DATA PROCESSING ADDENDUM

EURYAN Limited | FMEA & 8D Co-Authoring Platform

This Data Processing Addendum ("**DPA**") forms part of, and is incorporated by reference into, the Principal Agreement between EURYAN Limited, a company incorporated in England and Wales with company number 16834496, ("**Provider**"), and the customer entity identified in the Principal Agreement ("**Customer**").

No signature is required. By entering into the Principal Agreement, Customer accepts the version of this DPA published at euryan.com/legal/dpa as at the effective date of the Principal Agreement. A countersigned counterpart is available on request.

Versioning. Provider may publish updated versions. An updated version applies to an existing Customer only from the commencement of that Customer's next renewal term, or earlier by written agreement, except where required to comply with Data Protection Laws or a direction of a Supervisory Authority, in which case it applies on thirty (30) days' written notice.

Referenced documents. Two documents are incorporated into this DPA by reference and form part of it: the Security Overview published at euryan.com/legal/security, and the Subprocessor List published at euryan.com/legal/subprocessors.

---

1. DEFINITIONS

1.1 "Controller", "Processor", "Data Subject", "Personal Data", "Processing", "Personal Data Breach" and "Supervisory Authority" have the meanings given in the Data Protection Laws.

1.2 "**Data Protection Laws**" means the UK GDPR and the Data Protection Act 2018 and, where applicable to the Processing, Regulation (EU) 2016/679 (the "**EU GDPR**") and relevant national implementing laws.

1.3 "**Customer Content**" means all data, records, documents, parameters and materials uploaded to, or generated within, the Services by or on behalf of Customer, including FMEA records, 8D reports, engineering parameters, test data and Outputs.

1.4 "**Customer Personal Data**" means that subset of Customer Content, and any other data, which constitutes Personal Data and which Provider Processes on behalf of Customer under the Principal Agreement. Customer Content is not, of itself, Personal Data.

1.5 "**Principal Agreement**" means the pilot, subscription or other written agreement under which Provider supplies the Services for a fee. It excludes any free case study or proof-of-concept engagement, which is addressed in clause 2.6.

1.6 "**Security Overview**" means the technical and organisational measures published at euryan.com/legal/security. "**Subprocessor List**" means the list published at euryan.com/legal/subprocessors.

1.7 "**Services**" means the FMEA and 8D co-authoring platform supplied under the Principal Agreement. "**Outputs**" means content generated by the Services in response to instructions from an authorised user.

1.8 "**Subprocessor**" means any third party engaged by Provider to Process Customer Personal Data.

1.9 "**SCCs**" means the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914. "**UK Addendum**" means the International Data Transfer Addendum to those clauses, version B1.0, issued under section 119A(1) of the Data Protection Act 2018.

2. SCOPE AND ROLES

2.1 **Roles.** Customer is the Controller of Customer Personal Data (or a Processor acting for an ultimate Controller); Provider is the Processor (or sub-processor).

2.2 **Details.** Schedule 1 sets out the information required by Article 28(3) and serves as Annex I to the SCCs where those clauses apply.

2.3 **Scope limitation.** This DPA governs Personal Data only. All rights and obligations in respect of Customer Content that is not Personal Data — including ownership, confidentiality, permitted use, and any use of Customer Content to develop, validate or improve the Services — are governed exclusively by the Principal Agreement and fall outside this DPA.

2.4 **No model development on Personal Data.** Provider does not use Customer Personal Data to train, tune, validate, benchmark or otherwise develop any machine learning model, whether its own or that of any third party.

2.5 **No independent use.** Provider shall not sell Customer Personal Data, Process it for its own commercial purposes, or disclose it to any third party except as permitted by this DPA or required by law.

2.6 **Free engagements excluded.** This DPA does not apply to any free case study, proof-of-concept or other no-charge engagement. Such engagements are pre-production and are governed by separate data-handling terms. Provider makes no representation that the environment used for them meets the technical and organisational measures in the Security Overview, or the hosting and Subprocessor arrangements described in this DPA.

3. PROCESSING INSTRUCTIONS

3.1 Provider shall Process Customer Personal Data only on documented instructions from Customer, including as to transfers to a third country, unless required otherwise by law to which Provider is subject. The Principal Agreement, this DPA,

and Customer's configuration and use of the Services constitute Customer's complete documented instructions.

3.2 Provider shall inform Customer without undue delay if, in its reasonable opinion, an instruction infringes Data Protection Laws, and may suspend the affected instruction pending resolution.

3.3 Where Provider receives a legally binding request from a public authority for Customer Personal Data, it shall notify Customer promptly unless prohibited by law, challenge the request where there are reasonable grounds, and disclose only the minimum legally required.

4. PROVIDER OBLIGATIONS

4.1 **Confidentiality.** Provider shall ensure that all personnel authorised to Process Customer Personal Data are subject to a binding duty of confidentiality and access such data on a need-to-know basis.

4.2 **Security.** Provider shall implement and maintain the measures set out in the Security Overview, being measures appropriate to the risk under Article 32. Provider may update the Security Overview from time to time provided the overall level of protection is not materially reduced.

4.3 **Data subject rights.** Taking into account the nature of the Processing, Provider shall assist Customer by appropriate technical and organisational measures, insofar as possible, to respond to requests under Chapter III of the UK GDPR and EU GDPR. Provider shall forward to Customer without undue delay any such request received directly, and shall not respond substantively.

4.4 **Wider assistance.** Provider shall provide reasonable assistance to Customer in respect of Articles 32 to 36, including data protection impact assessments and prior consultation, taking into account the nature of the Processing and the information available to Provider. Provider shall maintain the record required by Article 30(2) and make it available on reasonable request.

4.5 **Cost.** Assistance under clauses 4.3 and 4.4 is included in the fees, save where a request is manifestly unfounded, excessive or repetitive, or requires bespoke engineering effort, in which case Provider may charge at its then-current rates having first notified Customer of the estimated charge.

5. SUBPROCESSORS

5.1 **General authorisation.** Customer grants Provider general written authorisation, for the purposes of Article 28(2), to engage the Subprocessors identified in the Subprocessor List.

5.2 **Notice of change.** Provider shall give at least thirty (30) days' prior written notice of the addition or replacement of any Subprocessor. Notice is given by updating the Subprocessor List and issuing a notification to the subscription service

maintained at that page, which Customer is entitled to join, and additionally by email to Customer's nominated contact on written request.

5.3 **Objection.** Customer may object on reasonable data protection grounds by written notice within fifteen (15) days of notice. The parties shall discuss in good faith. Where the objection is unresolved within thirty (30) days, Customer may terminate the affected Services on written notice and receive a pro-rata refund of fees paid in advance for the terminated portion. This is Customer's sole remedy in respect of such an objection.

5.4 **Flow-down.** Provider shall impose on each Subprocessor, by written contract, data protection obligations no less protective than those in this DPA, and remains fully liable for each Subprocessor's performance.

6. INTERNATIONAL TRANSFERS

6.1 Primary application hosting, database operations and backups are located in the European Union (Frankfurt, Germany). Transfers of Customer Personal Data from the United Kingdom to the European Union are made in reliance on the adequacy regulations made under section 17A of the Data Protection Act 2018.

6.2 Provider shall not transfer Customer Personal Data outside the United Kingdom or the EEA except where an adequacy decision or adequacy regulations apply, or where an appropriate safeguard is in place under Schedule 2.

6.3 Provider shall make available its transfer risk assessment on reasonable request.

7. PERSONAL DATA BREACH

7.1 Provider shall notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data.

7.2 The notification shall describe, so far as known, the nature of the breach including the categories and approximate number of Data Subjects and records concerned, the likely consequences, the measures taken or proposed, and a point of contact. Where information is not all available at once it shall be provided in phases without undue further delay.

7.3 Provider shall not notify a Supervisory Authority or any Data Subject on Customer's behalf unless required by law or instructed in writing by Customer. Notification of, or response to, a Personal Data Breach is not an acknowledgement of fault or liability.

8. AUDIT AND INFORMATION RIGHTS

8.1 Provider shall make available to Customer the information reasonably necessary to demonstrate compliance with Article 28 and this DPA, including its then-current certifications, audit reports and penetration test summaries where available, and

shall respond to one reasonable written security questionnaire in any twelve (12) month period.

8.2 Where the information provided under clause 8.1 is insufficient, Customer or an independent auditor appointed by Customer and not a competitor of Provider may audit Provider's Processing, no more than once in any twelve (12) month period save where required by a Supervisory Authority or following a Personal Data Breach, on thirty (30) days' notice, during normal business hours, in a manner that does not disrupt Provider's operations, subject to reasonable confidentiality undertakings, with no access to other customers' data, systems or premises, and at Customer's cost.

9. RETURN AND DELETION

9.1 On expiry or termination of the Principal Agreement, Provider shall, at Customer's written election made within thirty (30) days, delete or return Customer Personal Data. Absent an election, Provider shall delete. Where return is elected, Provider shall make the data available for export in a structured, commonly used, machine-readable format.

9.2 Provider shall delete from live systems within thirty (30) days of the election or expiry of the election period, and from backup media within sixty (60) days thereafter or on expiry of the applicable backup rotation cycle, whichever is earlier. Until deleted, any residual copy remains subject to this DPA. Provider shall certify deletion in writing on request.

9.3 Provider may retain Customer Personal Data where required by law, for the period required only, and shall continue to protect it in accordance with this DPA.

10. LIABILITY AND PRECEDENCE

10.1 Liability under this DPA is subject to the exclusions and limitations in the Principal Agreement and counts towards, and does not increase, the aggregate cap in that agreement. Nothing excludes liability that cannot lawfully be excluded, nor affects Data Subjects' rights.

10.2 In the event of conflict, the SCCs prevail over this DPA, and this DPA prevails over the Principal Agreement, in each case in respect of Personal Data only. Where the Security Overview or Subprocessor List conflicts with the body of this DPA, the body of this DPA prevails.

11. GENERAL

11.1 **Term.** This DPA takes effect on the effective date of the Principal Agreement and continues until the later of termination of that agreement and completion of deletion or return under clause 9. Clauses 4.1, 8, 9, 10 and 11 survive.

11.2 **Severability.** If any provision is held invalid or unenforceable, the remainder continues in full force.

11.3 **Governing law.** This DPA is governed by the laws of England and Wales, and the parties submit to the exclusive jurisdiction of the courts of England and Wales, save where the SCCs require otherwise in respect of the transfers they govern.

SCHEDULE 1 — DETAILS OF PROCESSING

This Schedule constitutes Annex I to the SCCs where those clauses apply. Annex II is populated by the Security Overview and Annex III by the Subprocessor List, each as published at the effective date and as updated in accordance with clauses 4.2 and 5.2.

Part A — Parties

	Data exporter	Data importer
Identity	Customer, as identified in the Principal Agreement	EURYAN Limited, company number 16834496
Role	Controller, or Processor for an ultimate Controller	Processor, or sub-processor
Contact	As stated in the Principal Agreement	info@euryan.com

Part B — Description of processing

Aspect	Detail
Subject matter	Provision of a software-as-a-service platform for co-authoring, reviewing and managing FMEA records and 8D problem-solving reports, using a structured knowledge graph and constrained AI agents.
Nature and purpose	Hosting, storage, structuring, indexing, querying, transmission and display of Customer Personal Data for the sole purpose of providing the Services, together with authentication, access control, audit logging, support and security monitoring.
Duration and frequency	Continuous for the term of the Principal Agreement, plus the period until deletion or return is completed under clause 9.
Categories of Data Subjects	Determined by Customer through its configuration and use of the Services. Typically Customer's employees and contractors in engineering, quality and programme roles, platform administrators, and authorised supply chain personnel.
Categories of Personal Data	Determined by Customer through its configuration and use of the Services. Typically identification and contact data, authentication data, usage and technical data including

Aspect	Detail
	access logs and telemetry, attribution data recording the individual named as author, reviewer, approver or action owner of a record, and support data.
Special category data	None. Customer shall not upload Article 9 or Article 10 data to the Services.
Retention	For the duration of the Principal Agreement and thereafter in accordance with clause 9. Log retention periods are stated in the Security Overview.
Competent supervisory authority	The Information Commissioner's Office (United Kingdom). For Processing subject to the EU GDPR, the lead authority under Article 56, or the authority of the member state in which Customer's EU representative is established.

Exclusion for clarity. Engineering content within the Services — including failure modes, effects, causes, controls, severity, occurrence and detection ratings, risk and action priority values, material and process parameters, and test results — is Customer Content and is not Processed as Personal Data, except to the extent a record contains attribution data as described above.

SCHEDULE 2 — CROSS-BORDER TRANSFERS

1. **Adequacy first.** Where the destination is covered by UK adequacy regulations or an EU adequacy decision, that mechanism applies and no further safeguard is required.
2. **EU transfers.** Where the EU GDPR applies and no adequacy decision covers the transfer, the SCCs are incorporated by reference: Module Two where Customer is a Controller, or Module Three where Customer is a Processor. Clause 7 (docking) applies. Clause 9: Option 2, with the notice period in clause 5.2 of this DPA. Clause 11: the optional independent dispute resolution wording does not apply. Clause 17: governing law is the law of Ireland. Clause 18(b): the courts of Ireland. Annex I is populated by Schedule 1, Annex II by the Security Overview, and Annex III by the Subprocessor List.
3. **UK transfers.** Where the UK GDPR applies and no adequacy regulations cover the transfer, the UK Addendum is incorporated by reference. Table 1 is populated by Schedule 1 Part A; Table 2 by the modules selected in paragraph 2; Table 3 by Schedule 1, the Security Overview and the Subprocessor List. In Table 4, neither party may end the UK Addendum as set out in section 19.
4. **Replacement mechanisms.** If a transfer mechanism above is invalidated, replaced or amended, the parties shall in good faith adopt the replacement or an alternative lawful mechanism without undue delay.

END OF DATA PROCESSING ADDENDUM