

Schedule 8

Data Processing Agreement

About this Schedule

The Data Processing Agreement (**DPA**) in this Schedule is specifically incorporated by reference into the Master Services Agreement (**Agreement**) between Customer and Supplier to the extent the Supplier is required to process Personal Data of individuals who reside in the United Kingdom or the European Economic Area.

1. General Terms

- 1.1 This DPA applies to any processing of Personal Data by Supplier in the provision of the Services pursuant to the Agreement where such Personal Data relates to individuals who reside in the United Kingdom or the European Economic Area (**EEA**) and whose Personal Data is in scope of the United Kingdom (**UK**) Data Protection Legislation or European Data Protection Legislation.
- 1.2 Where the Personal Data processed does not relate to individuals who reside in the UK or the EEA, only clauses 1., 2.2(a), 2.2(b), 2.2(c), 2.2(g), 2.3(c), 3, 4 and 5 of this DPA apply to the processing of that Personal Data.
- 1.3 Without prejudice to clause 2.6(d)((v)) and notwithstanding anything to the contrary in the Agreement, in the event of any conflict or inconsistency between the terms of this DPA and the Agreement, the terms of this DPA will prevail.
- 1.4 Words not defined in this DPA will have the definition used in the Agreement. The words **include** or **including** are not words of limitation.

2. Data Protection Terms and Conditions

- 2.1 **Customer's Obligations** – Customer agrees and warrants that Customer's processing of Personal Data, including the transfer to Supplier of the Personal Data, is carried out in accordance with Applicable Data Protection Legislation.
- 2.2 **Supplier's Obligations** – Supplier agrees, represents and warrants:
 - (a) *Following instructions:* that Supplier will process the Personal Data only on behalf of Customer and in accordance with Customer's reasonable written instructions provided from time to time, the terms of the Agreement, this DPA and the Applicable Data Protection Legislation and not for any other purpose at any time. Customer agrees to reimburse Supplier for any reasonable, verifiable and material costs it incurs in complying with any additional instructions provided under this clause 2.2(a) after the date of this DPA which are not specified in this DPA or the Agreement, provided such costs are notified to Customer in writing in advance of being incurred;

- (b) *Security*: that Supplier will, before processing the Personal Data, implement appropriate technical and organisational security measures as required by the Applicable Data Protection Legislation, the Agreement or this DPA as necessary to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of processing. Those measures will include:
- (i) assisting Customer in fulfilling its obligation to respond to requests for exercising the Data Subjects' rights, insofar as this is possible;
 - (ii) ensuring that all employees, or Subcontractors that are engaged in the processing of Personal Data are under a contractual obligation to keep the Personal Data confidential and adhere to the terms of this DPA and the Applicable Data Protection Legislation;
- (c) *Control over Subcontractors*: that Supplier will not disclose Personal Data to any third parties other than to Subcontractors to whom disclosure is necessary in order for Supplier and Subcontractor to carry out the Services agreed to in the Agreement. Any disclosure to Subcontractors will only be made by Supplier on the basis that:
- (i) the Subcontractor is subject to written terms no less onerous than the obligations and standards as those on Supplier under this DPA; and
 - (ii) in the event that a Subcontractor fails to fulfil its data protection obligations under the written agreements with Supplier (as referred to in this DPA) or under the Applicable Data Protection Legislation, Supplier will remain liable to the fullest extent possible to Customer for the performance of Subcontractor's obligations thereunder or under the Applicable Data Protection Legislation;
- (d) *Supplier locations*: that data in respect of the Services will be stored in servers located in Australia;
- (e) *Prompt notice of events (except data breach, as defined in 2.2(g) below)*: that Supplier will promptly and without undue delay (but no later than 48 hours) notify Customer in writing about:
- (i) any legally binding request for disclosure or decryption of the Personal Data by a law enforcement authority including a Requesting Body, unless such notification is prohibited by law in which case, no later than 48 hours after such prohibition is removed;
 - (ii) any request or inquiry received directly from the Data Subjects;

- and
- (iii) any situation arising where the Personal Data will be at risk on the site of Supplier (or Subcontractor) by seizures, insolvency or bankruptcy measures or by any other activities of third parties (in which case, Supplier will inform all third parties in writing that the Personal Data is the sole property of Customer, or Data Subject, as applicable);
 - (f) *Prompt responses to enquiries:* that Supplier will respond promptly to Customer, supervisory authorities or Data Subjects relating to the processing of Personal Data;
 - (g) *Prompt notice of data breach:* without prejudice to clause 2.3(a), that Supplier will notify Customer in writing promptly and without undue delay, after becoming aware of any known or reasonably suspected accidental or unauthorised loss, misuse, destruction, deletion, alteration, disclosure, access, prevention of access, or other compromise, including a penetration of Supplier's or Subcontractor's network or computer resources, that occurs with respect to any Personal Data or any other possible non-compliance with data protection laws including the Applicable Data Protection Legislation (**data breach**). The notification of a data breach will at a minimum specify (in as much detail as is reasonably available) the information required by the Applicable Data Protection Legislation (including Article 33 of the GDPR and UK GDPR (as applicable)) or the information reasonably required by either Customer or a supervisory authority in relation to the data breach from time to time;
 - (h) *Assistance with Customer's obligations:* that Supplier will provide reasonable assistance at no charge to enable Customer to comply with:
 - (i) any obligations it may have in respect of a duty to notify a data breach;
 - (ii) an obligation to maintain documentation of all processing operations under its responsibility;
 - (iii) the provision of overviews of the same;
 - (iv) an obligation to carry out a data impact assessment when required (including any prior consultations with a supervisory authority); and
 - (v) the Applicable Data Protection Legislation; and
 - (i) *Accountability:* that Supplier will assist Customer in ensuring compliance with its own respective obligations in relation to this DPA and Applicable Data Protection Legislation by making available to Customer all information

necessary to demonstrate such compliance.

2.3 Representations and Warranties – Supplier further agrees, represents and warrants:

- (a) if Supplier cannot comply with the DPA or the Applicable Data Protection Legislation for whatever reason, Supplier will inform Customer promptly in writing (but no later than 48 hours) of the specific reasons for its inability to comply, in which case (except when as a result of a change in any applicable law) Customer is entitled to suspend the transfer of data and, for the period of such suspension, receive an appropriate refund for any amounts paid to Supplier during such period;
- (b) that Supplier has no knowledge of or reason to believe that any law applicable to it (including the Applicable Data Protection Legislation) prevents it from fulfilling the instructions received from Customer and the obligations under this DPA and the Applicable Data Protection Legislation. In the event of a change in any applicable law that is likely to have a substantial adverse effect on Supplier's compliance with the representations, warranties and obligations provided under this DPA or the Applicable Data Protection Legislation, Supplier will, without prejudice to its other obligations, notify Customer in writing of the change as soon as it

is aware, in which case Customer is entitled to suspend the transfer of data and receive an appropriate refund of any amounts paid to Supplier during such period;

- (c) that Supplier has put in place technical and organisational measures necessary, including as described in clause 2.2(b), to ensure a level of security appropriate to the risks presented by the processing (including transfer) and the nature, scope and context of the Personal Data to be protected having regard to the state of the art, applicable industry standards and the cost of their implementation;
- (d) where Personal Data is subject to a transfer under clause 2.6, to confirm if requested by Customer (which request can be made once every 12 months as from the Effective Date) that, to the best of its knowledge, no order to disclose or decrypt Personal Data (which is subject to the terms of this DPA) by a Requesting Body has been received by Supplier or any of its Subcontractors; and
- (e) save to the extent prohibited by applicable law, that it will conduct a satisfactory background check with respect to each employee, contractor, agent, affiliate, subcontractor (and any entity under the direction or control of Supplier or subcontractors) who processes or could process Personal Data. In the case of any Subcontractor or entity under the

direction or control of Supplier or Subcontractor, requiring such entity to conduct satisfactory background checks on anyone who provides services related to Supplier's provision of the Services to Customer. For the purposes of this clause, satisfactory background checks will include as a minimum (modified as appropriate under applicable laws to the extent necessary to ensure maximum coverage of the foregoing requirements, or waived where it is not permitted under applicable laws), the following requirements: (i) criminal history check over the 10 year period prior to the date such employee or contractor commences its engagement with the Supplier or Subcontractor; and (ii) verification of eligibility to lawfully work in the applicable country.

2.4 Supplier Indemnity and Limitations of Liability

- (a) Subject to clause 2.4(b), Supplier will indemnify and hold harmless and keep Customer indemnified and reimburse Customer for all damages, losses, judgments, settlements, liabilities, costs or expenses incurred by Customer in respect of any breach of this DPA or the Applicable Data Protection Legislation by Supplier or its Subcontractors.
- (b) Notwithstanding anything to the contrary in the Agreement or this DPA, Supplier's indemnification obligation hereunder and any

claims for damages by Customer against Supplier for a breach of this DPA or the Applicable Data Protection Legislation by Supplier or Subcontractor or any third party under the direction or control of Supplier will be limited in aggregate to the amount of fees paid to Supplier under the Agreement in the preceding 12 months.

- 2.5 **Termination obligations** – the Parties agree that on the termination or expiry of the Agreement, Supplier will promptly (but no later than 30 business days after such termination), at the choice of Customer, (i) return all Personal Data in its possession or under its control and the copies thereof to Customer; or (ii) destroy all the Personal Data and provide certification in writing by a duly authorised executive of Supplier to Customer that it has done so without retaining any copies, unless applicable law prevents Supplier from doing so, in which case Supplier represents, warrants and agrees that it will guarantee the confidentiality and security of the Personal Data retained in accordance with this DPA and all applicable laws including the Applicable Data Protection Legislation and will not process the Personal Data in its possession thereafter for any other purpose.

2.6 Data transfers

- (a) This clause 2.6 applies to Personal Data which has been transferred:
 - (i) from the Data Exporter subject to GDPR which is only permitted in

accordance with European Data Protection Legislation if a Transfer Solution is applicable to that transfer (**EEA Restricted Transfer**); or (ii) from the Data Exporter subject to UK GDPR which is only permitted in accordance with the UK Data Protection Legislation if a Transfer Solution is applicable to that transfer (**UK Restricted Transfer**). For the avoidance of doubt, clauses 2.6, Annexure 1 and Annexure 2 do not apply to Personal Data which is transferred to a country which has been declared as offering an adequate level of protection through a European Commission decision (**Adequacy Decision**).

- (b) Where an EEA Restricted Transfer is made, the Parties will:
- (i) to the extent that the Data Exporter is processing the Personal Data in its capacity as a controller and the Data Importer is processing the Personal Data in its capacity as a processor, comply with the Controller to Processor module of the Standard Contractual Clauses (which are hereby incorporated into this DPA, as amended by Annexure 1); and
 - (ii) to the extent that each of the Data Exporter and Data Importer is processing the Personal Data in its capacity as a processor, comply with the Processor to Processor module of the Standard Contractual Clauses (which are hereby
- incorporated into this DPA, as amended by Annexure 1).
- (c) Where a UK Restricted Transfer is made, the Parties will comply with the UK International Data Transfer Addendum (which is hereby incorporated into this DPA, as amended by Annexure 2);
- (d) In addition, Supplier represents, warrants and agrees:
- (i) without prejudice to the other obligations imposed on Supplier under this clause 2.6, that the Standard Contractual Clauses apply to Supplier in respect of its processing of Personal Data except that the contents of the annexures to the Standard Contractual Clauses will be replaced by the relevant information in this DPA including in clause 3, and are deemed executed by the Parties upon execution of the Agreement;
 - (ii) to use reasonable endeavours to comply with any specific requirements identified by Customer in respect of a transfer under clause 2.6(a), which requirements are designed to comply with any written guidance and/or recommendations issued by supervisory authorities in the EEA and/or the UK, including the European Data Protection Board, in respect of the decision of the Court of Justice of the European Union known as Schrems II (Case C-311/18);

- (iii) where access to Personal Data of Data Subjects has been granted as described in clause 2.2(e)(i), to cooperate with the Customer in order to provide reasonable assistance to such Data Subjects (upon their written request) in exercising their rights under the laws of the country of establishment of Supplier, to the extent any access by a Requesting Body has failed to comply with the laws applicable in the country of establishment of Supplier and/or the country of residence of the Data Subject.
- (iv) that rights and benefits under this clause 2.6 may be enforced by any Data Subject whose Personal Data is processed pursuant to this clause 2.6; and
- (v) notwithstanding any provision to the contrary, in the event of any conflict, inconsistency, or incongruity, between the terms of this DPA or the Agreement, and the Standard Contractual Clauses, the terms of the applicable Standard Contractual Clauses will, in all respects and at all times, prevail without any exception or modification (save in respect of the UK Addendum, which will take precedence over the Standard Contractual Clauses in respect of transfers from the UK).

3. **Scope of data processing**

- 3.1 **Scope** – the scope, manner (including potential onward transfers) and purpose of the collection, processing and use of the Personal Data are:
- (a) *Data Exporter*: The Customer who has appointed Supplier as its outsourced service provider (**Data Exporter**). In providing the Services, Supplier may process Personal Data as outlined below.
 - (b) *Data Importer*: The Supplier who may, where appropriate, provide the following activities which are relevant to the transfer of Personal Data (**Data Importer**):
 - (i) Triggering an invitation to use the Kinatico Compliance User App, including inviting the data subject to register, create an account, and accept relevant Kinatico Compliance User app terms of use;
 - (ii) Asking the Data Subject to respond to a request from the Customer, where the Data Subject has been asked to request verification services from Supplier and share a copy of relevant results with the Customer;
 - (iii) Data Subject support, where Supplier will view Personal Data when providing support or assistance to the Data Subject in respect of the above;
 - (iv) Facilitating and reporting on Requirement completion by workers, to enable reporting, monitoring and management

of Customer's workforce compliance.

3.2 **Subject matter, nature and purpose of the processing** – where applicable, the Personal Data transferred may be subject to the following basic processing activities:

- (a) Personal Data that will be processed by Supplier's systems and personnel when providing Services in accordance with the Agreement; and
- (b) Personal data of Data Subjects who are contacting Supplier for support or to resolve application related issues, and where Supplier will view unstructured Personal Data while providing the support.

3.3 **Categories** – the categories of Personal Data and categories of Data Subjects whose data is processed under this DPA are:

- (a) *Categories of data*: names and email addresses of Data Subjects.
- (b) *Data Subjects*: the Personal Data transferred may concern the following categories of Data Subjects, which may arise out of prospective, or existing relationships between Customer and:
 - (i) partners, employees or other workers; or
 - (ii) advisors, consultants or other professional experts.

3.4 **Duration** – the duration of the processing is the term of this DPA, unless otherwise indicated. The maximum data retention period of the

Personal Data transferred is as indicated by Customer through its instructions described in clause 2.2(a).

3.5 The Parties agree and acknowledge that where they are required to make any choices or specify any timeframes with respect to any of the provisions of the Standard Contractual Clauses, such choices and specifications are set out in Annexure 1 of this DPA.

4. Information Security

4.1 In supplying the Services, Supplier will comply with its policies relating to information security as outlined in the Agreement.

4.2 Supplier agrees maintain its compliance to ISO 27001, including annual audit by authorised independent auditors. Compliance will require maintenance of the following technical measures in the course of supplying the Services:

- (a) maintenance of access request records and logs of access activities for a minimum of six months for all systems that store, access, process and transmit confidential data, including Personal Data;
- (b) encryption of Personal Data in transit (including electronic transmission and transportation between physical locations) using at least TLS 1.2 encryption standard; and
- (c) encryption of Personal Data at rest (including when stored on devices, servers, or portable electronic media, and in backups or

archives) using, at a minimum, AES-256 encryption standard.

5. Definitions

For the purposes of this DPA, all terms:

- (a) defined in the Agreement bear the same meaning in this DPA, unless the context otherwise requires; and
- (b) defined in Applicable Data Protection Legislation bear a corresponding similar meaning for similar concepts in such Applicable Data Protection Legislation, and for the avoidance of doubt “personal data” will include “personal information” as defined in the *Privacy Act 1988* (C’t’h) and Personal Data.

Furthermore, for the purposes of this DPA:

Agreement means the Master Services Agreement between Customer and Supplier for the Services, and to which this DPA is a Schedule and forms part.

Applicable Data Protection Legislation means, to the extent Customer or any Personal Data is subject to such legislation, the European Data Protection Legislation, the UK Data Protection Legislation, the New Zealand Privacy Act 2020 and any other laws, provisions, directives, guidance or regulations affecting privacy, personal data or artificial intelligence and any updated, additional, modified or replacement laws, provisions, directives, guidance or regulations relating to the same subject matter, in each case as may be promulgated after the effective date of this DPA (regardless of whether such legislation applies directly to Supplier).

Data Exporter and **Data Importer** is defined in clause 3.1 above.

Data Subject is a Worker under the Agreement.

DPA means this data processing agreement between the Customer and the Supplier, comprising this schedule including annexures.

EEA means the European Economic Area.

European Data Protection Legislation means, to the extent Customer or any personal data is subject to such legislation, the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**GDPR**) and any national laws implementing or supplementing the same and any updated, additional, modified or replacement laws, provisions, directives, guidance or regulations relating to the same subject matter as the GDPR, in each case as may be promulgated after the effective date of this DPA (regardless of whether such legislation applies directly to Supplier).

Personal Data means personal data created or processed as part of, or in connection with, the Services agreed to in the Agreement or provided by Customer (or any third party on its behalf) to Supplier (or any of its agents, affiliates, sub-contractors or Subcontractors) in connection with the Agreement.

Requesting Body means a non-EEA established law enforcement authority or state security body accessing or requesting access or decryption of personal data transferred pursuant to clause 2.6(a).

Standard Contractual Clauses (SCCs) means the Controller to Processor module, or the Processor to Processor module of the

Standard Contractual Clauses, (as applicable) for the transfer of personal data from a Data Exporter to a Data Importer which are approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as amended in Annexure 1 of this DPA.

Subcontractor means any affiliate, parent, subsidiary or any third party under the direction or control of Supplier including the contractors, agents and subcontractors of Supplier.

Transfer Solution means the Standard Contractual Clauses or any other safeguards under the Applicable Data Protection Legislation applicable to a relevant transfer of personal data that has the effect of permitting that transfer in accordance with such Applicable Data Protection Legislation. For the avoidance of doubt, a Transfer Solution is not required in relation to the transfer of personal data to a country which has been declared as offering an adequate level of protection through an Adequacy Decision.

UK Data Protection Legislation means, to the extent Customer or any personal data is

subject to such legislation, all laws, relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR, the UK Data Protection Act 2018, and any provisions, directives, guidance or regulations relating to these, in each case as may be promulgated after the effective date of this DPA (regardless of whether such legislation applies directly to Supplier).

UK GDPR means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

UK International Data Transfer Addendum means the addendum to the Standard Contractual Clauses issued under SI19A9(1) of the United Kingdom's Data Protection Act 2018, as amended in Annexure 2 of this DPA.

Annexure 1 – Standard Contractual Clauses

Standard Contractual Clauses:

The Parties' choices with respect to various clauses of the Standard Contractual Clauses are as follows:

- For the purposes of clause 17 of the Standard Contractual Clauses, the Parties agree that the governing law will be the law of the Republic of Ireland;
- For the purposes of clause 18 paragraph (b) of the Standard Contractual Clauses, the Parties agree that any dispute arising from the Standard Contractual Clauses will be resolved by the courts of the Republic of Ireland.

Optional clauses:

- For the purposes of clause 9 paragraph (a) of the Standard Contractual Clauses, the Parties agree to select Option 2 of clause 9 (a) of the Standard Contractual Clauses;
- For the purposes of clause 9 paragraph (a) of the Standard Contractual Clauses, the Parties specify the time period as follows: 21 business days;
- For the purposes of clause 11 of the Standard Contractual Clauses, the Parties agree that the optional clause under clause 11 (a) of the Standard Contractual Clauses will not apply;
- For the purposes of clause 13 paragraph (a) of the Standard Contractual Clauses, the competent Supervisory Authority will be the competent Supervisory Authority that has supervision over the relevant Data Exporter;
- For the purposes of clause 17 of the Standard Contractual Clauses, the Parties agree to select Option 1 of clause 17 of the Standard Contractual Clauses.

Annexure 2 – UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

1. In relation to transfers of Personal Data protected by UK GDPR, the Standard Contractual Clauses:
 - apply as completed in accordance with Annexure 1 above; and
 - are deemed amended as specified by the UK International Data Transfer Addendum, which is deemed executed by the parties and incorporated into and forming an integral part of this DPA.
2. In addition:
 - Table 1 is deemed completed respectively with the Customer details (as Data Exporter) and Supplier details (as Data Importer) as set out in the Agreement.
 - Table 2 is deemed completed by selecting "the Approved EU SCCs".
 - Table 3 is deemed completed with the information contained in the Agreement (as to list of parties) and clause 3, clause 4 and Annexure 1 of this DPA.

- Table 4 is deemed completed by selecting both “importer” and “exporter”.
- Any conflict between the terms of the Standard Contractual Clauses and the UK International Data Transfer Addendum will be resolved in accordance with section 10 and section 11 of the UK International Data Transfer Addendum.

Version history

This is version 2.0 of this Schedule.

Version	Approved	Effective	Notes
1.0	16/06/2025	16/06/2025	First version published
2.0	16/09/2026	13/10/2026	Changes in nomenclature