Data Processing Agreement

Last Updated: February 25th, 2025

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:

- **"Applicable Data Protection Laws"**: All privacy and data protection laws that apply, including the UK GDPR and the Data Protection Act 2018, and any other relevant regulations.
- **"Personal Data"**: Any information relating to an identified or identifiable natural person, as defined under the Applicable Data Protection Laws.
- **"Processing"**: Any operation performed on Personal Data, including collection, storage, modification, transfer, or deletion.
- **"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.
- **"Sub-Processor"**: Any third party engaged by the Provider to process Personal Data on behalf of the Customer.
- **"Standard Contractual Clauses (SCCs)"**: The clauses approved by the European Commission or UK authorities for ensuring adequate data protection in international transfers.

2. Roles and Responsibilities

2.1 Customer’s Responsibilities

- The Customer is the Data Controller and is responsible for ensuring that Personal Data provided to the Provider is collected and processed lawfully, in compliance with all applicable data protection laws, including the UK GDPR and the Data Protection Act 2018.
- The Customer is responsible for obtaining necessary consents from Data Subjects, ensuring that they are informed of their rights under Applicable Data Protection Laws, and providing them with a Privacy Notice outlining how their Personal Data will be collected, used, and processed. The Customer must also ensure that the data subjects have been notified of their rights to access, rectify, erase, restrict, or object to the processing of their Personal Data, and that any data transfer to the Provider complies with all applicable legal requirements.
- The Customer remains responsible for ensuring that any third-party services, systems, or processors they engage outside of the Provider comply with applicable data protection laws. The Provider is not liable for unauthorised data processing conducted by third-party services that the Customer chooses to integrate with.

2.2 Provider’s Responsibilities

- The Provider is the Data Processor and shall only process Personal Data on the documented instructions from the Customer, unless required to do so by law. The Provider shall ensure that Personal Data is processed solely for the purposes outlined in the Agreement and this Data Processing Agreement (DPA).
- The Provider will assist the Customer in complying with its obligations under the Applicable Data Protection Laws, including providing support in responding to Data Subject requests such as the right of access, rectification, erasure, restriction, data portability, and objection to processing, as well as in ensuring compliance with the security, breach notification, and impact assessment obligations. The Provider will also cooperate with the Customer in fulfilling its obligations to notify Data Subjects and data protection authorities, where required, in the event of a Personal Data Breach.

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.

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.

5. Data Breach Notification

5.1 Notification of Data Breach

In the event of a Personal Data Breach, the Provider will notify the Customer without undue delay (within 72 hours) after becoming aware of the breach. The notification shall include:

- The nature and scope of the breach.
- Categories and number of affected Data Subjects.
- Measures taken to mitigate the breach and prevent further incidents.

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 Transfer of Personal Data

The Provider shall not transfer Personal Data outside the UK unless:

- The recipient country has an adequacy decision under the UK GDPR.
- Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) are in place.
- The Customer has provided prior written consent.

6.2 Notification of Data Transfers

- The Customer will be notified of any international data transfers involving Personal Data.

7. Use of Sub-Processors

7.1 Sub-Processor Engagement

- The Customer authorises 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 and provide notice to the Customer of any changes. The Customer has the right to object to new Sub-Processors on reasonable privacy/security grounds.
- The Provider shall notify the Customer at least 30 days in advance before appointing any new Sub-Processor. If the Customer objects on reasonable data protection grounds within this period, the Provider will engage in good faith discussions to resolve the concern.

7.3 Liability for Sub-Processors

- The Provider remains fully liable for any breaches caused by its Sub-Processors. If a Sub-Processor is found responsible for a breach, the Provider retains the right to seek damages or contractual remedies from the Sub-Processor to recover costs incurred by the Customer.

8. Data Retention and Deletion

8.1 Retention Period

- Upon termination, all Personal Data shall be deleted or returned within 30 days unless required to be retained by law. Backup copies shall be securely retained in accordance with Provider policy before automatic deletion, except where legally required to retain them.

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, JSON). Such data migration assistance will be provided at the Provider's standard professional service rates.

9. Liability and Indemnification

9.1 Indemnification

- The Customer shall indemnify the Provider for any claims, penalties, or damages arising from the Customer's failure to comply with Applicable Data Protection Laws or unauthorised instructions provided to the Provider.

9.2 Provider's Indemnification

- The Provider shall indemnify the Customer for breaches caused by its own negligence or non-compliance with this Agreement.

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

- Any disputes under this Agreement shall follow the dispute resolution process outlined in the BrokerCentral 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.

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 AES-256 encryption.
- **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 uses strong password policies, multi-factor authentication (MFA), and identity management practices to secure user access to systems processing Personal Data.
- The Provider enforces the principle of "least privilege," ensuring that each user only has access to the data they need to perform their job functions.

2. Incident Management and Response

2.1 Incident Detection

- The Provider maintains a security operations team available 24/7 to detect, respond to, and mitigate any security incidents that may affect Personal Data.
- The Provider's hosting service uses intrusion detection and prevention systems (IDS/IPS) to monitor network traffic and systems for suspicious activity.

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 within 72 hours of detecting any 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. Personal Data will be deleted or anonymised upon the termination of the Agreement or when the data is no longer required for processing.

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 conducts regular vulnerability assessments and penetration testing to identify and address security weaknesses.
- The Provider also maintains a patch management process to ensure that all systems are up-to-date with the latest security patches.

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 performs regular backups of Personal Data and stores backups in secure, geographically redundant locations.
- In the event of a disaster or data loss, the Provider has procedures in place to restore Personal Data within a defined recovery time objective (RTO).

6.2 Disaster Recovery Plan

- The Provider maintains a comprehensive disaster recovery plan that is tested, at minimum annually, to ensure the swift recovery of services in the event of a catastrophic incident.
- The Provider's business continuity plan also includes procedures for maintaining essential services during disruptions.

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.