# SUPPLIER DATA PROCESSING AGREEMENT

## Endava PLC | February 2025

This DPA is entered into on [Contract date], by and between Endava entity referred to in the supply contract (**Contract**) and the Supplier as stated in the Contract (each a “Party”, collectively the “**Parties”**). This DPA governs the processing of personal data between the Parties, ensuring compliance with applicable data protection laws and regulations, including but not limited to General Data Protection Regulation (**GDPR**), the UK Data Protection Act 2018 and any other relevant privacy laws (“**Data Protection Laws”**). In the event of a conflict, the terms of this DPA and applicable Data Protection Laws shall prevail over any conflicting terms in the Contract.

This DPA sets out the obligation of each Party in their respective roles.
The Parties acknowledge and agree that their roles as Controller, Processor, and sub-processor depend on the nature of the Processing activities as agreed between the Parties in the Contract. Unless otherwise stated in the Contract or this DPA, Endava acts as the Controller and the Supplier as the Processor.

### 1. Definitions

1.1 Unless otherwise stated this DPA, the terms “**Controller**”, “**Processor**”, **“Processing” and “Personal Data**” shall have the meanings ascribed to them under the applicable Data Protection Laws, unless otherwise defined in the Contract.

### 2. Responsibilities of the Parties

2.1 Joint or Independent Controllers

2.1.1 In the event Endava and Supplier act as joint or independent Controllers, each Party shall ensure compliance with Data Protection Laws and obtain and maintain all necessary consents, notices or other lawful basis for Processing Personal Data.

2.2 Supplier as Processor or Sub-Processor

2.2.1 In the event the Supplier acts as a Processor or sub-processor, the Supplier shall:

2.2.1.1 process Personal Data solely as instructed by Endava (and as set out under **Annex A**), unless required by law, in which case the Supplier must notify Endava before Processing (where permissible by law)

2.2.1.2 process Personal Data to the extent necessary to comply with legal obligations;

2.2.1.3 obtain Endava’s prior written consent prior to transferring Personal Data to sub-processors or a third country;

2.2.1.4 notify Endava without undue delay if any instruction from Endava is in breach of Data Protection Laws.

2.2.1.5 ensure that only authorized persons and those subject to confidentiality obligations, no less stringent than those between the Parties, shall process the Personal Data.

2.2.1.6 notify Endava immediately in the event of any Personal Data protection breaches (including security breaches), or of any complaints submitted to any Personal Data supervisory authority.

## 3. Technical and Organizational Measures (TOMs)

3.1.1 The Supplier shall:

3.1.1.1 implement and maintain the TOMs outlined in **Annex B**.

3.1.1.2 apply TOMs at all times in accordance with this DPA and technological advances.

3.1.1.3 undertake to document in writing, including electronically, any changes made to TOMs, without lowering their security level and to inform Endava of any changes, without undue delays.

3.1.1.4 at Endava's request, contribute to Endava's records of Processing activities. The Supplier will provide Endava with any relevant information and documentation.

## 4. Use of Sub-Processors

4.1.1 Supplier shall set out the existing sub-processors in **Annex C**. and notify Endava in writing (email sufficient) of any replacements or additional sub-processors.

4.1.2 Endava has 14 days' receipt of notice to object to new sub-processor. In absence of any opposition, Endava consents to the use of such new sub-processors.

4.1.3 Supplier shall ensure that all sub-processors adhere to the same data protection obligations as those set out in this DPA. If a sub-processor does not comply with the obligations set out in this DPA, Supplier remains fully liable to Endava for breach of compliance with such obligations.

4.1.4 Any Personal Data transfers to third countries made either by Supplier itself or by its sub-processors are subject to Endava's prior written approval.

## 5. Cooperation and Assistance

5.1.1 Supplier will deliver to Endava promptly and without undue delay any data subject requests.

5.1.2 Supplier will assist Endava by all available and reasonable means, as well as by implementing appropriate TOMs, to ensure Endava's adherence to its obligation to respond to any data subject rights requests. Any direct communication between the Supplier and data subject is only permitted with Endava's prior written consent.

5.1.3 Supplier will provide assistance to Endava to ensure Endava's compliance with its legal obligations.

5.1.4 Supplier will support Endava for any data protection impact assessments required by Data Protection Laws and any consultations with relevant supervisory authorities. At Endava's reasonable request, Supplier will provide all necessary and requested information and documentation.

5.1.5 Supplier will inform Endava of any data protection breach within 24 (twenty-four) hours of awareness and shall include the following information:

a) nature of Personal Data breach, type of information disclosed, categories and number of data subjects affected;

b) name and contact details of person(s) responsible for data protection or of another point of contact within their organization;

c) probable consequences of incident; and

d) measures taken or proposed to mitigate and remedy the breach.

5.1.6 Any developments made by the Supplier on its systems used to process Endava's Personal Data will ensure compliance with Data Protection Laws and guidelines, including data protection by design and by default principles.

## 6. Return or deleting Personal Data

6.1.1 On termination of this DPA and at Endava's request, Supplier shall return to Endava all Personal Data (including copies), unless applicable law requires its mandatory storage and Processing.

## 7. Audit rights

7.1 Endava may audit Supplier's compliance with this DPA and its TOMs. At Endava's request, Supplier will make available to Endava any information at its disposal, to prove such compliance with Data Protection Law.

7.2 Audits will be carried out without affecting Supplier's operations and its obligations under this DPA. Endava shall provide no less than 14 days' notice before commencing an audit.

7.3 Endava shall not be required to provide Supplier with a copy of any such audit report, but may provide, at Supplier's request, a summary of their findings.

## 8. Miscellaneous

8.1 The liability of the Parties for breaches of data protection obligations is governed by the Contract.

8.2 The Parties will maintain the confidentiality of this DPA.

8.3 Unless otherwise provided, any amendment to this DPA will be made in writing by its Parties

8.4 This DPA shall terminate in accordance with the terms in the Contract.

8.5 Annexes A, B and C are binding to the Parties and form part of r this DPA.

Endava: [signature] Supplier: [signature]

Date: [Contract date] Date: [Contract date]

Also valid without signature based upon Supplier and Endava confirmatory actions.

## Annex A: Personal Data processed by Processor

**[The Parties shall confirm the categories of Personal Data being processed]**

- Personal Data to be processed by Processor
- Data Subjects
- Nature and purpose of Processing
- Restrictions to Processing

Each Party will appoint one person responsible for overseeing the performance of this DPA.

## Annex B: Processor technical and organizational measures [Art. 32 GDPR] that apply to Supplier

Considering state-of-the-art technology, implementation costs, nature, object and context, Processing purposes as well as variation in probability and severity of the risk to rights and freedoms of individuals, Processor shall implement appropriate technical and organizational measures (**TOM**) to ensure a level of security appropriate to risk.

Special attention shall be paid to the risks associated with Personal Data Processing performed by Processor in the Controller's name and behalf, especially risks related to either destruction, loss, modification or disclosure of Personal Data, or to unauthorized access, either accidentally or illegally, to Personal Data which are transmitted, stored or otherwise processed, in particular if this may lead to material or moral damage.

The Processor will take the following measures in particular (Article 32 GDPR):

I. Measures to ensure Personal Data confidentiality:

1. Secure access systems (access keys) to locations where Personal Data is processed, including stored.

2. Access control for the use of such systems.

4. Measures regarding the pseudonymization of data.

Personal Data will be processed so they can no longer be attributed to a specific data subject without use of additional information. Pseudonymization requires separate storage of this additional information and is subject to technical and organizational measures to prevent unauthorized identification of data subjects.

II. Measures to ensure Personal Data integrity:

1. Measures or control of Personal Data encryption / transmission.

2. Personal Data entry control: Measures to verify and establish whether and by whom personal data have been entered, modified or deleted in / from the Processor Personal Data Processing systems.

II. Measures to ensure availability and resilience of Personal Data

III. Periodic testing and evaluation of TOM effectiveness

IV. Workplace control / organizational measures

V. Measures to limit un-authorized adding of personal data Processing purposes

VI. Personal Data protection at the time of its conception: measures to ensure that Personal Data protection is envisaged from the time of its initial conception, which includes measures to ensure transparency and possibility to intervene on the data, as well as measures to safeguard data subjects' rights.

## Annex C: List of Sub-Processors contracted by Supplier