Agreement.

Categories of Sub-Processors may include:

- cloud hosting providers;
- infrastructure and platform providers;
- customer support providers;
- monitoring and security providers;
- analytics providers;
- communication service providers;
- AI service providers; and
- professional advisers and contractors.

The Provider shall maintain and make available an up-to-date Sub-Processor list in accordance with this Agreement.

10. Frequency of Processing

Processing shall occur on a continuous and ongoing basis as necessary to provide the Services during the Term of the Agreement.

