DATA PROCESSING AGREEMENT

Last updated: 20th March 2026

This Data Processing Agreement (**DPA**) is entered into between **Kernel AI Ltd**, trading as **Primer** (**Primer**, **Processor**, **we**, **us**, or **our**), and the customer entity that has entered into the applicable Terms of Use, order form, master services agreement, or other agreement governing the customer's use of the Services (**Customer**, **Controller**, **you**, or **your**).

This DPA forms part of and is incorporated into the agreement between the parties governing the Customer's use of the Services (the **Main Agreement**).

1. PURPOSE AND SCOPE

1.1 This DPA applies where and to the extent Primer processes Personal Data on behalf of the Customer as a processor in connection with the Services.

1.2 This DPA does not apply to the extent Primer processes Personal Data as an independent controller.

1.3 This DPA sets out the parties' obligations with respect to such processing under Applicable Data Protection Law.

2. DEFINITIONS

In this DPA:

Applicable Data Protection Law means all laws and regulations applicable to the processing of Personal Data under the Main Agreement, including, where applicable, the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003, and, to the extent applicable, the EU GDPR.

Customer Personal Data means Personal Data processed by Primer on behalf of the Customer in connection with the Services.

Data Subject, **Personal Data**, **Personal Data Breach**, **processing**, **processor**, **controller**, and **supervisory authority** have the meanings given to them in Applicable Data Protection Law.

Subprocessor means any third party engaged by Primer to process Customer Personal Data on behalf of the Customer in connection with the Services.

UK GDPR means the UK General Data Protection Regulation as defined in section 3(10) of the Data Protection Act 2018.

Any capitalised terms not defined in this DPA have the meanings given to them in the Main Agreement.

3. ROLES OF THE PARTIES

3.1 The parties acknowledge that, for the processing of Customer Personal Data covered by this DPA, the Customer acts as controller and Primer acts as processor, except where Applicable Data Protection Law requires otherwise.

3.2 The Customer is responsible for complying with its obligations as controller under Applicable Data Protection Law, including ensuring that it has a valid legal basis for the processing and for instructing Primer lawfully.

3.3 Nothing in this DPA relieves either party of its own direct responsibilities and liabilities under Applicable Data Protection Law.

4. DETAILS OF PROCESSING

4.1 The subject matter, duration, nature, and purpose of the processing, and the types of Personal Data and categories of Data Subjects, are described in **Schedule 1** to this DPA.

4.2 The Customer may update Schedule 1 from time to time by written agreement with Primer, or by updating the relevant information in an order form or other written instructions accepted by Primer.

5. PROCESSING INSTRUCTIONS

5.1 Primer will process Customer Personal Data only on the Customer's documented instructions, including with regard to transfers of Customer Personal Data to a third country or an international organisation, unless required to do so by applicable law.

5.2 The Main Agreement, this DPA, the Customer's configuration and use of the Services, and the Customer's written instructions provided through the Services or otherwise in writing, together constitute the Customer's documented instructions to Primer for the processing of Customer Personal Data.

5.3 Primer will inform the Customer if, in Primer's opinion, an instruction infringes Applicable Data Protection Law. Primer is not required to comply with an instruction that it reasonably believes is unlawful.

5.4 If Primer is required by applicable law to process Customer Personal Data other than on the Customer's instructions, Primer will inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

6. CONFIDENTIALITY

Primer will ensure that persons authorised to process Customer Personal Data are subject to obligations of confidentiality or are under an appropriate statutory obligation of confidentiality.

7. SECURITY

7.1 Primer will implement and maintain appropriate technical and organisational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data, taking into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of processing, and the risks to the rights and freedoms of natural persons.

7.2 Without limiting the generality of Section 7.1, Primer will maintain security measures appropriate to the risks presented by the processing undertaken under the Main Agreement.

7.3 The security measures in **Schedule 2** describe Primer's baseline technical and organisational measures as of the effective date of this DPA. Primer may update those measures from time to time, provided that such updates do not materially reduce the overall level of protection for Customer Personal Data.

8. SUBPROCESSING

8.1 The Customer grants Primer general written authorisation to engage Subprocessors in connection with the provision of the Services.

8.2 Primer will make an up-to-date list of Subprocessors available to the Customer upon written request.

8.3 Primer will impose on each Subprocessor, by written contract, data protection obligations that are no less protective of Customer Personal Data than those set out in this DPA, to the extent applicable to the nature of the services provided by that Subprocessor.

8.4 Primer remains responsible for the performance of each Subprocessor's obligations to the extent required by Applicable Data Protection Law.

8.5 Primer may add or replace Subprocessors from time to time. Primer will notify the Customer of any material changes to its Subprocessors at least 14 days before a new Subprocessor begins processing Customer Personal Data, by email, through the Services, or by other reasonable means, except where a shorter period is reasonably necessary for security, legal, or urgent operational reasons, in which case Primer will notify the Customer as soon as reasonably practicable. If the Customer objects on reasonable data protection grounds to a new Subprocessor, the parties will work together in good faith to address the objection. If the parties are unable to resolve the objection within a reasonable period, the Customer may stop using the affected Services or terminate the affected portion of the Services in accordance with the Main Agreement.

9. DATA SUBJECT RIGHTS

Taking into account the nature of the processing, Primer will provide reasonable assistance to the Customer, by appropriate technical and organisational measures where possible, to enable the Customer to respond to requests from Data Subjects exercising their rights under Applicable Data Protection Law.

If Primer receives a request from a Data Subject relating to Customer Personal Data, Primer may, where appropriate, direct the Data Subject to the Customer. Primer will notify the Customer of such request where legally permitted and reasonably practicable.

10. ASSISTANCE TO THE CUSTOMER

Taking into account the nature of the processing and the information available to Primer, Primer will provide reasonable assistance to the Customer with the Customer's compliance obligations under Articles 32 to 36 of the UK GDPR and equivalent provisions of Applicable Data Protection Law, including as relevant in relation to:

1. security of processing;
2. notification of Personal Data Breaches to supervisory authorities or Data Subjects;
3. data protection impact assessments; and
4. prior consultation with a supervisory authority.

11. PERSONAL DATA BREACHES

11.1 Primer will notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data.

11.2 To the extent available, such notification will include information reasonably necessary for the Customer to meet its obligations under Applicable Data Protection Law, including the nature of the breach, the categories and approximate number of Data Subjects affected, the categories and approximate number of Personal Data records affected, and the measures taken or proposed to address the breach.

11.3 Primer may provide the information in phases as it becomes available.

12. AUDITS AND INFORMATION RIGHTS

12.1 Primer will make available to the Customer all information reasonably necessary to demonstrate Primer's compliance with this DPA and Applicable Data Protection Law obligations applicable to processors.

12.2 To the extent such information is not sufficient for the Customer's reasonable compliance needs, Primer will allow for and contribute to audits, including inspections, conducted by the Customer or an independent auditor mandated by the Customer, subject to the following conditions:

(a) the Customer must give reasonable prior written notice;

(b) audits must be conducted during normal business hours and in a manner that minimises disruption to Primer's business;

(c) the Customer and its auditor must comply with Primer's reasonable confidentiality, security, and health and safety requirements;

(d) the Customer may not exercise its audit rights more than once in any 12-month period unless required by a supervisory authority or following a Personal Data Breach affecting Customer Personal Data;

(e) the auditor must not be a competitor of Primer and must be bound by confidentiality obligations no less protective than those in the Main Agreement; and

(f) the Customer will bear its own costs of the audit and reimburse Primer for its reasonable internal costs in responding to audits, except where the audit reveals a material breach of this DPA by Primer.

13. INTERNATIONAL TRANSFERS

13.1 The Customer authorises Primer and its Subprocessors to transfer Customer Personal Data internationally where reasonably necessary to provide the Services, provided that Primer ensures that such transfers are made in accordance with Applicable Data Protection Law.

13.2 To the extent that the processing of Customer Personal Data involves a restricted transfer under Applicable Data Protection Law to a jurisdiction that is not recognised as providing an adequate level of protection, the parties agree that the transfer mechanism set out in **Schedule 3** will apply automatically and is incorporated into this DPA by reference.

13.3 The parties will comply with, and take any actions reasonably necessary to give effect to, the transfer mechanism described in Schedule 3, including providing relevant information and completing any supplementary details reasonably required for the relevant transfer.

13.4 If Primer adopts an alternative lawful transfer mechanism for a restricted transfer, Primer may update Schedule 3 accordingly, provided that the updated mechanism affords a level of protection for Customer Personal Data that is not materially less protective than the mechanism it replaces and is valid under Applicable Data Protection Law.

14. RETURN AND DELETION OF CUSTOMER PERSONAL DATA

14.1 Upon termination or expiry of the Main Agreement, and at the Customer's choice, Primer will either:

(a) make Customer Personal Data available to the Customer for export in a commonly used machine-readable format, if the Customer makes a written request within 30 days after termination or expiry; or

(b) delete Customer Personal Data from Primer's active systems.

14.2 After providing the export requested under Section 14.1(a), or if no request is made within the 30-day period, Primer will delete Customer Personal Data from its active systems within 90 days after termination or expiry, except to the extent retention is required by applicable law.

14.3 Residual copies in backup or disaster-recovery systems will be deleted in accordance with Primer's standard retention schedules and will remain subject to the confidentiality and data-protection obligations of this DPA pending deletion.

15. LIABILITY

15.1 Each party's liability arising out of or in connection with this DPA is subject to the exclusions and limitations of liability set out in the Main Agreement, unless Applicable Data Protection Law requires otherwise.

15.2 Nothing in this DPA excludes or limits either party's liability to the extent such liability cannot lawfully be excluded or limited.

16. GENERAL

16.1 Except as expressly modified by this DPA, the Main Agreement remains in full force and effect.

16.2 In the event of any conflict between this DPA and the Main Agreement with respect to the processing of Customer Personal Data, this DPA will prevail.

16.3 This DPA is governed by the governing law and dispute resolution provisions set out in the Main Agreement, unless Applicable Data Protection Law requires otherwise.

16.4 This DPA may be executed by electronic signature and in counterparts.

SCHEDULE 1 – DETAILS OF PROCESSING

A. Subject Matter of the Processing

Provision of the Services by Primer to the Customer under the Main Agreement.

B. Duration of the Processing

For the duration of the Main Agreement, plus any period during which Customer Personal Data is retained in accordance with the Main Agreement and this DPA.

C. Nature and Purpose of the Processing

Hosting, storage, organisation, retrieval, analysis, generation, transmission, support, security, troubleshooting, and other processing activities necessary to provide and maintain the Services and to comply with the Customer's documented instructions. For the avoidance of doubt, the nature and purpose of processing does not include using Customer Personal Data to train or fine-tune foundational artificial intelligence models made available to other customers.

D. Categories of Data Subjects

Depending on the Customer's use of the Services, Data Subjects may include:

- Customer personnel and authorised users;
- individuals named or referenced in Customer Inputs or related materials;
- contacts, counterparties, or third parties whose Personal Data is included in materials submitted by the Customer; and
- any other individuals whose Personal Data the Customer submits to the Services.

E. Types of Personal Data

Depending on the Customer's use of the Services, Personal Data may include:

- names;
- business contact details;
- job titles and employer details;
- account and authentication data;
- communications content;
- files, prompts, notes, instructions, watchlists, documents, and other materials submitted to the Services;
- metadata relating to use of the Services; and
- any other Personal Data submitted by or on behalf of the Customer.

F. Special Categories of Personal Data

The parties do not intend for the Customer to submit special category Personal Data to the Services unless expressly agreed in writing by Primer.

SCHEDULE 2 – SECURITY MEASURES

Primer will maintain technical and organisational measures appropriate to the risks presented by the processing, which include measures such as:

- access controls and authentication measures designed to limit access to Customer Personal Data to authorised personnel;
- role-based access management where appropriate;
- encryption of data in transit and, where appropriate, at rest;
- logging and monitoring of systems and access events;

- vulnerability management and security patching processes;
- backup and disaster recovery measures;
- incident response processes;
- workforce confidentiality obligations and security awareness measures; and
- vendor and Subprocessor due diligence processes appropriate to the nature of the services provided.

SCHEDULE 3 – INTERNATIONAL TRANSFER MECHANISMS

A. UK Restricted Transfers

Where a restricted transfer of Customer Personal Data is made from the United Kingdom to a country or recipient not recognised under Applicable Data Protection Law as providing an adequate level of protection, the parties agree that the **UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses** issued under section 119A of the Data Protection Act 2018 (the **UK Addendum**) is incorporated into this DPA and applies to that transfer.

For the purposes of the UK Addendum:

1. the version of the Approved EU Standard Contractual Clauses that applies is the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the **EU SCCs**);
2. the relevant module of the EU SCCs will be:
    - **Module Two (Controller to Processor)** where the Customer is transferring Customer Personal Data to Primer as processor; and
    - **Module Three (Processor to Processor)** where Primer transfers Customer Personal Data to a Subprocessor on the Customer's behalf;
3. the parties, contact details, description of the transfer, categories of Data Subjects, types of Personal Data, frequency of the transfer, nature of the processing, purpose of the transfer, retention periods, and technical and organisational measures are as set out in the Main Agreement, this DPA, Schedules 1 and 2, and any relevant order form;
4. for the purposes of the UK Addendum and the EU SCCs, the Customer is the data exporter and Primer is the data importer in relation to transfers from the Customer to Primer, and Primer is the data exporter and the relevant Subprocessor is the data importer in relation to onward transfers by Primer to a Subprocessor on the Customer's behalf; and
5. if and to the extent the UK Addendum requires any election, completion, or specification not otherwise set out in this DPA, the parties will complete it in a manner reasonably necessary to give effect to the transfer.

B. EEA Restricted Transfers

Where a restricted transfer of Customer Personal Data is made from the European Economic Area to a country or recipient not recognised under Applicable Data Protection Law as providing an adequate level of protection, the parties agree that the **EU SCCs** are incorporated into this DPA and apply to that transfer.

For the purposes of the EU SCCs:

1. the relevant module of the EU SCCs will be:
    - **Module Two (Controller to Processor)** where the Customer is transferring Customer Personal Data to Primer as processor; and
    - **Module Three (Processor to Processor)** where Primer transfers Customer Personal Data to a Subprocessor on the Customer's behalf;
2. where applicable, Clause 7 (Docking Clause) of the EU SCCs is deemed to apply;
3. in Clause 9 of the EU SCCs, Option 2 applies, and the time period for prior notice of Subprocessor changes will be the period set out in Section 8.5 of this DPA;
4. in Clause 11 of the EU SCCs, the optional language does not apply;
5. in Clause 17 of the EU SCCs, the governing law is the law of Ireland;
6. in Clause 18(b) of the EU SCCs, the parties submit to the courts of Ireland;
7. for the purposes of Clause 13 of the EU SCCs, the competent supervisory authority will be the supervisory authority of the EEA member state in which the data exporter is established, or, where the data exporter is not established in the EEA, the supervisory authority of the EEA member state in which the data exporter's representative is established;
8. Annex I and Annex II of the EU SCCs are deemed completed with the information set out in the Main Agreement, this DPA, Schedules 1 and 2, and any relevant order form; and
9. for the purposes of the EU SCCs, the Customer is the data exporter and Primer is the data importer in relation to transfers from the Customer to Primer, and Primer is the data exporter and the relevant Subprocessor is the data importer in relation to onward transfers by Primer to a Subprocessor on the Customer's behalf.

C. Conflicts

To the extent of any conflict between this DPA and the UK Addendum and/or the EU SCCs, the UK Addendum and/or the EU SCCs will prevail solely in relation to the relevant restricted transfer.