ARTICLE 28 AGREEMENT

Data Processing Agreement

Guest names are third-party personal data, so processing them needs a written agreement under Article 28 of the UK GDPR. This is it. You accept it by a separate tick at sign-up, not folded into the terms of service, and you can read the whole of it here before you enter a single name.

Version	Last updated	You are	We are
1.0	15 August 2026	The controller	The processor

1. Parties and roles

- 1.1 This Agreement is between you, the account holder (the **Controller**), and MABUREDE AI LTD, registered in England and Wales under company number 17157267 with its registered office at Flat 47 Ludham Lismore Circus, London, England, NW5 4SE, trading as Tablemark (the **Processor**).
- 1.2 The Controller determines why and how the personal data of guests is processed. The Processor processes that data only on the Controller's documented instructions, which are given by using the service and by the settings the Controller chooses within it.
- 1.3 This Agreement takes effect when the Controller accepts it at sign-up, by a tick separate from the acceptance of the Terms of Service, and continues for as long as the Processor holds any guest data for the Controller.
- 1.4 Terms such as personal data, processing, data subject, personal data breach and supervisory authority have the meanings given in the UK GDPR and the Data Protection Act 2018.

2. Subject matter, duration and purpose

- 2.1 **Subject matter:** production of place cards, escort cards, table numbers, menu cards, seating plans, floor plan artwork and entrance guide video for an event organised or serviced by the Controller.
- 2.2 **Duration:** for each event, until the retention period chosen by the Controller expires, until 14 days after the event date recorded by the Controller, or until the Controller deletes the event — whichever occurs first.
- 2.3 **Purpose:** generating the outputs described above, and nothing else. The Processor will not process guest data for its own purposes.

3. Categories of data and data subjects

- 3.1 **Data subjects:** guests invited to the Controller's event, including guests who are children, and any person named on a list the Controller uploads.
- 3.2 **Personal data:** name as entered, card name derived from it, title where given, the original source row, table allocation, seating constraints referencing named guests, and — only where the Controller has switched the field on — dietary notes.
- 3.3 **Special category data:** dietary notes may reveal religious belief or health information and are therefore treated as Article 9 data. The field is disabled by default. Where the Controller enables it, the Controller confirms it has a lawful basis under both Article 6 and Article 9.
- 3.4 The Processor does not create, request or store any field describing a relationship, a social note, a seating strategy, a guest profile or any inference about a data subject. No such field exists in the system.

4. Prohibited processing

- 4.1 The Processor **will not** use guest data, or anything derived from it, to train, fine-tune, evaluate, benchmark or otherwise develop any machine learning model, whether its own or a third party's.
- 4.2 The Processor **will not** profile, score, label, segment or analyse data subjects, and will not enrich guest data from any other source.
- 4.3 The Processor **will not** use guest data for marketing of any kind, will not contact data subjects, and provides no mechanism by which it could.
- 4.4 The Processor **will not** sell, licence, rent, publish or otherwise disclose guest data to any third party, including in aggregated, pseudonymised or anonymised form, except to the sub-processors listed in clause 7 and where required by law.

5. Retention, deletion and return

- 5.1 The Controller selects a retention period of 30, 60 or 90 days. Where no selection is made, 90 days applies.
- 5.2 Where the Controller records an event date, all guest data for that event is deleted 14 days after that date, or at the end of the retention period, whichever occurs first.
- 5.3 The Controller may delete an event and all guest data within it at any time, immediately, from within the service. The Processor will act on that instruction without delay and without requiring a reason.
- 5.4 Deletion removes the data from live systems. Encrypted backups are cycled out within 35 days and deleted records are not restored from them.
- 5.5 A single-guest video clip contains a data subject's name and is deleted 7 days after it is created, regardless of the event retention period.
- 5.6 On request before deletion, the Processor will return the guest data to the Controller in a structured, commonly used, machine-readable format.

6. Security

- 6.1 The Processor implements appropriate technical and organisational measures under Article 32, including: encryption in transit using TLS; encryption at rest; field-level encryption of guest name fields; multi-factor authentication for production access; role-based access control; logging of every read and export of a guest list; encrypted backups; and salted password hashing.
- 6.2 Personnel with access to guest data are bound by confidentiality obligations that survive the end of their engagement.
- 6.3 Staff access to a Controller's guest data occurs only where the Controller has raised a support request that requires it, and every such access is recorded in a log the Controller can inspect.
- 6.4 The Processor tests and reviews these measures periodically and will not materially reduce them during the term.

7. Sub-processors

- 7.1 The Controller gives general authorisation for the Processor to engage the sub-processors listed below. Each is bound by written terms imposing data protection obligations no less protective than this Agreement.
- 7.2 The Processor gives the Controller at least **30 days** written notice before adding or replacing a sub-processor. The Controller may object on reasonable data protection grounds within that period; if the objection cannot be resolved, the Controller may terminate and receive a refund of the unused portion of any prepaid period.
- 7.3 The Processor remains fully liable to the Controller for the acts and omissions of its sub-processors.

PURPOSE	REGION	DATA REACHED	SAFEGUARD
Model inference	United Kingdom and United States	Guest names and list text you submit for processing	UK IDTA and Standard Contractual Clauses
Cloud hosting and database	European Economic Area	Account records, events, guest records, exports	Processing within the EEA under an adequacy decision
File and image storage	European Economic Area	Generated card artwork, export files, video files	Processing within the EEA under an adequacy decision
Transactional email delivery	European Economic Area and United States	Account email address, message content you send us	UK IDTA and Standard Contractual Clauses
Payment processing	European Economic Area and United States	Billing name, billing address, card details entered on the payment page	UK IDTA and Standard Contractual Clauses
Error and uptime monitoring	European Economic Area	Technical logs, error traces, IP address	Processing within the EEA under an adequacy decision

8. International transfers

- 8.1 Where guest data is transferred outside the United Kingdom or the European Economic Area, the transfer is made under the UK International Data Transfer Addendum to the EU Standard Contractual Clauses, or under the Standard Contractual Clauses, supported by a transfer risk assessment.
- 8.2 Model inference may occur outside the United Kingdom. This is stated plainly rather than described as use of industry standard providers, and the regions involved are listed in clause 7.
- 8.3 The Controller may request a copy of the transfer mechanism applying to any particular transfer.

9. Data subject rights

- 9.1 The Processor will assist the Controller, by appropriate technical and organisational measures and insofar as possible, in responding to requests from data subjects exercising rights under Chapter III of the UK GDPR.
- 9.2 Where a data subject contacts the Processor directly — for example a guest who has found their name on a list — the Processor will not act on that request itself. It will pass the request to the Controller without undue delay and act on the Controller's instruction. The Processor will tell the data subject that it has done so.
- 9.3 The Processor makes an export and deletion function available in the service so that the Controller can satisfy most requests without contacting the Processor at all.

10. Personal data breach

- 10.1 The Processor will notify the Controller **without undue delay and in any event within 72 hours** of becoming aware of a personal data breach affecting the Controller's guest data.
- 10.2 The notification will describe the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point for further information. Where the full picture is not available at the time, information is provided in phases without further undue delay.
- 10.3 The Processor will assist the Controller in meeting its own obligations under Articles 33 and 34, including any decision about whether to inform data subjects. That decision belongs to the Controller.

11. Audit and assurance

- 11.1 The Processor will make available to the Controller the information necessary to demonstrate compliance with Article 28.
- 11.2 Controllers on the Venue plan may request a written annual compliance statement covering the measures in clause 6 and the sub-processor list in clause 7.
- 11.3 Where an audit or inspection is required by a supervisory authority, the Processor will cooperate, on reasonable notice, during business hours and subject to confidentiality.

12. Controller obligations

- 12.1 The Controller confirms that it has a lawful basis for holding the guest data it uploads, that it is entitled to instruct the processing described here, and that its own privacy information covers this processing.
- 12.2 The Controller confirms it will not upload guest data for an event it is not organising or servicing, and will not use the service to build a marketing list. See the Acceptable Use Policy.
- 12.3 The Controller is responsible for completing the per-name confirmation step before export. The Processor blocks export until it is complete, but the decision recorded at each confirmation is the Controller's.

13. General

- 13.1 This Agreement is governed by the law of England and Wales and the courts of England and Wales have exclusive jurisdiction.
- 13.2 Where this Agreement conflicts with the Terms of Service in relation to guest data, this Agreement prevails.
- 13.3 Amendments required by a change in data protection law take effect on 30 days notice to the Controller.
- 13.4 Contact for all matters under this Agreement: support@maburedeai.shop, or MABUREDE AI LTD, Flat 47 Ludham Lismore Circus, London, England, NW5 4SE.

MABUREDE AI LTD (17157267) · support@maburedeai.shop

Registered office: Flat 47 Ludham Lismore Circus, London, England, NW5 4SE. Registered in England and Wales.