Data Protection Addendum

This current consolidated Acceptable Use Policy was published on 1 June 2026.

1 DEFINITIONS

1.1 In this Data Protection Addendum defined terms shall have the same meaning, and the same rules of interpretation shall apply as in the remainder of our Agreement. In addition, in this Data Protection Addendum the following definitions have the meanings given below:

Controller has the meaning given to that term in Data Protection Laws;

Data Protection Laws means, as applicable to either party or the Services: (a) the EU GDPR; (b) the UK GDPR and the UK DPA 2018; (c) any laws which implement or supplement any such laws; and (d) any laws that replace, extend, re-enact, consolidate or amend any of the foregoing;

Data Protection Losses means all liabilities arising directly or indirectly from any breach or alleged breach of any of the Data Protection Laws or of this Data Protection Addendum, including all: (a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); (b) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; (c) compensation which is ordered by a court or Supervisory Authority to be paid to a Data Subject; and/or (d) costs of compliance with investigations by a Supervisory Authority;

Data Subject has the meaning given to that term in Data Protection Laws;

Data Subject Request means a request made by a Data Subject to exercise any rights of Data Subjects under Chapter III of the GDPR in relation to any Protected Data;

EEA Data Protection Laws means Data Protection Laws applicable under the laws of the European Economic Area, the European Union or any of their member states;

EEA Protected Data means Protected Data to which any EEA Data Protection Laws apply;

EU GDPR means the General Data Protection Regulation, Regulation (EU) 2016/679;

GDPR means the EU GDPR and the UK GDPR (as applicable in the circumstances);

International Recipient means the organisations, bodies, persons and other recipients to which Transfers of the Protected Data are prohibited under paragraph 7.1 without the Customer's prior written authorisation;

Lawful Safeguards means such legally enforceable mechanism(s) for Transfers of Personal Data as may be permitted under Data Protection Laws from time to time;

List of Sub-Processors means the latest version of the list of Sub-Processors, if applicable, used by the Supplier, as Updated from time to time, and provided to the Customer on request;

Personal Data has the meaning given to that term in Data Protection Laws;

Personal Data Breach means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;

Processing has the meaning given to that term in Data Protection Laws (and related terms such as process, processes and processed have corresponding meanings);

Processing Instructions has the meaning given to that term in paragraph 3.1.1;

Processor has the meaning given to that term in Data Protection Laws;

Protected Data means Personal Data in the Customer Data;

Relevant Law means: (a) in respect of EEA Protected Data, all applicable law(s) of the European Economic Area and European Union and of the relevant member state(s) of either; and (b) in respect of UK Protected Data, all applicable law(s) of the United Kingdom (or of any part of the United Kingdom);

Sub-Processor means a Processor engaged by the Supplier or by any other Sub-Processor for carrying out processing activities in respect of the Protected Data on behalf of the Customer;

Supervisory Authority means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;

Transfer bears the same meaning as the word 'transfer' in Article 44 of the GDPR (and related terms such as Transfers, Transferred and Transferring have corresponding meanings);

UK Data Protection Laws means the Data Protection Laws applicable under the laws of the United Kingdom (or of any part of the United Kingdom), including the UK GDPR and UK DPA 2018;

UK DPA 2018 means the United Kingdom's Data Protection Act 2018;

UK GDPR has the meaning given to that term in the UK DPA 2018; and

UK Protected Data means Protected Data to which any UK Data Protection Laws apply.

2 PROCESSOR AND CONTROLLER

2.1 The parties agree that, for the Protected Data, the Customer shall be the Controller and the Supplier shall be the Processor. Nothing in our Agreement relieves the Customer of any responsibilities or liabilities under any Data Protection Laws.

2.2 To the extent the Customer is not sole Controller of any Protected Data it warrants that it has full authority and authorisation of all relevant Controllers to instruct the Supplier to process the Protected Data in accordance with our Agreement.

2.3 The Supplier shall process Protected Data in compliance with:

2.3.1 the obligations of Processors under Data Protection Laws in respect of the performance of its obligations under our Agreement; and

2.3.2 the terms of our Agreement.

2.4 The Customer shall ensure that it, its Affiliates and each Authorised User shall at all times comply with:

2.4.1 all Data Protection Laws in connection with the processing of Protected Data, the use of the Services (and each part) and the exercise and performance of its respective rights and obligations under our Agreement, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and

2.4.2 the terms of our Agreement.

2.5 The Customer warrants, represents and undertakes, that at all times:

2.5.1 the processing of all Protected Data (if processed in accordance with our Agreement) shall comply in all respects with all Data Protection Laws, including in terms of its collection, use and storage;

2.5.2 fair processing and all other appropriate notices have been provided to the Data Subjects of the Protected Data (and all necessary consents from such Data Subjects obtained and at all times maintained) to the extent required by all Data Protection Laws in connection with all processing activities in respect of the Protected Data that may be undertaken by the Supplier and its Sub-Processors in accordance with our Agreement;

2.5.3 the Protected Data is accurate and up to date;

2.5.4 except to the extent resulting from Transfers to International Recipients made by the Supplier or any Sub-Processor, the Protected Data is not subject to the laws of any jurisdiction outside of the United Kingdom and European Economic Area;

2.5.5 it shall establish and maintain adequate security measures to safeguard the Protected Data in its possession or control (including from unauthorised or unlawful destruction, corruption, processing or disclosure) and maintain complete and accurate backups of all Protected Data provided to the Supplier (or anyone acting on its behalf) so as to be able to immediately recover and reconstitute such Protected Data in the event of loss, damage or corruption of such Protected Data by the Supplier or any other person;

2.5.6 all instructions given by it to the Supplier in respect of Personal Data shall at all times be in accordance with Data Protection Laws; and

2.5.7 it has undertaken due diligence in relation to the Supplier's processing operations and commitments and it is satisfied (and at all times it continues to use the Services remains satisfied) that:

(a) the Supplier's processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage the Supplier to process the Protected Data;

(b) the technical and organisational measures set out in the Information Security Addendum and our Agreement (each as Updated from time to time) shall (if the Supplier complies with its obligations under such policy and our Agreement) ensure a level of security appropriate to the risk in regards to the Protected Data as required by Data Protection Laws; and

(c) the Supplier has sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws.

2.6 If the Supplier is subject to any applicable laws at any time that conflict with any of its obligations under this Data Protection Addendum it may immediately terminate our Agreement by notice unless the conflict has been resolved to the Supplier's satisfaction prior to such notice of termination.

3 INSTRUCTIONS AND DETAILS OF PROCESSING

3.1 Insofar as the Supplier processes Protected Data on behalf of the Customer, the Supplier:

3.1.1 unless required to do otherwise by Relevant Law, shall (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Customer's documented instructions as set out in our Agreement (including with regard to Transfers of Protected Data to any International Recipient), as Updated from time to time (Processing Instructions);

3.1.2 if Relevant Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Customer of any such requirement before processing the Protected Data (unless Relevant Law prohibits such information on important grounds of public interest); and

3.1.3 shall promptly inform the Customer if the Supplier becomes aware of a Processing Instruction that, in the Supplier's opinion, infringes Data Protection Laws, provided that: (a) this shall be without prejudice to paragraphs 2.4 and 2.5; and (b) to the maximum extent permitted by applicable law, the Supplier shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any processing in accordance with the Processing Instructions following the Customer's receipt of the information required by this paragraph 3.1.3.

3.2 The Customer agrees that:

3.2.1 the Supplier (and each Sub-Processor) is not obliged to undertake any processing of Protected Data that the Supplier believes infringes any of the Data Protection Laws and shall not be liable (or subject to any reduction or set-off of any Fees otherwise payable to the Supplier) to the extent that it (or any Sub-Processor) is delayed in or fails to perform any obligation under our Agreement as a result of not undertaking any processing in such circumstances; and

3.2.2 without prejudice to any other right or remedy of the Supplier, in the event the Customer has not resolved any Processing Instruction notified to it under paragraph 3.1.3 such that it is lawful in the Supplier's opinion within 5 Business Days of such notification then such circumstances are a material breach of our Agreement by the Customer that cannot be remedied and the Supplier may terminate our Agreement in accordance with its terms.

3.3 The Customer shall be responsible for ensuring all Authorised Affiliates and Authorised Users read and understand the Privacy Policy (as Updated from time to time).

3.4 The Customer acknowledges and agrees that the execution of any computer command to process (including deletion of) any Protected Data made in the use of any of the Subscribed Services by an Authorised User will be a Processing Instruction (other than to the extent such command is not fulfilled due to technical, operational or other reasons, including as set out in the User Manual). The Customer shall ensure that Authorised Users do not execute any such command unless authorised by the Customer (and by all other relevant Controller(s)) and acknowledges and accepts that if any Protected Data is deleted pursuant to any such command the Supplier is under no obligation to seek to restore it.

3.5 Subject to applicable Subscribed Service Specific Terms or the Order Form the processing of the Protected Data by the Supplier under our Agreement shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in the schedule to this Addendum.

4 TECHNICAL AND ORGANISATIONAL MEASURES

4.1 The Supplier shall implement and maintain technical and organisational measures:

4.1.1 in relation to the processing of Protected Data by the Supplier, as set out in the Information Security Addendum; and

4.1.2 to assist the Customer insofar as is possible (taking into account the nature of the processing) in the fulfilment of the Customer's obligations to respond to Data Subject Requests relating to Protected Data, in each case at the Customer's cost on a time and materials basis in accordance with the Supplier's Standard Pricing Terms. The parties have agreed that (taking into account the nature of the processing) the Supplier's compliance with paragraph 6.1 shall constitute the Supplier's sole obligations under this paragraph 4.1.2.

4.2 During the period in which the Supplier processes any Protected Data, the Customer shall regularly undertake a documented assessment of whether the security measures implemented in accordance with paragraph 4.1 are sufficient to protect the Protected Data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access to the extent required by Data Protection Laws in the circumstances. The Customer shall promptly notify the Supplier of full details of any additional measures the Customer believes are required as a result of the assessment. The Customer acknowledges that the Supplier provides a commoditised one-to-many service and the needs or assessments of other customers may differ. The Supplier shall not be obliged to implement any further or alternative security measures, but this is without prejudice to the Customer's right to terminate our Agreement for convenience in accordance with the express provisions of our Agreement if it concludes the measures adopted by the Supplier are no longer sufficient for its needs.

5 USING STAFF AND OTHER PROCESSORS

5.1 Subject to paragraph 5.2, the Supplier shall not engage (nor permit any other Sub-Processor to engage) any Sub-Processor for carrying out any processing activities in respect of the Protected Data in connection with our Agreement without the Customer's prior written authorisation. The Customer shall not unreasonably object to any new Sub-Processor (or any change to any of the Sub-Processors).

5.2 The Customer:

5.2.1 authorises the appointment of any Sub-Processors identified on the List of Sub-Processors as at Order Acceptance; and

5.2.2 authorises the appointment of each Sub-Processor (or any change to any of the Sub-Processors) identified on the List of Sub-Processors as Updated from time to time. The Customer's right to object to the appointment of a new Sub-Processor (or any change to any of the Sub-Processors) following the relevant Update Notice introducing that change may be exclusively exercised by terminating our Agreement in accordance with its rights following the Update Notification introducing the change before that Update takes effect in accordance with our Agreement.

5.3 The Supplier shall:

5.3.1 prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, ensure (subject to clause 8.4) that each Sub-Processor is appointed under a written contract containing materially the same obligations as under paragraphs 2 to 12 (inclusive) (including those obligations relating to sufficient guarantees to implement appropriate technical and organisational measures);

5.3.2 remain fully liable for all the acts and omissions of each Sub-Processor as if they were its own.

5.4 The Supplier shall ensure that all natural persons authorised by it (or by any Sub-Processor) to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data confidential in a manner consistent with the Supplier's confidentiality obligations under our Agreement.

6 ASSISTANCE WITH COMPLIANCE AND DATA SUBJECT RIGHTS

6.1 The Supplier shall refer all Data Subject Requests it receives to the Customer without undue delay. The Customer shall pay the Supplier for all work, time, costs and expenses incurred by the Supplier or any Sub-Processor(s) in connection with such activity, calculated on a time and materials basis at the Supplier's rates set out in the Supplier's Standard Pricing Terms.

6.2 The Supplier shall provide such assistance as the Customer reasonably requires (taking into account the nature of processing and the information available to the Supplier) to the Customer in ensuring compliance with the Customer's obligations under Data Protection Laws with respect to:

6.2.1 security of processing;

6.2.2 data protection impact assessments (as such term is defined in Data Protection Laws);

6.2.3 prior consultation with a Supervisory Authority regarding high risk processing; and

6.2.4 notifications to the Supervisory Authority and/or communications to Data Subjects by the Customer in response to any Personal Data Breach, provided the Customer shall pay the Supplier for all work, time, costs and expenses incurred by the Supplier or any Sub-Processor(s) in connection with providing the assistance in this paragraph 6.2, calculated on a time and materials basis at the Supplier's rates set out in the Supplier's Standard Pricing Terms.

7 INTERNATIONAL DATA TRANSFERS

7.1 Subject to paragraphs 7.2 and 7.3, the Supplier shall not Transfer any Protected Data:

7.1.1 in or to any country or territory; and/or

7.1.2 to an organisation and/or its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries, without the Customer's prior written authorisation except where required by Relevant Law (in which case the provisions of paragraph 3.1 shall apply).

7.2 The Customer hereby authorises the Supplier (or any Sub-Processor) to Transfer any Protected Data for the purposes for which such data may be processed under our Agreement to any International Recipient(s), provided all such Transfers of Protected Data to an International Recipient shall (to the extent required under Data Protection Laws) be effected by way of Lawful Safeguards and in accordance with Data Protection Laws and our Agreement. The provisions of our Agreement (including this Data Protection Addendum) shall constitute the Customer's instructions with respect to Transfers in accordance with paragraph 3.1.1.

7.3 The Customer acknowledges that due to the nature of cloud services, the Protected Data may be Transferred to recipients or other geographical locations in connection with use of the Services further to access and/or computerised instructions initiated by Authorised Users. The Customer acknowledges that the Supplier does not control such processing and the Customer shall ensure that Authorised Users (and all others acting on its behalf) only initiate the Transfer of Protected Data to recipients or other geographical locations if Lawful Safeguards are in place and that such Transfer is in compliance with all Relevant Laws.

7.4 The Supplier and each Sub-Processor is not obliged to undertake any unlawful Transfer of Protected Data and shall not be liable to the extent that it (or any Sub-Processor) is delayed in or fails to perform any obligation under our Agreement due to it (or any Sub-Processor) being unable (or believing it is unable) to undertake any Transfer in a lawful manner. The Fees payable to the Supplier shall not be discounted or set-off as a result of any delay or non-performance of any obligation in accordance with this paragraph 7.4.

8 INFORMATION AND AUDIT

8.1 The Supplier shall maintain, in accordance with Data Protection Laws binding on the Supplier, written records of all categories of processing activities carried out on behalf of the Customer.

8.2 On request, the Supplier shall provide the Customer (or auditors mandated by the Customer) with a copy of the third party certifications and audits to the extent made generally available to its customers. Such information shall be confidential to the Supplier and shall be Supplier's Confidential Information as defined in our Agreement, and shall be treated in accordance with applicable terms.

8.3 In the event that the Customer, acting reasonably, deems the information provided in accordance with paragraph 8.2 insufficient to satisfy its obligations under Data Protection Laws, the Supplier shall, on request by the Customer make available to the Customer such information as is reasonably necessary to demonstrate the Supplier's compliance with its obligations under this Data Protection Addendum and Article 28 of the GDPR, and allow for and contribute to audits, including inspections, by the Customer (or another auditor mandated by the Customer) for this purpose provided:

8.3.1 such audit, inspection or information request is reasonable, limited to information in the Supplier's possession or control and is subject to the Customer giving the Supplier reasonable (and in any event at least 60 days') prior notice of such audit, inspection or information request;

8.3.2 the parties (each acting reasonably and consent not to be unreasonably withheld or delayed) shall agree the timing, scope and duration of the audit, inspection or information release together with any specific policies or other steps with which the Customer or third party auditor shall comply (including to protect the security and confidentiality of other customers, to ensure the Supplier is not placed in breach of any other arrangement with any other customer and so as to comply with the remainder of this paragraph 8.3);

8.3.3 the Customer shall ensure that any such audit or inspection is undertaken during normal business hours, with minimal disruption to the businesses of the Supplier;

8.3.4 the duration of any audit or inspection shall be limited to one Business Day;

8.3.5 all costs of such audit or inspection or responding to such information request shall be borne by the Customer, and the Supplier's costs, expenses, work and time incurred in connection with such audit or inspection shall be reimbursed by the Customer on a time and materials basis in accordance with the Supplier's Standard Pricing Terms;

8.3.6 the Customer's rights under this paragraph 8.3 may only be exercised once in any consecutive 12 month period, unless otherwise required by a Supervisory Authority or if the Customer (acting reasonably) believes the Supplier is in breach of this Data Protection Addendum;

8.3.7 the Customer shall promptly (and in any event within one Business Day) report any non-compliance identified by the audit, inspection or release of information to the Supplier;

8.3.8 the Customer agrees that all information obtained or generated by the Customer or its auditor(s) in connection with such information requests, inspections and audits shall be Supplier's Confidential Information as defined in our Agreement, and shall be treated in accordance with applicable terms;

8.3.9 the Customer shall ensure that each person acting on its behalf in connection with such audit or inspection (including the personnel of any third party auditor) shall not by any act or omission cause or contribute to any damage, destruction, loss or corruption of or to any systems, equipment or data in the control or possession of the Supplier while conducting any such audit or inspection; and

8.3.10 this paragraph 8.3 is subject to paragraph 8.4.

8.4 The Customer acknowledges and accepts that relevant contractual terms agreed with Sub-Processor(s) may mean that the Supplier or Customer may not be able to undertake or facilitate an information request or audit or inspection of any or all Sub-Processors pursuant to paragraph 8.3 and:

8.4.1 the Customer's rights under paragraph 8.3 shall not apply to the extent inconsistent with relevant contractual terms agreed with Sub-Processor(s);

8.4.2 to the extent any information request, audit or inspection of any Sub-Processor are permitted in accordance with this paragraph 8.4, equivalent restrictions and obligations on the Customer to those in paragraphs 8.3.1 to 8.3.10 (inclusive) shall apply together with any additional or more extensive restrictions and obligations applicable in the circumstances; and

8.4.3 paragraphs 5.3.1 and 8.3 shall be construed accordingly.

8.5 Notwithstanding paragraph 8.4, the Supplier shall ensure that it has appropriate mechanisms in place to ensure its Sub-Processors meet their obligations under Data Protection Laws and the Supplier's obligations in respect of Protected Data under our Agreement. The Customer accepts that the provisions of paragraph 8.4 shall satisfy the Supplier's obligations in that regard.

9 BREACH NOTIFICATION

9.1 In respect of any Personal Data Breach, the Supplier shall, without undue delay (and in any event within 72 hours):

9.1.1 notify the Customer of the Personal Data Breach; and

9.1.2 provide the Customer with details of the Personal Data Breach.

10 DELETION OF PROTECTED DATA AND COPIES

Following the end of the provision of the Services (or any part) relating to the processing of Protected Data the Supplier shall dispose of Protected Data in accordance with its obligations under our Agreement, including Clause 12.6 of the Master SaaS Terms. The Supplier shall have no liability (howsoever arising, including in negligence) for any deletion or destruction of any such Protected Data undertaken in accordance with our Agreement.

11 COMPENSATION AND CLAIMS

11.1 The Supplier shall be liable for Data Protection Losses (howsoever arising, whether in contract, tort (including negligence) or otherwise) under or in connection with our Agreement:

11.1.1 only to the extent caused by the processing of Protected Data under our Agreement and directly resulting from the Supplier's breach of our Agreement; and

11.1.2 in no circumstances to the extent that any Data Protection Losses (or the circumstances giving rise to them) are contributed to or caused by any breach of our Agreement by the Customer (including in accordance with paragraph 3.1.3(b)).

11.1A For the avoidance of doubt, the Supplier's liability for Data Protection Losses under this paragraph 11 shall be subject to and shall not exceed the limitations and caps set out in Clause 17 of the Master SaaS Terms, including the insurance proceeds cap in Clause 17.6 in respect of claims arising from loss or corruption of Customer Data or a security or cyber breach.

11.2 If a party receives a compensation claim from a person relating to processing of Protected Data in connection with our Agreement or the Services, it shall promptly provide the other party with notice and full details of such claim.

11.3 The parties agree that the Customer shall not be entitled to claim back from the Supplier any part of any compensation paid by the Customer to the extent that the Customer is liable to indemnify or otherwise compensate the Supplier in accordance with our Agreement.

11.4 This paragraph 11 is intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

11.4.1 to the extent not permitted by Relevant Law (including Data Protection Laws); and

11.4.2 that it does not affect the liability of either party to any Data Subject.

12 SURVIVAL

This Data Protection Addendum (as Updated from time to time) shall survive termination (for any reason) or expiry of our Agreement and continue until no Protected Data remains in the possession or control of the Supplier or any Sub-Processor, except that paragraphs 10 to 12 (inclusive) shall continue indefinitely.

13 DATA PROTECTION CONTACT

Should any questions arise, the Supplier's data protection team can be contacted at support@kudosoftware.com

---

THE SCHEDULE — DATA PROCESSING DETAILS

Subject-matter of processing:

Supplier's performance of the Services.

Duration of the processing:

Until the earlier of final termination or final expiry of our Agreement, except as otherwise expressly stated in our Agreement.

Nature and purpose of the processing:

- Processing in accordance with the rights and obligations of the parties under our Agreement;
- Processing as reasonably required to provide the Services; and
- Processing as initiated, requested or instructed by Authorised Users in connection with their use of the Services, or by the Customer, in each case in a manner consistent with our Agreement.

Type of Personal Data:

Names, titles, positions, e-mail addresses, phone numbers, and any other Personal Data that Authorised Users choose to input into the Platform in the course of using the Services, including but not limited to site visit records, attendance data, scheduling and availability information, and other operational data relating to identifiable individuals.

Categories of Data Subjects:

Authorised Users, employees, contractors, site personnel, customers, or other Data Subjects, including those of the Customer and any other individuals whose Personal Data is processed by the Customer in connection with its use of the Services.

Special categories of Personal Data:

None.