Human-AI Systems Data Processing Annex

Document: Human-AI Systems Data Processing Annex
Version: 1.0
Effective from: 18 May 2026
Status: Template — invoked only where the relevant SOW expressly states that HAS is engaged to act as a processor of Personal Data on behalf of the Client.

---

1. Status and Scope

1.1 This Data Processing Annex (the **"Annex"**) supplements the Human-AI Systems Master Services Agreement (the **"MSA"**) between Human-AI Systems Limited (**"HAS"**) and the Client. Capitalised terms used in this Annex that are not defined herein have the meanings given to them in the MSA.

1.2 This Annex applies only where the relevant Statement of Work (**"SOW"**) expressly states that the Services include HAS acting as a processor of Personal Data on behalf of the Client. Where this Annex applies, it forms part of the Agreement between the parties and, in the event of conflict between this Annex and the body of the MSA in respect of the processing of Personal Data, this Annex shall prevail.

1.3 The particulars of the processing to which this Annex applies for a given engagement are set out in **Annex A** (Particulars of Processing) to this Annex, which must be completed and agreed for each SOW invoking this Annex.

---

2. Definitions

In this Annex, the following terms have the meanings set out below. Other capitalised terms are as defined in the MSA.

"Applicable Data Protection Law" means the UK GDPR, the Data Protection Act 2018, and any other law applicable to the processing of Personal Data in connection with the Services.

"Controller", **"Processor"**, **"Data Subject"**, **"Personal Data"**, **"Personal Data Breach"**, **"Processing"** (and **"process"**), and **"Special Category Personal Data"** have the meanings given to them in the UK GDPR.

"Sub-processor" means any third party engaged by HAS to process Personal Data on behalf of the Client in connection with the Services.

"TOMs" means the technical and organisational measures set out in **Annex B** (Technical and Organisational Measures).

---

3. Role of the Parties

3.1 The Client is the Controller of the Personal Data processed under the relevant SOW, and HAS is the Processor.

3.2 HAS shall process Personal Data only on the documented instructions of the Client, including the instructions set out in the SOW, in Annex A to this Annex, and in any further written instructions given by the Client from time to time. If HAS reasonably considers that an instruction from the Client infringes Applicable Data Protection Law, HAS shall notify the Client promptly and shall not be obliged to act on the instruction pending resolution.

3.3 Where Applicable Data Protection Law requires HAS to process Personal Data otherwise than on the Client's instructions (for example, to comply with a legal obligation), HAS shall, where lawful, notify the Client of that requirement before processing.

---

4. HAS Obligations as Processor

HAS shall:

(a) **Confidentiality of personnel** — ensure that all personnel and Sub-processors authorised to process the Personal Data are bound by appropriate confidentiality obligations;

(b) **Security** — implement and maintain the TOMs set out in Annex B to ensure a level of security appropriate to the risk, taking into account the state of the art, the nature, scope, context, and purposes of processing, and the risk to the rights and freedoms of natural persons, in accordance with Article 32 of the UK GDPR;

(c) **Sub-processors** — comply with clause 5 of this Annex in respect of any Sub-processors;

(d) **Assistance with Data Subject rights** — taking into account the nature of the processing, assist the Client by appropriate technical and organisational measures, insofar as possible, in fulfilling the Client's obligation to respond to requests from Data Subjects to exercise their rights under Chapter III of the UK GDPR;

(e) **Assistance with controller obligations** — assist the Client in ensuring compliance with the Client's obligations under Articles 32 to 36 of the UK GDPR (security, breach notification, data protection impact assessments, prior consultation), taking into account the nature of the processing and the information available to HAS;

(f) **Personal Data Breach notification** — notify the Client without undue delay, and in any event within seventy-two (72) hours, of HAS becoming aware of any actual or reasonably suspected Personal Data Breach affecting the Client's Personal Data, providing such information as is then available to enable the Client to meet its own notification obligations under Articles 33 and 34 of the UK GDPR;

(g) **Return or deletion** — at the Client's written election, return to the Client or securely delete (and procure that any Sub-processors return or securely delete) all Personal Data processed under the relevant SOW at the end of the provision of Services relating to processing, save for any copy which Applicable Data Protection Law requires HAS to retain (in which case the obligations of this Annex shall continue to apply to that retained copy for so long as it is held); and

(h) **Audit and information** — make available to the Client all information necessary to demonstrate compliance with the obligations set out in this Annex and Article 28 of the UK GDPR, and allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client, in accordance with clause 8 of this Annex.

---

5. Sub-processors

5.1 The Client provides general written authorisation for HAS to engage Sub-processors for the processing of Personal Data, subject to compliance with this clause 5.

5.2 The Sub-processors approved as at the Effective Date of the relevant SOW are listed in **Annex C** (Authorised Sub-processors) to this Annex.

5.3 HAS shall give the Client at least thirty (30) days' prior written notice of any intended addition or replacement of a Sub-processor, during which the Client may object on reasonable grounds related to Applicable Data Protection Law. If the Client objects and the parties cannot resolve the objection in good faith within a further fifteen (15) Business Days, the Client may terminate the affected SOW for convenience under clause 13.2 of the MSA without further notice.

5.4 HAS shall enter into a written agreement with each Sub-processor that imposes obligations no less onerous than those set out in this Annex, in accordance with Article 28(4) of the UK GDPR, and shall remain liable to the Client for the acts and omissions of any Sub-processor as if they were HAS's own.

---

6. International Transfers

6.1 HAS shall not transfer (or permit any Sub-processor to transfer) any Personal Data outside the United Kingdom or the European Economic Area without ensuring that an appropriate transfer mechanism is in place, including (as applicable) the UK International Data Transfer Agreement (UK IDTA), the UK Addendum to the EU Standard Contractual Clauses, or another mechanism recognised under Applicable Data Protection Law.

6.2 The Client authorises HAS to use the UK IDTA, the UK Addendum, or successor mechanisms as the transfer mechanism for any restricted transfer of Personal Data under this Annex, and the Client shall enter into such mechanisms with HAS or any relevant Sub-processor on request to give effect to this clause.

6.3 Where this Annex includes transfers to a Sub-processor located outside the United Kingdom or the European Economic Area, the relevant transfer mechanism shall be set out or referenced in Annex C.

---

7. Personal Data Breach Notification

7.1 The notification given by HAS under clause 4(f) shall include, to the extent then available to HAS:

(a) a description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects affected, and the categories and approximate number of Personal Data records affected;

(b) the likely consequences of the Personal Data Breach;

(c) the measures taken or proposed to be taken by HAS to address the Personal Data Breach and to mitigate its possible adverse effects;

(d) the name and contact details of a HAS point of contact for further information; and

(e) any other information reasonably requested by the Client to enable the Client to meet its obligations under Articles 33 and 34 of the UK GDPR.

7.2 Where it is not possible to provide all of the information in clause 7.1 at the time of the initial notification, HAS shall provide the information in phases as it becomes available without further undue delay.

---

8. Audit Rights

8.1 HAS shall, on no less than thirty (30) days' prior written notice (or such shorter notice as is required by a competent supervisory authority or by the urgency of a Personal Data Breach), permit the Client (or an independent auditor mandated by the Client and reasonably acceptable to HAS) to audit HAS's compliance with this Annex no more than once in any twelve (12) month period, except where a Personal Data Breach or a request from a supervisory authority justifies a more frequent audit.

8.2 Audits shall be conducted during normal business hours, with reasonable advance notice, and in a manner that does not unreasonably interfere with HAS's business operations. The auditor shall sign reasonable confidentiality undertakings before the audit.

8.3 HAS may satisfy the audit obligation by providing the Client with copies of any current independent third-party audit reports (for example, ISO 27001 certifications or SOC 2 reports) covering the relevant processing activities, supplemented by responses to reasonable written questions from the Client, provided that such reports cover the matters the Client would reasonably wish to verify.

8.4 The Client shall bear the costs of any audit it initiates, save where the audit identifies material non-compliance with this Annex, in which case HAS shall reimburse the Client's reasonable audit costs.

9. Liability

9.1 The liability of each party under or in connection with this Annex shall be subject to the limitations and exclusions set out in clause 10 of the MSA, including the sub-cap for data protection liability set out in clause 10.4.

9.2 As between the parties, each party shall bear its own administrative fines imposed on it by a supervisory authority, save to the extent that such fines arise from the other party's breach of its obligations under this Annex or Applicable Data Protection Law, in which case the breaching party shall, subject to clause 9.1, reimburse the non-breaching party for such fines.

---

10. Term and Termination

10.1 This Annex shall remain in force for so long as HAS processes Personal Data on behalf of the Client under any SOW invoking this Annex.

10.2 The obligations in clauses 4 (in respect of confidentiality, breach notification, and return or deletion of Personal Data), 7, 8, and 9 shall survive termination of the Annex or the relevant SOW for so long as HAS retains any Personal Data of the Client.

Annex A — Particulars of Processing

To be completed and agreed for each SOW invoking this Annex.

Item	Particulars
Subject matter of the processing	[Description, e.g. "configuration of the Client's AI assistant solution and provision of ongoing administrative support"]
Duration of the processing	[Duration linked to SOW term, plus any post-termination period needed for return/deletion]
Nature of the processing	[E.g. "collection, organisation, structuring, storage, retrieval, consultation, use, disclosure by transmission, alignment, combination, restriction, erasure, or destruction"]
Purpose of the processing	[Specific purposes, e.g. "to provide the Services described in the SOW dated [X]"]
Categories of Personal Data	[E.g. names, contact details, employment details, system usage logs, etc. List all categories. Do NOT include special category data unless explicitly agreed

Item	Particulars
	and Annex B reviewed.]
Categories of Data Subjects	[E.g. Client's employees, Client's customers, Client's suppliers, etc.]
Special Category Personal Data	[Default: None. If any, list categories and justify lawful basis.]
Frequency of transfer	[Continuous / one-off / periodic — describe.]
Retention period	[How long HAS will retain the Personal Data for the purposes of the Services]
Recipients	[Any third parties to whom HAS will disclose the Personal Data, including Sub-processors per Annex C]

Annex B — Technical and Organisational Measures

Default minimum measures applied by HAS unless varied in the SOW.

Access control

- Multi-factor authentication on all systems used to access Client Personal Data
- Role-based access control on the principle of least privilege
- Periodic review of access rights
- Immediate revocation of access on personnel change or end of engagement

Encryption

- Personal Data at rest in HAS-controlled systems is encrypted using industry-standard encryption (AES-256 or equivalent)
- Personal Data in transit is encrypted using TLS 1.2 or higher

Personnel security

- Confidentiality undertakings in place for all HAS personnel and Sub-processors with access to Personal Data
- Personnel given training on data protection obligations and HAS information security policies

Operational security

- Anti-malware protections on all endpoints used in connection with the Services
- Patch management and vulnerability monitoring on HAS systems
- Logging of access to Personal Data sufficient to support breach detection and audit

Business continuity

- Regular backup of HAS systems holding Personal Data

- Documented procedures for restoration in the event of system failure or breach

Sub-processor management

- Written agreements in place with all Sub-processors imposing equivalent obligations
- Sub-processor list maintained and provided to the Client per Annex C

Incident response

- Documented incident response procedure including detection, containment, eradication, recovery, and notification
- Personal Data Breach notification to the Client within 72 hours of HAS becoming aware

Where an SOW requires additional or alternative measures (for example, ISO 27001 certification, SOC 2 attestation, or specific sector requirements), those measures will be set out in or appended to the SOW and shall apply in addition to or, where expressly stated, in place of the measures above.

Annex C — Authorised Sub-processors

To be completed and agreed for each SOW invoking this Annex. The Client provides general authorisation for the Sub-processors listed below subject to clause 5 of this Annex.

Sub-processor	Address / Jurisdiction	Description of Processing	Transfer Mechanism (if outside UK/EEA)
[Sub-processor name]	[Address / country]	[What they do — e.g. “cloud hosting infrastructure”]	[UK IDTA / UK Addendum / N/A]
[Sub-processor name]	[Address / country]	[Description]	[Mechanism]
[Sub-processor name]	[Address / country]	[Description]	[Mechanism]

Common Sub-processors for HAS engagements may include, by way of illustration: cloud providers (Microsoft Azure, Google Cloud, Amazon Web Services); productivity platforms (Google Workspace, Microsoft 365); communication tools (Slack, Zoom); AI providers (Anthropic, OpenAI). The actual Sub-processors authorised for any engagement must be listed above before this Annex takes effect for that engagement.

Execution

Where this Annex is invoked, it forms part of the Agreement between HAS and the Client and does not require separate signature, provided that the SOW invoking it identifies it by name and version. Where the Client requires the Annex to be signed

separately, the parties may execute a signature page in form reasonably acceptable to both parties for the purpose.

Version Control

Version	Date	Notes
1.0	18 May 2026	First published version

This Annex is the standard form on which Human-AI Systems Limited acts as a processor of Personal Data on behalf of its clients, where the relevant Statement of Work expressly invokes it. Published alongside the HAS Master Services Agreement at https://human-ai-systems.com/legal/.