DATA PROTECTION ADDENDUM (DPA)

Infollion Research Services Limited

This Data Protection Addendum ("Addendum") between **Infollion Research Services Limited** ("**Infollion**") and the Customer (as defined in the Agreement) forms part of the **Infollion** Terms of Service set forth at **https://www.infollion.com/privacy-policy**, or such other written or electronic agreement incorporating this Addendum, in each case governing Customer's access to and use of the Services (the "Agreement").

Customer enters into this Addendum on behalf of itself and any Affiliates authorised to use the Services under the Agreement who have not entered into a separate contractual arrangement with **Infollion**. For the purposes of this Addendum only, and except where otherwise indicated, references to "Customer" shall include Customer and such Affiliates. The Parties agree that the terms set out below shall be added as an Addendum to the Agreement.

1. Definitions

In this Addendum, the following terms shall have the meanings set out below, and cognate terms shall be construed accordingly:

- "Affiliate" means an entity that owns or controls, is owned or controlled by, or is under common control or ownership with either Customer or Infollion, where control means the power to direct the management and policies of an entity, whether through ownership of voting securities, by contract, or otherwise.
- "Customer Personal Data" means any Personal Data provided by or made available by Customer to **Infollion**, or collected by **Infollion** on behalf of Customer, which is Processed by **Infollion** to perform the Services.
- "Controller to Processor SCCs" means (i) the standard contractual clauses for cross-border transfers published by the European Commission on 4 June 2021, as adopted by the European Commission and the Swiss Federal Data Protection and Information Commissioner ("Swiss FDPIC") (collectively, "EU SCCs"); (ii) the international data transfer addendum ("UK Transfer Addendum") adopted by the UK Information Commissioner's Office ("UK ICO"); or (iii) any similar clauses adopted by a data protection regulator relating to transfers of Personal Data to Third Countries, including any successor clauses.
- "Data Protection Laws" means any local, state, or national law regarding the processing of Personal Data applicable to **Infollion** in the jurisdictions in which the Services are provided to Customer, including without limitation the Digital Personal Data Protection Act, 2023 (India), the EU GDPR, the UK GDPR, the Swiss DPA, and the CCPA/CPRA, together with privacy, security, and data protection laws generally.
- "EU Area" means the European Union, European Economic Area, United Kingdom, and Switzerland, and "EU Area Law" means the laws relating to data protection, security, or privacy that apply in the EU Area, including the EU GDPR, UK GDPR, and Swiss DPA, and any successors or amendments thereto.

- "Security Incident" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data being Processed by **Infollion**.
- "Services" means the services to be supplied by **Infollion** to Customer or Customer's Affiliates pursuant to the Agreement.
- "Third Country" means a country that, where required by applicable Data Protection Laws, has not received an adequacy decision from an applicable authority relating to cross-border transfers of Personal Data.

The terms "Business", "Business Purpose", "Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Process", "Processor", "Sell", "Service Provider", "Share", "Sub-processor", "Supervisory Authority", "Data Fiduciary", "Data Principal", and "Third Party" have the meanings given to them under applicable Data Protection Laws. Capitalised terms not otherwise defined in this Addendum have the meanings given in the Agreement.

2. Scope of Addendum

This Addendum applies to **Infollion**'s Processing of Customer Personal Data under the Agreement, to the extent such Processing is subject to Data Protection Laws. This Addendum is governed by the governing law of the Agreement unless otherwise required by Data Protection Laws.

3. Roles of the Parties

The Parties acknowledge and agree that, with regard to the Processing of Customer Personal Data, and as more fully described in Annex 1, Customer acts as a Business, Controller, or Data Fiduciary, and **Infollion** acts as a Service Provider, Processor, or Data Processor. This Addendum applies solely to the Processing of Customer Personal Data by **Infollion** acting as a Processor, Sub-processor, or Third Party (as specified in Annex 1).

Customer shall be solely responsible for timely communications to its Affiliates or the relevant Controller(s) receiving the Services, where such communications are required under applicable Data Protection Laws. Customer is also solely responsible for complying with Security Incident notification laws applicable to Customer and for fulfilling its own obligations to notify government authorities, affected individuals, or others in relation to any Security Incident.

4. Data Processing Terms

4.1 Customer Obligations

Customer shall comply with all applicable Data Protection Laws in connection with this Addendum and the Processing of Customer Personal Data. Customer shall Process Customer Personal Data within the Services and provide **Infollion** with instructions that comply with applicable Data Protection Laws. As between the Parties, Customer is solely responsible for the lawfulness of the collection of Customer Personal Data and its transfer to **Infollion**. Customer agrees not to provide **Infollion** with any data concerning a natural person's health, religion, or any special categories of data as defined in Article 9 of the GDPR.

4.2 Provider Obligations

Infollion shall comply with all applicable Data Protection Laws in the Processing of Customer Personal Data, and shall:

- (a) Documented Instructions: Process Customer Personal Data only for the purposes of the Agreement and as set out in Annex 1, and otherwise solely on the documented instructions of Customer. The Agreement, this Addendum, and Customer's use of the Services' features constitute Customer's written instructions. **Infollion** shall not Sell or Share Customer Personal Data, nor use, retain, disclose, or otherwise Process it outside its business relationship with Customer or for any other purpose, except as required or permitted by law. **Infollion** shall promptly inform Customer if it determines it can no longer meet its obligations under Data Protection Laws, or if, in its opinion, an instruction infringes applicable Data Protection Laws. Customer reserves the right to take reasonable steps to ensure Processing is consistent with its obligations and to discontinue and remediate any unauthorised use of Customer Personal Data.
- (b) Permitted Processing: Process Customer Personal Data solely to the extent necessary to (i) perform the Business Purposes and its obligations under the Agreement; (ii) operate, manage, test, maintain, and enhance the Services; (iii) disclose aggregate statistics about the Services in a manner that prevents identification or re-identification of any individual; or (iv) protect the Services from threats; or where required by a court order or authorised governmental agency, provided prior notice is given to Customer where legally permitted; or as otherwise expressly authorised by Customer. **Infollion** shall not combine Customer Personal Data with Personal Data received from another person or collected from its own interactions with individuals, except as permitted under the Agreement to perform the Services.
- (c) Confidentiality: Ensure that personnel authorised to Process Customer Personal Data are bound by confidentiality obligations or an appropriate statutory duty of confidentiality.
- (d) Security Measures: Implement and maintain the technical and organisational measures set out in Annex 1, and, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, as well as the risks to the rights and freedoms of natural persons, maintain measures designed to ensure a level of security appropriate to the risk in accordance with Article 32 of the GDPR, including pseudonymisation and encryption of Customer Personal Data; ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems; restoring availability and access to Customer Personal Data in a timely manner following a physical or technical incident; and regularly testing, assessing, and evaluating the effectiveness of these measures.
- (e) Sub-processors: Customer generally authorises **Infollion** to engage Sub-processors, including those listed in Annex 2, subject to **Infollion** (i) notifying Customer at least **[30]** calendar days in advance of any intended changes or additions to Annex 2; (ii) imposing data protection obligations on each Sub-processor that are materially the same as those in this Addendum; and (iii) remaining liable to Customer for any failure by a Sub-processor to fulfil its obligations. Customer may object in writing on reasonable data protection grounds within **[30]** days of such notice, following which the Parties shall work together in good faith for up to **[30]** days to find a commercially reasonable solution. Where no solution is found, either Party may terminate the affected Services on written notice, without penalty, but without prejudice to fees incurred prior to termination.

- (f) Compelled Disclosure: To the extent legally permissible, promptly notify Customer of any legally binding request for disclosure of Customer Personal Data (such as by law, court order, or subpoena). Where a request is not legally binding, Customer Personal Data will not be disclosed, and **Infollion** will notify Customer of the rejection of the request. A record of all legally binding disclosure requests shall be maintained.
- (g) Data Subject Requests: To the extent legally permissible, promptly notify Customer of any communication from a Data Subject or Data Principal regarding the Processing of Customer Personal Data, or any communication from a Supervisory Authority. **Infollion** will not respond to any such request unless expressly authorised by Customer or required by law, and will reasonably assist Customer, through appropriate technical and organisational measures, in fulfilling Customer's obligation to respond to requests for exercising Data Subject rights. Customer agrees to pay **Infollion** for reasonable time and out-of-pocket expenses incurred in providing such assistance.
- (h) Breach Notification: Upon becoming aware of a Personal Data Breach involving Customer Personal Data, notify Customer without undue delay **[and in any event within 72 hours]**, including, to the extent reasonably available, all information reasonably required by Customer to comply with its own breach reporting obligations. **Infollion** shall take all measures necessary to remedy or mitigate the effects of the Security Incident and keep Customer reasonably informed. Notification of a Security Incident is not an acknowledgement of fault or liability. Security Incidents do not include unsuccessful attempts that do not compromise the security of Customer Personal Data, such as unsuccessful log-in attempts, pings, port scans, or denial-of-service attacks on firewalls or networked systems.
- (i) Assistance: To the extent required by applicable Data Protection Laws, provide reasonable assistance to Customer with its obligations under Articles 32 to 36 of the GDPR (security, breach notification, data protection impact assessments, and prior consultation), taking into account the nature of the Processing and the information available to **Infollion**. Customer agrees to pay for reasonable time and expenses incurred in connection with assistance under Articles 35 and 36.
- (j) Return or Deletion: Cease Processing Customer Personal Data on termination or expiry of the Agreement and, at Customer's option, return or delete (including by rendering non-readable) all copies of Customer Personal Data within **[90 days]**, except to the extent applicable law requires retention. Any retained Customer Personal Data remains subject to the confidentiality obligations of the Agreement.
- (k) Records and Audits: Maintain records necessary to demonstrate compliance with its obligations, and make available to Customer information reasonably necessary to demonstrate compliance with this Addendum, allowing for and contributing to audits, including inspections, by Customer or an independent auditor mandated by Customer, subject to reasonable prior notice, conduct during normal business hours, and measures to prevent unnecessary disruption. In the first instance, once per year, **Infollion** will provide responses to security assessments **and, where available, its ISO 27001 certificate]**; only where compliance cannot be established from these shall Customer request an inspection. Customer agrees to pay for reasonable time and expenses incurred in connection with audits and assessments.

5. Warranties

The Parties warrant that they, and any staff and subcontractors, will comply with their respective obligations under applicable Data Protection Laws for the term of the Agreement.

6. Restricted Transfers

The Parties agree that where a transfer of Customer Personal Data from Customer or its Affiliates (as exporter) to **Infollion** (as importer) is a Restricted Transfer and EU Area Law applies, the transfer shall be subject to the appropriate Controller to Processor SCCs, which are incorporated into this Addendum as follows:

- EU GDPR: The EU SCCs will apply, completed as follows: Module Two (controller to processor) will apply; in Clause 7, the optional docking clause will apply; in Clause 9, Option 2 will apply and the notice period for Sub-processor changes shall be as set out in Section 4.2(e); in Clause 11, the optional language will not apply; in Clause 17, Option 1 will apply and the EU SCCs will be governed by **[Irish]** law; in Clause 18(b), disputes shall be resolved before the courts of **[the Republic of Ireland]**; Annex I of the EU SCCs shall be deemed completed with the information in Annex 1 to this Addendum; and Annex II of the EU SCCs shall be deemed completed with the information in Section 4 of Annex 1.
- Swiss DPA: The EU SCCs shall apply as above, with references to the EU GDPR read as references to the Swiss DPA, references to the EU, Union, Member State, and Member State law read as references to Switzerland and Swiss law, references to the competent supervisory authority and courts read as references to the relevant Swiss authority and courts, and with the SCCs governed by the laws of Switzerland.
- UK GDPR: The EU SCCs shall apply as above, as modified by the Part 2 Mandatory Clauses of the UK Transfer Addendum, which is incorporated into this Addendum. Tables 1 to 3 of Part 1 of the UK Addendum shall be completed with the information in Annex 1, and Table 4 shall be deemed completed by selecting both "Importer" and "Exporter".
- India (DPDPA): Transfers of personal data outside India shall be made in accordance with the DPDPA, 2023 and shall not be made to any country or territory restricted by the Central Government by notification.

AI processing clause: Infollion shall process Personal Data using AI and machine learning technologies within hosting region, Mumbai India, in accordance with this Addendum and applicable Data Protection Laws. Such AI processing is limited to the provision of the Services and shall be conducted only to the extent necessary to achieve the specified purposes. Delete if not applicable.}}

Infollion shall not participate in any other Restricted Transfers of Customer Personal Data unless made in compliance with applicable Data Protection Law and pursuant to the relevant Standard Contractual Clauses between the exporter and importer. If the applicable Transfer Mechanism is insufficient to safeguard the transferred Customer Personal Data, the data importer will promptly implement supplementary measures (such as encryption or pseudonymisation) to ensure the data is protected to the standard required under Data Protection Laws. If the data importer receives a request from a public authority to access Personal Data, it will, where legally allowed, challenge the request, promptly notify the data exporter, disclose only the minimum amount of Personal Data required, and keep a record of the disclosure.

7. Precedence

The provisions of this Addendum are supplemental to the Agreement. In the event of any inconsistency, the order of precedence shall be: (a) any Standard Contractual Clauses or other agreed cross-border transfer mechanisms; (b) this Addendum; and (c) the Agreement. Where any provision of this Addendum or the Agreement contradicts the Controller to Processor SCCs, the SCCs will control.

8. Indemnity

To the extent permissible by law, Customer shall defend **Infollion** and its Affiliates (the "Indemnified Parties") from and against any claims, demands, suits, or proceedings brought by any third party, and shall indemnify and hold harmless the Indemnified Parties from and against all losses, damages, liabilities, fines, penalties, settlements, and costs (including reasonable legal, investigatory, and consultancy fees) arising from any breach by Customer of this Addendum or of its obligations under applicable Data Protection Laws. **Infollion** may participate in the defence or settlement of any such claim with counsel of its choosing at its own expense.

9. Severability

If any section or sub-section of this Addendum is held by a court or competent authority to be unlawful or unenforceable, it shall not invalidate or render unenforceable any other section of this Addendum.

10. Miscellaneous

This Addendum takes into account and follows the principles of privacy by design and by default; achieving security of Processing; notification of breaches involving Customer Personal Data to the relevant Supervisory Authority and to Customer; conducting privacy impact assessments where appropriate and required by applicable Data Protection Law; and providing assistance where prior consultation with Supervisory Authorities is required. Infollion shall comply with all applicable statutory and regulatory requirements **[and maintains alignment with ISO/IEC 27001:2022.**

Where a Data Subject or Data Principal wishes to exercise rights under applicable Data Protection Law, including access, correction, or erasure of Personal Data in Infollion ’s control, or wishes to raise a concern or complaint relating to Customer Personal Data, they may contact the **[Data Protection Officer / Grievance Officer]**:

Name: Ms Aastha Talwar

Email: **aastha.talwar@infollion.com]**

Annex 1 — Description of Processing Activities

This Annex sets out details of the Processing of Customer Personal Data by **Infollion** in connection with the Services.

1. List of Parties

Data Exporter	
Name	Customer (as defined in the Agreement)
Address	As set forth in the relevant Order Form
Contact person	As set forth in the relevant Order Form
Activities relevant to the transfer	Recipient of the Services provided by Infollion under the Agreement
Signature and date	As set out in the Agreement
Role	Controller / Business / Data Fiduciary
Data Importer	
Name	**Infollion Research Services Limited**
Address	5th Floor, Tower C, Unitech Cyber Park, Sector 39, Gurugram, Haryana, India – 122001
Contact person	**Abhishek Jha, CFO , secretarial@infollion.com**
Activities relevant to the transfer	Provision of the Services to Customer in accordance with the Agreement
Signature and date	As set out in the Agreement
Role	Processor / Service Provider / Data Processor

2. Competent Supervisory Authority

As determined by application of Clause 13 of the EU SCCs. For processing subject to the DPDPA, the competent authority is the Data Protection Board of India.

3. Processing Information

Categories of data subjects	Customer's authorised users of the Services
Categories of personal data	Processed automatically by the Services: **[e.g., names, email login and usage data]**. Processed where provided by Customer or its authorised users: **[e.g., address, date of birth, employment details, or other data uploaded to the platform]**.

Sensitive / special category data	None. Customer agrees not to submit special categories of data to the Services.
Frequency of the transfer	Continuous, for the duration of the Agreement
Nature and purpose of the processing	The provision of the Services to Customer as described in the Agreement and accompanying Order Forms, including hosting, storage, retrieval, analysis, and display of Customer Personal Data within the platform.
Retention period	As described in the Agreement, this Addendum, and accompanying Order Forms; Customer Personal Data is returned or deleted within **[90 days]** of termination, subject to legal retention requirements.
CCPA Business Purposes (where applicable)	helping to ensure security and integrity; debugging to identify and repair errors; performing services on behalf of the business; internal research for technological development; verifying or maintaining the quality or safety of the service; engaging sub-contractors meeting CCPA service provider requirements; and preventing, detecting, or investigating security incidents.

4. Technical and Organisational Security Measures

The following measures are implemented by **Infollion** as data importer to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing and the risks to the rights and freedoms of natural persons:

- Security Management: Designated security personnel responsible for the information security programme; management-approved security policies reviewed at least annually; independent third-party risk assessments at least annually; a risk treatment programme covering penetration testing, vulnerability management, and patch management; a vendor management programme; and regular review of security incidents including root cause analysis.**The information security management system complies with ISO/IEC 27001:2022**
- Personnel Security: Background checks to the extent legally permissible; written confidentiality agreements at the time of hire; privacy and security training for all personnel; and role-appropriate additional requirements for personnel handling Customer Personal Data.
- Access Controls: Formal access management with request, review, approval, and provisioning; periodic access reviews; multi-factor authentication or single sign-on for administrators and end users; least privilege and need-to-know principles; unique user IDs; strong password policies covering complexity, expiry, lockout, and reuse; and audit logging of access and changes.
- Infrastructure and Network Security: Hosting on **[Linode & E2E]** with multi-availability-zone resilience and regular backup restoration testing; hardened server operating systems; code review processes; disaster recovery programmes that are regularly planned and tested; security logging to support audits and detect attacks; regular

vulnerability scans with risk-based remediation; and virtual firewall or security group controls on the production environment.

- Encryption and Data Handling: HTTPS (SSL/TLS) encryption for data in transit and encryption for data at rest; logical isolation of each customer's data in the multi-tenant environment; a central authentication system across the Services; and secure disposal of Customer Personal Data through defined data destruction processes.
- Incident Response: Documented incident management policies with escalation procedures, monitoring of communication channels for security incidents, prompt reaction to suspected or known incidents, mitigation of harmful effects, and documentation of incidents and outcomes.

Execution

IN WITNESS WHEREOF, the Parties have caused this Addendum to be executed by their duly authorised representatives.

For Infollion Research Services Limited	For Customer
Signature: _____	Signature: _____
Name: **Abhishek Jha**	Name: _____
Designation: **CFO**	Designation: _____
Date: _____	Date: _____