DATA PROCESSOR AGREEMENT

RECITALS

This Data Processor Agreement including its Schedules ("DPA") forms part and incorporates the terms of the Master Services Agreement or other written or electronic agreement between the Smartstream Technologies entity that is a party to that agreement and the Customer, and reflects the parties' agreement with regard to the Processing of Personal Data. In the event of conflict, this DPA takes precedence with respect to data protection matters.

The parties acknowledge that: (i) the Controller determines the purposes and means of processing Personal Data and is solely responsible for the lawfulness of that processing; (ii) the Processor processes Personal Data solely on behalf of, and under the documented instructions of, the Controller; and (iii) both parties are committed to compliance with applicable data protection law, including the EU GDPR (2016/679), the UK GDPR/DPA 2018, and applicable US state privacy laws including CCPA/CPRA, VCDPA, CPA, and other enacted US state privacy statutes (collectively, "Applicable Laws").

PART 1 — DEFINITIONS

1.1 "Personal Data" means any information relating to an identified or identifiable natural person, as defined under Applicable Laws, including "personal information" as defined under US state privacy laws.
1.2 "Processing" has the meaning given under GDPR Article 4(2) and equivalent definitions under Applicable Laws.
1.3 "Data Subject" means the identified or identifiable individual to whom Personal Data relates.
1.4 "Sub-Processor" means any third party engaged by the Processor to carry out Processing activities on behalf of the Controller.
1.5 "Security Incident" means a confirmed accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data that is reasonably likely to result in a risk to the rights and freedoms of natural persons.
1.6 "Restricted Transfer" means a transfer of Personal Data to a country outside the UK or EEA not deemed to provide an adequate level of protection.
1.7 "SCCs" means the European Commission's standard contractual clauses (Decision 2021/914) and/or the UK International Data Transfer Agreement / Addendum, as applicable.
1.8 "Sensitive Data" means Personal Data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, data concerning sex life or sexual orientation, or government identifiers under applicable US law.
1.9 "Services" means the services provided by the Processor under the Principal Agreement.

PART 2 — SCOPE AND NATURE OF PROCESSING

2.1 Schedule of Processing Activities. The details of Processing are set out in Schedule 1. Processing outside the scope of Schedule 1 is not covered by this DPA.
2.2 Instructions. The Processor shall process Personal Data only: (a) in accordance with the Controller's documented instructions, including those in this DPA and the Principal Agreement; or (b) as required by Applicable Laws, in which case the Processor shall, to the extent permitted by law, inform the Controller before processing.

2.3 Adequacy of Instructions. The Controller is responsible for ensuring its instructions are lawful, complete, and technically feasible. The Processor shall not be liable for any failure directly resulting from inadequate, ambiguous, or unlawful instructions provided by the Controller.
2.4 Notification of Conflicting Instructions. If the Processor reasonably believes an instruction infringes Applicable Laws, it shall promptly notify the Controller. The Processor shall not be required to follow instructions it reasonably and in good faith believes to be unlawful, and shall incur no liability for declining to do so.
2.5 Controller Responsibility. The Controller is solely responsible for: (a) determining the lawful basis for Processing; (b) fulfilling all transparency and notice obligations to Data Subjects; and (c) ensuring that Personal Data provided to the Processor is accurate, adequate, and not excessive.

PART 3 — PROCESSOR OBLIGATIONS

3.1 Confidentiality. The Processor shall ensure that persons authorised to process Personal Data are subject to binding obligations of confidentiality.
3.2 Data Minimisation. The Processor shall process only Personal Data reasonably necessary to perform the Services as described in Schedule 1, and shall not sell or share Personal Data for purposes unrelated to the Services.
3.3 No Sale or Sharing. The Processor shall not: (a) sell Personal Data or share it for cross-context behavioural advertising; (b) use Personal Data for the Processor's own commercial purposes unrelated to the Services.
3.4 Sensitive Data. The Processor shall apply heightened safeguards to Sensitive Data where explicitly authorised in Schedule 1. The Processor shall have no obligation with respect to Sensitive Data inadvertently submitted by the Controller outside the scope of Schedule 1.
3.5 Data Subject Rights Assistance. The Processor shall: (a) forward Data Subject rights requests clearly directed to the Processor to the Controller within **ten (10) business days**; (b) provide reasonable technical assistance to enable the Controller to fulfil Data Subject rights, at the Controller's reasonable expense where such assistance requires material effort beyond the standard Services.
3.6 Controller Assistance. Where required under GDPR Article 28(3)(f), the Processor shall provide reasonable assistance with security, breach notification, DPIAs, and supervisory authority consultations. Such assistance shall be provided at the Controller's cost where it falls outside the scope of the Services.

PART 4 — SECURITY

4.1 Technical and Organisational Measures. The Processor shall implement and maintain appropriate security measures as set out in Schedule 2, appropriate to the risk presented by the Processing.
4.2 Evolving Standards. The Processor may update security measures over time provided the overall level of protection is not materially reduced. The Processor shall notify the Controller of any material reduction with at least **30 days' notice**.
4.3 Controller-Side Security. The Controller is responsible for the security of its own systems, access credentials, and interfaces used to transmit Personal Data to the Processor. The Processor shall not be liable for Security Incidents arising from vulnerabilities or acts or omissions on the Controller's side of the processing environment.
4.4 Security Incident Notification. Upon becoming aware of a confirmed Security Incident affecting the Controller's Personal Data, the Processor shall: (a) notify the Controller without undue delay and **no later than 72 hours** after confirmation; (b) provide, to the extent reasonably available: a description of the incident, categories and approximate number of individuals and records affected, likely

consequences, and measures taken or proposed; (c) cooperate in good faith with the Controller's reasonable requests in connection with any required regulatory notification.
4.5 Notification Threshold. The Processor shall not be obligated to notify the Controller of security events that do not meet the definition of a Security Incident (e.g., unsuccessful access attempts, low-severity alerts), unless requested in writing by the Controller for a defined period.
4.6 Security Costs. The Processor's security obligations are reflected in the fees under the Principal Agreement. Requests for security measures beyond those in Schedule 2 may require additional fees.

PART 5 — SUB-PROCESSING

5.1 General Authorisation. The Controller grants general authorisation for the Processor to engage Sub-Processors listed in Schedule 3 and to replace them with Sub-Processors of equivalent capability.
5.2 New Sub-Processors. The Processor shall notify the Controller at least **14 days** in advance of adding a material new Sub-Processor. The Controller may object on reasonable, documented data protection grounds within **10 days** of notification.
5.3 Objection Resolution. If the Processor cannot accommodate a reasonable objection and the Sub-Processor is essential to delivery of the Services, the Controller's sole remedy shall be to terminate the affected services on **30 days' written notice** without liability for early termination fees attributable to the Sub-Processor change.
5.4 Sub-Processor Obligations. The Processor shall impose data protection obligations on Sub-Processors materially equivalent to those in this DPA, and shall remain liable for Sub-Processors' compliance to the same extent it would be liable if performing the processing directly.
5.5 Infrastructure Providers. The Controller acknowledges that the Processor's use of general infrastructure providers (e.g., cloud hosting, CDN, network services) does not require individual notification, provided such providers are subject to appropriate data protection terms.

PART 6 — INTERNATIONAL DATA TRANSFERS

6.1 Transfers from EU/EEA. Personal Data originating from the EU/EEA shall not be transferred outside the EEA except: (a) to a country subject to an adequacy decision; (b) subject to SCCs (EU Module 2); or (c) under another lawful derogation under GDPR Article 49.
6.2 Transfers from the UK. Transfers of UK Personal Data shall be subject to the UK IDTA or the UK Addendum to the EU SCCs, as applicable.
6.3 Data Privacy Framework. Where the Processor participates in the EU-US or UK Extension to the Data Privacy Framework, it shall maintain current certification.
6.4 Controller Responsibility for Upstream Transfers. The Controller is responsible for ensuring that any transfer of Personal Data to the Processor is itself lawful under Applicable Laws. The Processor's transfer obligations apply from the point of receipt.
6.5 US-to-US Transfers. The Processor shall comply with applicable US state privacy law requirements in respect of interstate transfers of Personal Data.

PART 7 — CONTROLLER OBLIGATIONS

7.1 Lawful Basis. The Controller warrants that it has established and maintains a valid lawful basis for all Processing in Schedule 1, and has provided all required notices to Data Subjects. The Processor shall not be liable for any failure arising from the Controller's inability to establish or maintain a lawful basis.

7.2 Accuracy and Lawfulness of Data. The Controller is solely responsible for the accuracy, completeness, relevance, and lawfulness of Personal Data provided to the Processor.
7.3 Sensitive Data. The Controller shall not submit Sensitive Data to the Processor without prior written agreement and amendment to Schedule 1. The Processor shall have no liability with respect to Sensitive Data submitted in breach of this clause.
7.4 Instructions. The Controller shall provide clear, timely, and documented instructions. Where the Controller fails to provide timely instructions, causing the Processor to make reasonable processing decisions, the Controller shall bear responsibility for those decisions.
7.5 CCPA Compliance. Where CCPA/CPRA applies, the Controller warrants that its privacy notices, opt-out mechanisms, and consumer rights fulfilment obligations are compliant. The Processor's obligations are conditioned on the Controller having met its upstream CCPA/CPRA obligations.
7.6 DPIA. Where a DPIA is required, it is the Controller's obligation to conduct it. The Processor shall provide reasonable assistance upon written request at the Controller's cost.

PART 8 — AUDITS AND RECORDS

8.1 Records of Processing. The Processor shall maintain records of Processing activities as required by GDPR Article 30(2) and equivalent requirements under Applicable Laws.
8.2 Audit Rights. The Processor shall, upon not less than **45 days' written notice**: (a) make available documentation and information reasonably necessary to demonstrate compliance with this DPA; (b) permit an audit by the Controller or an independent auditor, no more than **once per calendar year**, subject to the Processor's reasonable security, confidentiality, and operational requirements.
8.3 Audit Substitution. The Processor may satisfy audit obligations by providing current third-party audit reports (e.g., SOC 2 Type II, ISO 27001 certification, or equivalent). The Controller shall accept such reports as sufficient evidence of compliance unless it identifies a specific, documented gap not addressed by the report.
8.4 Audit Costs. All audit costs, including the Processor's reasonable internal costs in supporting an audit, shall be borne by the Controller.
8.5 Confidentiality of Audit. The Controller shall treat all audit findings and reports as the Processor's confidential information and shall not disclose them to third parties without prior written consent, except as required by law or a supervisory authority.

PART 9 — RETENTION AND DELETION

9.1 Retention Period. The Processor shall retain Personal Data for the period set out in Schedule 1, or for as long as necessary to provide the Services, whichever is shorter.
9.2 Deletion on Termination. Within **60 days** of termination or expiry of the Principal Agreement, or upon written request, the Processor shall, at the Controller's election: (a) securely delete or destroy all Personal Data; or (b) return all Personal Data in a commonly used, machine-readable format at the Controller's reasonable expense where export requires material effort.
9.3 Certification. Upon request, the Processor shall provide written certification of deletion within **30 days** of completion.
9.4 Legal Holds and Backups. The Processor may retain Personal Data beyond the deletion period: (a) where required by Applicable Laws; or (b) in automated backup systems for up to **90 days** following the deletion request, provided such backups are not actively accessed and are subject to secure deletion upon rotation.

PART 10 — LIABILITY

10.1 Liability Cap. Each party's total aggregate liability under this DPA shall not exceed the greater of: (a) the fees paid by the Controller to the Processor in the **twelve (12) months** preceding the event giving rise to the claim; or (b) such other cap as is set out in the Principal Agreement.
10.2 Carve-Outs from Cap. The liability cap in Section 10.2 shall not apply only to liability arising from a party's **fraud or wilful misconduct.**
10.3 Consequential Loss Exclusion. Neither party shall be liable for any indirect, consequential, special, incidental, or punitive damages, including loss of profits, revenue, goodwill, or data, even if advised of the possibility of such damages. This exclusion shall not apply to the extent prohibited by Applicable Laws or arising from fraud or wilful misconduct.
10.4 Regulatory Fines. Each party shall bear sole responsibility for regulatory fines imposed on it as a result of its own non-compliance. The Processor shall not be liable for fines imposed on the Controller arising from the Controller's own obligations as data controller.
10.5 Proportionate Liability. Where a Security Incident or data protection failure is caused or contributed to by both parties, liability shall be apportioned according to each party's respective degree of responsibility.

PART 11 — TERM AND TERMINATION

11.1 Term. This DPA shall be co-terminus with the Principal Agreement.
11.2 Survival. Obligations relating to confidentiality shall survive termination for the same period as set forth for such obligations in the Principal Agreement.
11.3 Breach. Either party may terminate this DPA with immediate effect upon written notice if the other party is in material breach and fails to remedy such breach within **45 days** of written notice (or such longer period as is reasonably necessary, provided the breaching party commences remediation within 14 days and diligently pursues it).
11.4 No Termination for Minor Breach. Immaterial or technical breaches that do not result in harm to Data Subjects or regulatory exposure shall not entitle either party to terminate.

PART 12 — GOVERNING LAW AND DISPUTES

12.1 EU/UK Matters. For Processing subject to GDPR or UK GDPR, this DPA shall be governed by the laws of [England & Wales / Republic of Ireland / Member State of establishment], and the parties submit to the exclusive jurisdiction of the courts of that jurisdiction.
12.2 US Matters. For Processing subject to US state privacy laws, this DPA shall additionally be construed in accordance with applicable US federal and state law.
12.3 Dispute Resolution. The parties shall attempt to resolve any dispute through good-faith senior-level negotiation for **30 days** before initiating formal proceedings.

PART 13 — GENERAL PROVISIONS

13.1 Order of Precedence. (1) mandatory provisions of Applicable Laws prevail; (2) this DPA prevails over the Principal Agreement with respect to data protection; (3) the Principal Agreement governs in all other respects.

13.2 Amendments. This DPA may be amended only by a written instrument signed by authorised representatives of both parties, except that either party may amend this DPA to the minimum extent necessary to comply with changes in Applicable Laws on **30 days' prior written notice**.

13.3 Processor Business Operations. Nothing in this DPA shall prevent the Processor from: (a) processing anonymised or aggregated data that cannot reasonably be re-identified; (b) using usage and performance metadata to improve and maintain the Services, provided such data does not identify individual Data Subjects; or (c) complying with legal obligations imposed on it as an independent data controller.

13.4 Severability. If any provision of this DPA is held invalid or unenforceable, the remaining provisions shall continue in full force and effect.

13.5 Entire Agreement. This DPA, together with its Schedules and the Principal Agreement, constitutes the entire agreement between the parties with respect to the Processing of Personal Data.

Schedule 1 — Processing Details

Element	Details
Subject matter	[e.g., HR data processing / customer support / SaaS platform]
Duration	Co-terminus with Principal Agreement
Nature of Processing	[e.g., storage, analysis, communication, support ticketing]
Purpose of Processing	[e.g., delivery of software services as described in the Principal Agreement]
Categories of Data Subjects	[e.g., employees, customers, end users, prospects]
Categories of Personal Data	[e.g., name, email, IP address, usage data, payment data]
Sensitive Data Authorised?	☐ Yes — specify: _____ ☐ No
Approximate volume	[e.g., up to 50,000 Data Subjects]
Transfer countries involved	[e.g., US, India, Philippines]
Retention period	[e.g., duration of Services + 30 days]

Schedule 2 — Technical and Organisational Security Measures

The Processor confirms it has implemented the following measures (or functional equivalents):

1. Access

Role-based access controls (RBAC) with least-privilege principles; multi-factor authentication (MFA) for privileged and remote access; periodic access reviews and revocation upon role changes or departure.

2. Encryption

Encryption at rest (AES-256 or equivalent); TLS 1.2 or higher for all data in transit; documented key management and rotation procedures.

3. Network Security

Firewalls and intrusion detection/prevention systems; network segmentation for systems holding Personal Data; annual penetration testing (summary results available on request).

4. Incident Response

Documented Incident Response Plan, reviewed annually; security logging and monitoring with alert thresholds; designated security responsibility.

5. Physical Security

Use of reputable third-party data centres with appropriate physical access controls and environmental protections.

Resilience & Continuity

6. Regular automated backups with tested restoration procedures; Business Continuity / Disaster Recovery plan, reviewed annually.

7. Personnel

Annual security awareness training for staff with access to Personal Data; binding confidentiality obligations for relevant personnel.

Schedule 3 — Approved Sub-Processors

Sub-Processor Name	Role	Location	Transfer Mechanism

Schedule 4 — International Transfer Mechanisms

Transfer Route	Mechanism	Reference
EU → US	EU SCCs (Module 2) or EU-US DPF	Commission Decision 2021/914
UK → US	UK IDTA or UK Addendum to SCCs	ICO approved addendum
EU/UK → Other Third Country	SCCs / IDTA / Adequacy Decision	As applicable
US → US (interstate)	Applicable state law compliance	CCPA, VCDPA, CPA, etc.