Sellestial

DATA PROCESSING ADDENDUM

Effective Date: 2025-09-17

This Data Processing Addendum (the "**DPA**") supplements and forms part of the agreement between **Sellestial, Inc.** ("**Processor**"), a Delaware C-corporation with a principal place of business at 251 Little Falls Drive, Wilmington, DE 19808, United States, and the entity that has entered into a SaaS Subscription Agreement or Master Services Agreement with Sellestial ("**Controller**").

Each of Processor and Controller is referred to herein as a "**Party**" and collectively as the "**Parties**."

This DPA is incorporated by reference into and forms part of either the SaaS Subscription Agreement ("**SSA**") or the Master Services Agreement ("**MSA**") between the Parties (each, a "**Principal Agreement**"). In the event of any conflict between a Principal Agreement and this DPA regarding the Processing of Personal Data, this DPA shall control.

1. BACKGROUND AND SCOPE

1.1 Purpose and Background

Controller wishes to engage Processor to provide certain services as described in the Principal Agreement, which may involve the Processing of Personal Data on Controller's behalf. This DPA sets forth the additional terms, conditions, and obligations of the Parties with regard to such Processing of Personal Data.

1.2 Applicability

This DPA shall apply only to the extent Processor Processes Personal Data that is subject to EU Data Protection Laws, the UK GDPR, the CCPA, or any other applicable data protection laws (collectively, "**Applicable Data Protection Laws**").

1.3 Order of Precedence

For data-protection matters the Parties agree to the following hierarchy: (i) the applicable Order Form or Statement of Work, (ii) this DPA (including any exhibits, addenda, and the

Standard Contractual Clauses), and (iii) the SSA or MSA, as applicable. Where these documents conflict on Personal Data topics, the higher-ranking document governs.

2. DEFINITIONS

Capitalized terms not defined herein shall have the meanings set forth in the Principal Agreement. In this DPA:

2.1 **"Controller"** has the meaning given to it (or to "business") under Applicable Data Protection Laws, and, as used herein, refers to the entity that determines the purposes and means of Processing Personal Data.

2.2 **"Processor"** has the meaning given to it (or to "service provider"/"processor") under Applicable Data Protection Laws, and, as used herein, refers to the entity that Processes Personal Data on behalf of the Controller.

2.3 **"EU Data Protection Laws"** means the EU General Data Protection Regulation 2016/679 ("**GDPR**"), as well as all EU or EEA member state laws implementing or supplementing the GDPR, and the GDPR as incorporated into UK law by virtue of Section 3 of the UK's European Union (Withdrawal) Act 2018 ("**UK GDPR**").

2.4 **"CCPA"** means the California Consumer Privacy Act of 2018 (Cal. Civ. Code §1798.100, et seq.), as amended by the California Privacy Rights Act ("CPRA"), and any related regulations.

2.5 **"Personal Data"** means any information relating to an identified or identifiable natural person and that is (i) subject to Applicable Data Protection Laws; and (ii) provided by Controller to Processor or otherwise collected or received by Processor on behalf of Controller in connection with the Principal Agreement.

2.6 **"Processing"** (and its grammatical variations) means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, including but not limited to collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment or combination, restriction, erasure, or destruction.

2.7 **"Security Measures"** means commercially reasonable administrative, technical, and organizational safeguards designed to protect the confidentiality, integrity, availability, and resilience of Personal Data in Processor's possession or control, as described in this DPA and further detailed in an attached exhibit, if applicable.

2.8 **"Subprocessor"** means any third party (including any Processor Affiliate) engaged by Processor to assist in Processing Personal Data on behalf of Controller under this DPA.

2.9 **"Standard Contractual Clauses" or "SCCs"** means the European Commission's standard contractual clauses for the transfer of Personal Data to third countries, including

the applicable modules and any successor clauses recognized under EU Data Protection Laws.

2.10 **"Prohibited Data"** means (i) special categories of personal data as described in Article 9 GDPR, (ii) data regarding criminal convictions or offenses, (iii) protected health information subject to HIPAA or similar laws, (iv) biometric identifiers, (v) personal data of children under sixteen (16) years of age, and (vi) any classified, export-controlled, or otherwise restricted data that the Parties have not expressly agreed in writing to Process.

3. ROLES AND RESPONSIBILITIES

3.1 Relationship of the Parties

For purposes of this DPA, the Parties acknowledge and agree that Controller is the Controller (or “business”) and Processor is the Processor (or “service provider”) with respect to the Processing of Personal Data hereunder.

3.2 Controller's Instructions

Processor shall Process Personal Data only in accordance with Controller’s documented instructions, which include the Principal Agreement and this DPA, unless otherwise required by law. If Processor believes any instruction violates Applicable Data Protection Laws, it shall promptly inform Controller. Processor shall not be liable for any claim arising from compliance with Controller’s instructions that Processor has timely communicated to Controller as being in violation of Applicable Data Protection Laws, absent Processor’s breach of this DPA.

3.3 Details of Processing

The subject matter, nature, and purpose of Processing, the types of Personal Data, and categories of Data Subjects are set out in **Exhibit A** (Description of Processing) to this DPA (or in the Principal Agreement or applicable Order Form if similar detail is provided there).

4. PROCESSOR OBLIGATIONS

4.1 Confidentiality

Processor shall ensure that any person it authorizes to Process Personal Data is subject to a duty of confidentiality (whether contractual or statutory) and shall not Process such data except on Processor's instructions.

4.2 Security Measures

Processor shall implement and maintain appropriate technical and organizational Security Measures to protect Personal Data from (i) accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access, and (ii) all other unlawful forms of Processing. Such measures shall be commensurate with the risk of Processing and the nature of the Personal Data, taking into account current industry practices and the costs of implementation. An illustrative description of such measures is appended as **Exhibit B** (Security Measures).

4.3 Assistance with Controller Obligations

Taking into account the nature of the Processing and the information available to Processor, Processor shall provide reasonable assistance to Controller with respect to:

a. **Data Subject Requests.** Processor shall, to the extent permitted by law, promptly notify Controller if it receives a request from a Data Subject to exercise rights under Applicable Data Protection Laws (e.g., access, rectification, erasure, restriction, data portability, or objection). Processor shall not respond to such request except (i) to direct the Data Subject to contact Controller; or (ii) with Controller's prior written instructions.

b. **Compliance Obligations.** Processor shall assist Controller with Controller's obligations pursuant to Articles 32–36 of the GDPR (or equivalent requirements under other laws), including data protection impact assessments (DPIAs), consultations with supervisory authorities, and breach notification obligations, to the extent applicable and required.

c. **Audits.** Processor shall allow for and contribute to audits described in **Section 8** (Audits).

4.4 Personal Data Breach Notification

Processor shall, after becoming aware of any Personal Data Breach affecting Personal Data Processed on behalf of Controller, notify Controller within a maximum of 24 hours after becoming aware of a personal data breach and provide reasonable information regarding (i) the nature of the Personal Data Breach; (ii) the affected categories and approximate number of Data Subjects and records; (iii) the likely consequences; and (iv) any measures taken or proposed to address the breach. The Parties agree that Controller has the sole responsibility for complying with any third-party notification obligations arising from such a breach.

4.5 Data Minimization & Proportionality

Processor shall Process Personal Data only to the minimum extent necessary to fulfill its obligations under the Principal Agreement and this DPA, and shall not retain Personal Data longer than is necessary for such purposes, subject to any longer retention period required by applicable law.

4.6 No Sale of Personal Data (CCPA)

Processor shall not sell Personal Data or share Personal Data for cross-context behavioral advertising as defined under the CCPA, nor shall Processor collect, retain, use, or disclose Personal Data for any purpose other than for the specific purpose of performing the services specified in the Principal Agreement, including retaining, using, or disclosing Personal Data for a commercial purpose other than providing the services.

4.7 Prohibited Data

Controller shall not provide Processor with, and Processor shall have no obligation to Process, any Prohibited Data unless the Parties execute a written amendment expressly authorizing such Processing.

Sellestial

5. SUBPROCESSING

5.1 Authorization for Subprocessing

Controller authorizes Processor to engage Subprocessors to Process Personal Data in connection with the services under the Principal Agreement, provided that Processor maintains an up-to-date list of all current Subprocessors at https://sellestial.com/legal/SL-STD.pdf (the "**Subprocessor List**") and provides Controller with at least fifteen (15) business days' prior written notice (the “Notice Period”) of any intended addition or replacement of a Subprocessor. Processor shall not disclose or otherwise make available Personal Data to a proposed Subprocessor until (a) Controller has given its written approval or (b) the Notice Period has expired without Controller having raised a written objection in accordance with Section 5.3.

5.2 Subprocessor Obligations

Processor shall enter into a written agreement with each Subprocessor imposing data protection obligations that are substantially similar to those set forth in this DPA. Processor remains responsible for any acts or omissions of its Subprocessors that cause Processor to breach any of its obligations under this DPA.

5.3 Updates to Subprocessor List and Objection Right

Each notice delivered under Section 5.1 shall identify the proposed Subprocessor, its location, and the Processing activities it will perform. Controller may object to the engagement of the proposed Subprocessor on reasonable, data-protection-related grounds by delivering written notice to Processor within the Notice Period. Upon receipt of a timely objection, the Parties shall cooperate in good faith to resolve the objection, which may include considering an alternative Subprocessor or implementing additional safeguards. If the Parties do not reach a mutually acceptable resolution within thirty (30) calendar days after Processor receives Controller’s objection, Controller may, as its sole and exclusive remedy, terminate the affected services upon written notice.

6. INTERNATIONAL DATA TRANSFERS

6.1 Transfers of Personal Data

To the extent Processor Processes Personal Data from the EEA, UK, or Switzerland in a country that has not been deemed to provide an adequate level of protection under Applicable Data Protection Laws, the Parties agree that such transfers shall be governed by the appropriate transfer mechanism recognized or adopted by the European Commission or other relevant authority (e.g., Standard Contractual Clauses).

6.2 Standard Contractual Clauses (SCCs)

Where required by EU Data Protection Laws, the SCCs shall be deemed incorporated by reference or attached hereto as **Exhibit C**. The Parties will complete all relevant modules, appendices, and information required by the SCCs. If there is a conflict between the SCCs and this DPA, the SCCs shall prevail.

6.3 UK and Swiss Addenda

If Controller's Personal Data includes data protected by the UK GDPR or the Swiss Federal Act on Data Protection, the Parties shall incorporate any relevant addenda or amendments required for lawful transfers, including the UK International Data Transfer Addendum or Swiss-specific provisions, as applicable.

6.4 Additional Safeguards

Where required by law, the Parties shall evaluate on a case-by-case basis whether additional safeguards are necessary to lawfully transfer Personal Data outside of the EEA, UK, or Switzerland, in consideration of local legal frameworks, surveillance laws, and Processor's ability to protect Personal Data.

7. RETURN OR DELETION OF PERSONAL DATA

7.1 Return or Deletion

Upon expiration or termination of the Principal Agreement, Processor shall, at Controller's choice, either return or securely delete all Personal Data in its possession or control, unless retention is required by applicable law. If Controller fails to provide instructions for returning or deleting Personal Data within thirty (30) days following termination or expiration, Processor may delete such Personal Data.

Processor will send an automated reminder at least five (5) days before deletion and will ensure backups are purged at the end of their retention period.

7.2 Backup Copies

Processor may retain Personal Data in routine backup copies for the period such copies are retained in the ordinary course of business, provided that such Personal Data remains protected in accordance with this DPA and is not further Processed except for backup recovery or as otherwise required by law.

8. AUDITS

8.1 Audit Rights

Controller (or its appointed third-party auditor) may audit Processor's compliance with this DPA, including obtaining information about Processor's security practices and policies. Any audit shall be:

a. limited to once per 12-month period, unless required more frequently by law;

b. conducted during Processor's normal business hours upon reasonable advance written notice (30 days), and subject to any applicable confidentiality or security measures;

c. limited in scope to matters directly relevant to Processor's compliance with this DPA and Applicable Data Protection Laws.

8.2 Third-Party Certifications

In lieu of Controller conducting an audit, Processor may provide a current attestation or certificate (e.g., ISO 27001, SOC 2 Type II, or similar) or relevant audit reports prepared by an independent third party, along with any additional information reasonably requested by Controller.

8.3 Costs and Confidentiality

Controller shall bear any costs of the audit unless the audit reveals a material breach of this DPA by Processor, in which case Processor shall bear its own costs. Controller shall treat any information disclosed during the audit as Processor's confidential information.

9. LIABILITY

9.1 Liability

The liability of each Party under or in connection with this DPA (including its exhibits or annexes) is subject to the limitations of liability set forth in the Principal Agreement. If the Principal Agreement does not limit liability, then each Party's aggregate liability under this DPA shall not exceed the amounts paid or payable by Controller to Processor under the Principal Agreement in the twelve (12) months preceding the event giving rise to the liability.

9.2 Third-Party Beneficiaries

Except for Controller's Data Subjects (to the extent they may invoke certain rights under Applicable Data Protection Laws or the Standard Contractual Clauses, if applicable), there are no third-party beneficiaries to this DPA.

10. GOVERNING LAW

10.1 Governing Law

Except to the extent otherwise required by EU Data Protection Laws (or other Applicable Data Protection Laws), this DPA shall be governed by and construed in accordance with the governing law identified in the Principal Agreement.

Sellestial

11. GENERAL PROVISIONS

11.1 Entire Agreement; Amendments

This DPA, including any exhibits, annexes, or attachments, and the Principal Agreement constitute the entire agreement between the Parties relating to the Processing of Personal Data and supersede all prior agreements or understandings with respect to such subject matter. Any changes or modifications to this DPA must be in writing and signed by both Parties (or otherwise validly executed electronically, if agreed).

11.2 Severability

If any provision of this DPA is deemed invalid or unenforceable by a court of competent jurisdiction, the remainder of this DPA shall remain valid and in effect, and the Parties shall promptly amend the invalid provision so that it becomes valid and enforceable while preserving the Parties' original intent.

11.3 Conflict

In the event of any conflict or inconsistency between this DPA (and its exhibits or attachments) and the Principal Agreement, the terms of this DPA will prevail solely with respect to the Processing of Personal Data.

11.4 Counterparts

This DPA may be executed in counterparts (including by electronic signature or via digital agreement), each of which will be deemed an original and all of which together will constitute one instrument.

EXHIBIT A

DESCRIPTION OF PROCESSING

1. Subject Matter and Duration

a. **Subject Matter:** The Processing of Personal Data as described in the Principal Agreement and this DPA, for purposes of providing the agreed-upon SaaS or related services.

b. **Duration:** For the term of the Principal Agreement and any applicable record-retention or transition period thereafter, subject to any early return/deletion of data on Controller's request.

2. Nature and Purpose of Processing

a. Processor will host, store, collect, create, organize, use, modify, analyze, enrich, transfer, and otherwise process Personal Data as necessary to provide the services described in the Principal Agreement.

b. Processing may include analyzing data for AI-driven insights, sending data to third-party AI or data enrichment providers, generating outbound messages, and providing additional functionalities typical of sales or marketing automation platforms, as further described in the Principal Agreement.

3. Types of Personal Data

Depending on Controller's usage of the services, examples may include:

a. Basic contact data (e.g., names, email addresses, job titles)

b. Professional profiles (e.g., LinkedIn URLs, phone numbers, employer name, business contact details)

c. CRM data (e.g., contacts, deals, notes, communications)

d. Email or messaging content, logs, and metadata

e. Any other data that Controller or its Authorized Users choose to import or synchronize.

4. Categories of Data Subjects

a. Controller's customers or prospective customers (including leads or prospects)

b. Controller's employees, contractors, or authorized users (to the extent such data is collected or synchronized in the system)

c. Other individuals whose Personal Data may be contained in communications or CRM records provided by Controller to Processor.

5. Frequency of Transfer

Ongoing throughout the duration of the Principal Agreement, as determined by Controller's use of the services.

6. Obligations and Rights of Controller

a. Controller is solely responsible for ensuring that it has all necessary and appropriate consents or legal bases to process and transfer Personal Data to Processor, and for verifying that the security measures set forth in this DPA and the Principal Agreement satisfy Controller's compliance obligations under Applicable Data Protection Laws.

EXHIBIT B

SECURITY MEASURES

1. Organization of Information Security

a. Designated personnel responsible for information security and compliance.

b. Policies and procedures to protect information assets and review security practices regularly.

c. Formal ISO 27001-aligned ISMS with documented policies, risk assessments, and a designated ISO 27001 Management Representative.

2. Physical Security

a. **Cloud Data Center Reliance**. Processor does not maintain or operate its own on-premises data centers. All production servers and infrastructure are hosted through reputable third-party cloud service providers. Those providers maintain industry-

standard physical security controls for their facilities, including controlled access, 24/7 on-site security, surveillance, and intrusion detection.

b. **Minimal On-Site Storage**. Processor does not store Personal Data in paper form or on local servers within its office. All internal systems and employee devices access Personal Data via secure cloud-based tools and services.

c. **Workplace Controls**. Processor's office is a standard workspace without dedicated server rooms. Access to the office space is controlled (e.g., locked doors, building key cards), and visitors (if any) are supervised.

d. **Endpoint Security**. Employees use laptops for day-to-day operations. These laptops are password-protected, encrypted where practicable, and subject to Processor's acceptable use and security policies.

3. Logical Access Controls

a. Role-based access control.

b. Unique user IDs, strong password policies, multi-factor authentication where feasible.

c. Restricted administrative access to limited personnel with a need-to-know.

4. Data Encryption

a. Encryption of Personal Data in transit using TLS/SSL or equivalent.

b. Encryption at rest using AES-256 or equivalent for stored Personal Data.

c. Securing encryption keys with industry-standard key management processes.

5. Network Security

a. Firewalls, intrusion detection/prevention systems, and regular vulnerability scans.

b. Segregation of environments (e.g., development, staging, production) to minimize risk.

6. Operational Security

a. Maintenance of audit logs for key systems, with regular review for anomalies.

b. Formal change management procedures, including patching and updates for software.

7. Personnel Security

a. Background checks for employees with access to critical systems (as permitted by law).

b. Mandatory confidentiality and data protection training and acknowledgements.

8. Incident Response

a. Written incident response plan, with defined roles and responsibilities.

b. Procedures for escalation, investigation, remediation, and post-incident reviews.

9. Business Continuity & Disaster Recovery

a. Redundant systems and backup strategies for critical data.

b. Regular testing of failover and data recovery procedures.

10. Testing & Auditing

a. Periodic penetration testing and vulnerability assessments.

b. Third-party assessments or certifications (e.g., ISO 27001, SOC 2 Type II, or similar).

(Processor reserves the right to modify these Security Measures at any time, provided such modifications do not materially reduce the overall level of protection.)

EXHIBIT C

STANDARD CONTRACTUAL CLAUSES

(Controller to Processor — Module Two)

SECTION I

Sellestial

Clause 1

Purpose and scope

a. The purpose of these standard contractual clauses (hereinafter: **"Clauses"**) is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council (**"GDPR"**) for the transfer of personal data to a third country.

b. The Parties:

   i. **the natural or legal person(s), public authority/ies, agency/ies, or other body/ies (hereinafter "entity/ies") transferring the personal data**, as listed in **Annex I.A** (hereinafter each "data exporter"), and

   ii. **the entity/ies in a third country receiving the personal data** from the data exporter, directly or indirectly via another entity also party to these Clauses, as listed in **Annex I.A** (hereinafter each "data importer"),

have agreed to these Clauses, including the **Annexes**, which form an integral part thereof.

c. These Clauses apply with respect to the transfer of personal data as specified in **Annex I.B**.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Articles 46(1) and 46(2)(c) of the GDPR, and, with respect to data transfers from controllers to processors and/or processors to processors, Article 28(7) of the GDPR, provided they do not contradict data protection obligations the Parties have under the GDPR.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of the GDPR.

Clause 3

Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

    i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

    ii. Clause 8.1(b), 8.9(a), (c), (d), and (e);

    iii. Clause 9(a), (c), (d), and (e);

    iv. Clause 12(a), (d), and (f);

    v. Clause 13;

    vi. Clause 15.1(c), (d), and (e);

    vii. Clause 16(e).

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

a. Where these Clauses use terms defined in the GDPR, those terms shall have the same meaning as in the GDPR.

b. These Clauses shall be read and interpreted in the light of the provisions of the GDPR.

c. These Clauses shall not be interpreted in a way that contradicts the rights and obligations provided for in the GDPR.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data and the purposes of processing, are specified in **Annex I.B**.

SECTION II — OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The Parties warrant that they have taken appropriate technical and organisational measures to ensure the security of personal data, including protection against a personal data breach, in accordance with Article 32 GDPR.

8.1 Instructions

a. The data importer shall process the personal data only on documented instructions from the data exporter. By entering into these Clauses, the data importer confirms that it has received and will comply with the instructions set out in the Principal Agreement/DPA, as updated from time to time by the data exporter.

b. The data importer shall immediately inform the data exporter if it cannot follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in **Annex I.B**, unless it receives further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of the Clauses (including the Annexes) available to data subjects free of charge. To the extent necessary to protect business secrets or other confidential information, the data exporter may redact part of the text.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in **Annex I.B**. After the end of the provision of services, the data importer shall, at the data exporter's choice, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return all the personal data to the data exporter and delete existing copies, unless EU or Member State law requires storage of the personal data.

8.6 Security of processing

a. The data importer shall implement the technical and organisational measures specified in **Annex II** to ensure the security of personal data. This includes protecting data against breaches leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access.

b. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

c. The data importer shall ensure that any person acting under its authority, including a processor, is bound by confidentiality and processes the personal data only as instructed.

8.7 Sensitive data

If the transfer involves sensitive data, the data importer shall apply specific restrictions or safeguards to adequately protect such data, in accordance with the level of risk involved.

8.8 Onward transfers

The data importer shall only disclose personal data to third parties in the same country or another third country under the same conditions received from the data exporter. This includes onward transfers to a sub-processor or another recipient, ensuring an equivalent level of protection under these Clauses.

8.9 Documentation and compliance

a. The data importer shall be able to demonstrate compliance with these Clauses and shall keep appropriate documentation.

b. The data importer shall make such documentation available to the competent supervisory authority upon request.

Clause 9

Use of sub-processors

a. The data importer has the data exporter's general authorisation for the engagement of sub-processors as listed in **Annex III**. The data importer shall make available to the data exporter an up-to-date list of sub-processors and shall provide notice of any intended changes.

b. Where the data importer engages a sub-processor for carrying out specific processing activities on behalf of the data exporter, it shall conclude a contract with the sub-processor imposing the same data protection obligations as set out in these Clauses.

c. The data importer shall remain fully responsible to the data exporter for the sub-processor's performance.

Clause 10

Data subject rights

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has received instructions to do so from the data exporter.

b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests.

c. In addition, the data importer shall cooperate with the data exporter and follow its instructions to ensure compliance with applicable obligations under data protection law.

Clause 11

Redress

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints.

b. In case of a dispute, the data subject may lodge a complaint with the supervisory authority in the Member State of the data exporter's establishment.

Clause 12

Liability

a. Each Party shall be liable to the other Party for damages it causes by any breach of these Clauses.

b. The data importer shall be liable to the data subject if it fails to comply with these Clauses.

c. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach, all responsible Parties shall be jointly and severally liable.

Clause 13

Supervision

a. Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter shall act as competent supervisory authority.

b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses.

SECTION III — LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

a. The Parties warrant that they have no reason to believe that the laws in the third country of destination applicable to the processing of personal data by the data importer prevent it from fulfilling its obligations under these Clauses.

b. The data importer shall promptly notify the data exporter if, after having agreed to these Clauses, it has reason to believe it is or has become subject to laws that are likely to have a substantial adverse effect on the warranties provided by these Clauses.

c. Following a notification under paragraph (b), the data exporter shall identify appropriate measures to address the situation.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 **Notification**

a. The data importer agrees to notify the data exporter and, where possible, the data subject, if it:

    i. receives a legally binding request from a public authority for the disclosure of personal data; or

    ii. becomes aware of any direct access by public authorities to personal data.

b. If this is prohibited by law, the data importer shall use its best efforts to obtain a waiver of the prohibition, with a view to communicate as much information as possible.

15.2 **Review of legality and minimisation**

a. The data importer shall review the legality of any request for disclosure and challenge the request if it concludes there are grounds to do so.

b. The data importer shall not disclose personal data requested until required to do so under the applicable procedural rules.

SECTION IV — FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

a. Without prejudice to Clauses 14 and 15, if the data importer is in breach of these Clauses, the data exporter may instruct the data importer to suspend processing of personal data until the breach is remedied or the contract is terminated.

b. The data exporter shall be entitled to terminate the contract, insofar as it concerns processing of personal data under these Clauses, where:

    i. the data importer is in substantial or persistent breach of the Clauses; or

    ii. the data importer fails to comply with a binding decision of a competent court or supervisory authority.

c. Personal data shall be deleted or returned to the data exporter upon termination.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established (or, if no EU establishment, by the law of the EU Member State where the representative is located), provided such law allows for third-party beneficiary rights. If not, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights.

Clause 18

Choice of forum and jurisdiction

a. Any dispute arising from these Clauses shall be resolved by the courts of the EU Member State in which the data exporter is established.

b. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which they have their habitual residence.

c. The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

Sellestial

ANNEX I

A. LIST OF PARTIES

1. **Data Exporter**
    a. **Name**: The entity that has entered into the Principal Agreement with Sellestial (Controller)
    b. **Address**: As set forth in the Principal Agreement
    c. **Contact person's name, position, and contact details**: As set forth in the Principal Agreement
    d. **Activities relevant to the data transferred**: As described in the Data Processing Addendum / SaaS Subscription Agreement
2. **Data Importer**
    a. **Name**: Sellestial, Inc.
    b. **Address**: 251 Little Falls Drive, Wilmington, DE 19808, United States
    c. **Contact person's name, position, and contact details**: info@sellestial.com (Attn: Privacy Officer)
    d. **Activities relevant to the data transferred**: Processing on behalf of the data exporter as per the SaaS Subscription Agreement and DPA

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As detailed in **Exhibit A** of the DPA (e.g., Customer's leads, prospects, customers, employees, etc.).

Categories of personal data transferred

As detailed in **Exhibit A** of the DPA (e.g., contact details, CRM data, communications metadata, etc.).

Sensitive data transferred (if applicable)

[Specify if any special categories or sensitive personal data are transferred, or indicate “N/A” if not applicable.]

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)

Continuous/ongoing during the term of the Principal Agreement, as described in the DPA.

Nature of the processing

Hosting, storage, data enrichment, generation of AI-driven outputs, analytics, as detailed in the DPA.

Purpose(s) of the data transfer and further processing

To enable Sellestial to provide the agreed-upon SaaS platform and related services to the data exporter, as set out in the Principal Agreement and the DPA.

The period for which the personal data will be retained

For the duration of the Principal Agreement and as otherwise specified in the DPA.

Competent Supervisory Authority

The competent supervisory authority shall be the authority in the EU Member State (or UK, if applicable) where the data exporter is established or otherwise as specified by the GDPR/UK GDPR.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES

The technical and organisational security measures implemented by the data importer are as described in **Exhibit B** of the DPA (titled "Security Measures") and incorporated herein by reference. These measures include, but are not limited to:

a. Physical and logical access controls

b. Encryption of personal data in transit and at rest

c. Network security measures (firewalls, intrusion detection)

d. Vulnerability management and regular penetration testing

e. Incident response plans

f. Confidentiality and access restriction for personnel

Sellestial

ANNEX III

LIST OF SUB-PROCESSORS *(Module Two)*

Pursuant to Clause 9 of these SCCs, the data importer has the data exporter's general authorisation to engage the sub-processors listed on its online Subprocessor List, which is maintained at the URL specified in Section 5.1 of the DPA and is incorporated herein by reference. These Sub-processors fall into the following categories:

1. **Hosting / CDN Providers**: (e.g., DigitalOcean, Cloudflare, or similar)
2. **AI API Providers**: (e.g., OpenAI, Anthropic Claude, Google Gemini, or similar)
3. **Data Enrichment Providers**: (e.g., LeadMagic, ProApis Inc., BrightData, DataForSEO, PredictLeads, or similar)
4. **Payment Processors**: (e.g., Stripe)
5. **Accounting Software**: (e.g., Xero)
6. **Other Service Providers** as may be updated from time to time in accordance with the DPA.

Additional data-protection assurances

a. **No model training.** Customer Personal Data supplied to, or generated by, the above Sub-processors is not used to train, fine-tune, or otherwise improve any machine-learning model that is made available outside Controller's own tenancy or instance.

b. **Adequate jurisdictions and lawful transfers.** All Processing by the above Sub-processors occurs either (a) within jurisdictions recognized as providing an adequate level of protection (e.g., EEA, UK, Canada, Switzerland) or (b) under a valid cross-border transfer mechanism such as the EU-US Data Privacy Framework, the EU Standard Contractual Clauses, the UK International Data Transfer Addendum, or other equivalent safeguards.

c. **Purpose limitation.** Each Sub-processor processes Customer Personal Data solely as necessary to deliver the contracted services to Controller and for no other purpose, in accordance with the DPA and these SCCs.

Sellestial

Sellestial will update the Sub-processor List in accordance with Section 5 of the DPA and will ensure that any newly engaged Sub-processor is bound by written terms that impose data-protection obligations no less protective than those set out in the DPA and these SCCs.

By accepting or entering into the Principal Agreement that incorporates this DPA by reference, the Parties also agree to be bound by these Standard Contractual Clauses ("SCCs"), which are incorporated herein as Exhibit C.