

# Skedda Data Processing Addendum

**Version 2026.10 (October 2026) – applies automatically where the Agreement provides that it does, and otherwise when signed by both parties**

This Data Processing Addendum, including its Annexes (the “DPA”), applies between Skedda, Inc. (“Skedda”) and a customer that has subscribed to the Services (“Client”): (a) automatically, without signature, to the extent the agreement between them for the Services provides that it does; and (b) otherwise, when signed by both parties. For example, Skedda’s online terms of service apply this DPA automatically to Personal Data subject to European Data Protection Laws or US State Privacy Laws, and Skedda’s standard Order Form and the Skedda Terms of Service attached to it apply it automatically to all Personal Data. Where this DPA applies automatically, it takes effect from the date that agreement takes effect, and the SCCs are entered into as described in Section 7.3. Publication of this DPA does not by itself make it binding. Once it applies, it forms part of the agreement between Skedda and Client for the Services, whether that agreement is an Order Form and Skedda Terms of Service, Skedda’s online terms of service, or another written agreement (the “Agreement”). This DPA applies to the extent Skedda Processes Personal Data on behalf of Client in providing the Services.

Where signed, this DPA takes effect on the later of the effective date of the Agreement and the date on which both parties have signed it. If this DPA conflicts with the Agreement, this DPA prevails on the Processing of Personal Data. Capitalized terms not defined in this DPA have the meanings given in the Agreement. Where the Agreement uses different terms for the same concepts (for example, “Venue”, “Venue Account” or “Venue Data”), references in this DPA to “Client”, “Client Account” and “Client Data” mean those equivalent terms.

## 1. Definitions

“Client Data” has the meaning given in the Agreement or, if not defined there, means all data submitted to the Services by or on behalf of Client or its Users.

“Data Protection Laws” means all data protection and privacy laws and regulations applicable to a party’s Processing of Personal Data under the Agreement, including

European Data Protection Laws and US State Privacy Laws, in each case as amended or replaced from time to time.

“European Data Protection Laws” means, as applicable: (i) Regulation (EU) 2016/679 (“GDPR”); (ii) the GDPR as it forms part of the law of the United Kingdom, together with the Data Protection Act 2018 (“UK GDPR”); (iii) the Swiss Federal Act on Data Protection of 25 September 2020 and its ordinances (“FADP”); and (iv) Directive 2002/58/EC and national laws implementing any of the foregoing.

“European Data” means Personal Data subject to European Data Protection Laws.

“Personal Data” means any information in Client Data that relates to an identified or identifiable natural person and that is protected as “personal data”, “personal information” or an equivalent term under Data Protection Laws.

“Personal Data Breach” means a breach of security of the Services, or of other systems that Skedda or its Sub-Processors use to Process Personal Data, leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed by Skedda or its Sub-Processors. It does not include unsuccessful attempts or activities that do not compromise the security of Personal Data, such as unsuccessful log-in attempts, pings, port scans, and unsuccessful denial-of-service or other network attacks on firewalls or networked systems. It also does not include incidents affecting systems that are not operated by Skedda or its Sub-Processors, such as Client’s own systems or Third-Party Platforms.

“Processing” means any operation performed on Personal Data, whether or not by automated means, and “Process” and “Processed” are construed accordingly. “Controller”, “Processor”, “Data Subject” and “supervisory authority” have the meanings given in the GDPR, and include the equivalent terms under other Data Protection Laws (including “business”, “service provider” and “contractor” under US State Privacy Laws).

“Standard Contractual Clauses” or “SCCs” means the standard contractual clauses approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as amended or replaced.

“Sub-Processor” means any third party engaged by Skedda to Process Personal Data in providing the Services. Skedda’s employees and individual contractors are not Sub-Processors.

“Sub-Processor List” means the list of Skedda’s Sub-Processors published at <https://trust.skedda.com/subprocessors>, or any successor page on the Trust Center.

“Trust Center” means Skedda’s trust center at <https://trust.skedda.com>, or any successor site.

“UK Addendum” means the International Data Transfer Addendum to the SCCs (version B.1.0) issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018, as amended or replaced.

“US State Privacy Laws” means all US state laws relating to the protection and Processing of personal information, including the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and its implementing regulations (“CCPA”).

## 2. Roles and Scope

**2.1 Roles.** As between the parties, Client is the Controller of Personal Data and Skedda is its Processor. Where Client acts as a Processor on behalf of a third-party Controller (for example, an affiliate or customer of Client), Skedda is Client’s Sub-Processor, and Client is responsible for obtaining any authorizations that Controller requires. Client’s affiliates that are permitted to use the Services under the Agreement may benefit from this DPA only through Client. Client will exercise any rights under this DPA on their behalf, and those affiliates may not bring claims directly against Skedda, except to the extent the SCCs or Data Protection Laws give them a direct right.

**2.2 Details of Processing.** The subject matter, nature, purpose and duration of the Processing, and the categories of Personal Data and Data Subjects, are described in Annex 1.

**2.3 Skedda as Controller.** This DPA does not apply to personal data that Skedda Processes as a Controller. Skedda acts as a Controller only for: (a) business-contact, billing, account-administration and relationship-management data about Client’s personnel, including information about how Client’s administrators use the Services (such as sign-ins, features used, settings changes and support interactions), which Skedda uses to manage Client’s account, provide support, secure and improve the Services and communicate with Client about the Services, but not booking content or other Personal Data about Users who are not administrators, including where it appears in support interactions; (b) personal data

Skedda collects directly through Skedda's own websites, such as skedda.com and allbooked.com, other than booking sites Skedda hosts for its customers (for example, from visitors to those websites); and (c) the Skedda login that a User can use with more than one Skedda customer (the User's email address, password, sign-in identifiers from third-party sign-in providers, and the list of customers linked to the login), to the extent Skedda Processes it to maintain that login across customers. Skedda handles the data in (a) to (c) as described in its Privacy Policy (<https://support.skedda.com/legal/privacy-policy-for-venues>). Single sign-on that Client configures for the Client Account remains Client Data. Where Skedda accesses Personal Data within the Client Account to provide support, Skedda remains a Processor under this DPA.

### 3. Client Responsibilities

3.1 Compliance. Client will comply with Data Protection Laws in its use of the Services and its Instructions to Skedda. Client is solely responsible for: (a) the accuracy, quality and legality of Personal Data and the means by which Client obtained it; (b) providing any required notices and obtaining any required consents or other lawful basis for the Processing; (c) ensuring that Client has the right to provide Personal Data to Skedda for Processing under the Agreement; and (d) not taking any action that would make its provision of Personal Data to Skedda a "sale" or "share" under US State Privacy Laws. Client will tell Skedda without undue delay if it can no longer meet these responsibilities.

3.2 Instructions. The Agreement, this DPA and Client's configuration and use of the Services are Client's complete documented instructions to Skedda for the Processing of Personal Data ("Instructions"). Additional Instructions must be in writing, consistent with the Agreement and with the nature and lawful use of the Services.

3.3 Sensitive Data. Client will not submit to the Services any Sensitive Personal Information as defined in the Agreement or, if the Agreement does not define that term, any special categories of personal data, unless the Agreement expressly permits it.

3.4 Client Controls. Client is responsible for configuring the Services appropriately, including User roles and permissions, authentication settings and data-retention settings. Client is also responsible for independently determining whether the Services' security measures meet Client's own obligations under Data Protection Laws.

3.5 Channels. This DPA applies to Personal Data Processed through the Services. Client will not send Personal Data to Skedda by other means, such as email or support channels, except to the extent reasonably necessary to obtain support.

## 4. Skedda Obligations

4.1 Processing on Instructions. Skedda will Process Personal Data only on Client's Instructions, unless applicable law requires otherwise. In that case, Skedda will inform Client of the legal requirement before Processing, unless the law prohibits it. Skedda is not responsible for complying with Data Protection Laws that apply to Client or its industry but do not generally apply to Skedda as a provider of the Services.

4.2 Unlawful Instructions. Skedda will promptly inform Client if, in Skedda's opinion, an Instruction infringes Data Protection Laws. If Skedda cannot Process Personal Data as instructed because of a legal requirement, Skedda may suspend the affected Processing, other than storing and securing the data, until Client issues new lawful Instructions. Skedda will not be liable for failing to perform the affected Services during that period.

4.3 Personnel. Skedda will ensure that personnel authorized to Process Personal Data are bound by appropriate contractual or statutory confidentiality obligations.

4.4 Security. Skedda will implement and maintain appropriate technical and organizational measures to protect Personal Data, as described in Annex 2 (the "Security Measures"). Skedda may update the Security Measures from time to time, provided the updates do not materially reduce the overall protection of Personal Data.

4.5 Personal Data Breaches. Skedda will notify Client without undue delay, and in any event within 72 hours, after becoming aware of a Personal Data Breach. As information becomes available, Skedda will give Client information reasonably required for Client to meet its own notification obligations, including, where known, the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences and the measures taken or proposed. Skedda will take reasonable steps to contain, investigate and mitigate the breach. Notifying or responding to a Personal Data Breach does not mean Skedda acknowledges fault or liability. Except as Data Protection Laws or the SCCs require, this Section 4.5 does not apply to incidents caused by Client or its Users.

4.6 Assistance. Taking into account the nature of the Processing and the information available to Skedda, Skedda will provide reasonable assistance to Client with security, breach notification, data protection impact assessments and prior consultations with supervisory authorities, to the extent required by the Data Protection Laws that apply to Skedda's Processing under this DPA. Skedda may meet requests for this assistance by referring Client to materials on the Trust Center.

4.7 Anonymized Data. Client instructs Skedda to anonymize or de-identify Personal Data as needed to operate, secure, support and improve the Services. Data that meets the applicable legal standard for anonymized or de-identified data, such as anonymized statistical data, is not Personal Data and is not subject to this DPA, and Skedda may use it as permitted by the Agreement. Data is not treated as anonymized merely because it is aggregated.

4.8 Government Access Requests. If a public authority requests access to Personal Data, Skedda will, to the extent legally permitted and reasonably practicable, notify Client. Skedda may direct the authority to request the data from Client, and will disclose only the Personal Data it is legally required to disclose. For transfers subject to the SCCs, Clause 15 of the SCCs also applies.

## 5. Data Subject Requests

The Services include controls that Client can use to access, correct, export, delete or restrict Personal Data in response to Data Subjects' requests to exercise their rights ("Data Subject Requests"). Where Client cannot address a Data Subject Request through those controls, Skedda will provide reasonable assistance on Client's written request, including with inquiries from supervisory authorities. If Skedda receives a Data Subject Request that relates to Client, Skedda will promptly forward it to Client and may advise the Data Subject to contact Client. Client is responsible for responding to Data Subject Requests. Client will inform Skedda of any consumer request made under US State Privacy Laws that Skedda must comply with, and will provide the information Skedda needs to comply with it.

## 6. Sub-Processors

6.1 Authorization. Client gives Skedda general authorization to engage Sub-Processors. The Sub-Processors on the Sub-Processor List when this DPA takes effect are authorized. The

Sub-Processor List shows each Sub-Processor's function and location, and forms part of this DPA.

**6.2 Obligations.** Skedda will enter into a written agreement with each Sub-Processor that imposes data protection obligations no less protective of Personal Data than those in this DPA, to the extent applicable to the services the Sub-Processor provides. Skedda remains responsible for each Sub-Processor's performance of those obligations, subject to the Agreement's limitations of liability.

**6.3 Notice of New Sub-Processors.** Skedda will update the Sub-Processor List at least 30 days before a new Sub-Processor begins Processing Personal Data, and will send notice of the change by email, which may be sent through the Trust Center's update service. Skedda will subscribe Client's notice address under Section 12.6 to that service. Client may add or change subscribed addresses through the Trust Center or by email to [dpo@skedda.com](mailto:dpo@skedda.com). If Client unsubscribes an address, or the notice address Client provides is invalid or no longer in use, Skedda's update of the Sub-Processor List together with notice through that service still constitutes notice to Client under this Section 6.3. Where a new Sub-Processor is needed urgently to protect the security or continuity of the Services, Skedda will give notice as soon as reasonably practicable. Where the SCCs apply, this urgent-change exception applies only to the extent the SCCs permit it. The parties agree that notice given under this Section 6.3 is the means by which Skedda specifically informs Client in writing of intended changes for the purposes of Clause 9(a) of the SCCs.

**6.4 Objections.** Client may object to a new Sub-Processor on reasonable grounds relating to the protection of Personal Data, by notifying Skedda in writing within 30 days after the notice in Section 6.3 and stating the specific grounds. If Client does not object within that period, Client is deemed to have consented to the new Sub-Processor. The parties will discuss Client's concerns in good faith. Skedda may resolve the objection, at its option, by: (a) not using the Sub-Processor to Process Client's Personal Data; (b) taking corrective steps that Client reasonably accepts as addressing its concerns; or (c) ceasing to provide, or Client agreeing not to use, the part of the Services that relies on the Sub-Processor. If none of these is commercially reasonable in Skedda's judgment and the objection is not resolved within 30 days after Skedda receives it, either party may terminate only the Services that cannot be provided without the Sub-Processor, on written notice. Termination under this Section 6.4 is Client's sole and exclusive remedy for an objection.

6.5 Sub-Processor Agreements. Where Clause 9(c) of the SCCs requires Skedda to provide a copy of a Sub-Processor agreement, Skedda will do so only on Client's written request. Skedda may first remove all commercial information and any clauses unrelated to the SCCs or equivalent terms, and may provide the copy in a manner Skedda determines, on a confidential basis.

## 7. International Data Transfers

7.1 Global Processing. Client acknowledges that Skedda and its Sub-Processors may Process Personal Data in the United States and in other countries where they operate, as necessary to provide the Services. Client will ensure that its transfers of Personal Data to Skedda comply with Data Protection Laws, and Skedda will ensure that the transfers it makes as Processor comply with the Data Protection Laws that apply to it.

7.2 European Transfers. Skedda will not transfer European Data to a country or recipient that is not recognized as providing an adequate level of protection under European Data Protection Laws, unless the transfer is covered by an adequacy decision (including the EU-U.S. Data Privacy Framework and its UK and Swiss extensions, where the recipient is certified) or an appropriate safeguard applies, such as the SCCs, the UK Addendum or binding corporate rules.

7.3 EU SCCs. To the extent a transfer of European Data subject to the GDPR from Client to Skedda requires it, the parties enter into the SCCs, which are incorporated into this DPA, when both parties sign this DPA or, where this DPA applies automatically under the Agreement, when Client accepts the Agreement. Annex 1 identifies the parties using the details in the Agreement. Client is the "data exporter" and Skedda is the "data importer", and the SCCs apply as follows:

- (a) Module Two applies where Client is a Controller and Module Three applies where Client is a Processor;
- (b) in Clause 7, the optional docking clause applies;
- (c) in Clause 9, Option 2 (general written authorization) applies, with the notice period and procedure in Section 6;
- (d) in Clause 11, the optional language does not apply;

- (e) in Clause 17, Option 1 applies and the SCCs are governed by the laws of Ireland, and in Clause 18 disputes will be resolved by the courts of Ireland;
- (f) Annexes I and II of the SCCs are completed by Annexes 1 and 2 of this DPA, and Annex III by the Sub-Processor List;
- (g) the audits described in Clause 8.9 will be carried out in accordance with the procedures in Section 9, and the certification of deletion described in Clauses 8.5 and 16(d) will be provided only on Client's written request; and
- (h) Skedda will notify Client of Personal Data Breaches under Clause 8.6 in accordance with Section 4.5.

7.4 UK Transfers. For transfers of European Data subject to the UK GDPR, the SCCs apply as set out in Section 7.3, as amended by the UK Addendum. The parties agree to be bound by Part 2: Mandatory Clauses of the Approved Addendum (which is the UK Addendum), being the template Addendum B.1.0 issued by the UK Information Commissioner and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses. The information required by Tables 1 to 3 of Part 1 of the Approved Addendum is set out in Section 7.3 and Annexes 1 and 2. For Table 4, the data importer may end the Approved Addendum as permitted by its Section 19.

7.5 Swiss Transfers. For transfers of European Data subject to the FADP, the SCCs apply as set out in Section 7.3, with these changes: (a) references to the GDPR are to be read as references to the FADP; (b) the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner; (c) references to "Member State" do not prevent Data Subjects habitually resident in Switzerland from bringing claims in Switzerland; and (d) where transfers are exclusively subject to the FADP, the SCCs are governed by Swiss law and disputes will be resolved by the courts of Switzerland.

7.6 Order of Precedence. If the SCCs or the UK Addendum apply, they prevail over this DPA and the Agreement to the extent of any conflict. Nothing in this DPA or the Agreement modifies, limits or contradicts them.

7.7 Alternative Transfer Mechanisms. If Skedda adopts another lawful transfer mechanism for European Data, such as certification under the EU-U.S. Data Privacy Framework, that mechanism may be relied on to the extent it covers the transfer and for as long as it remains valid. The SCCs and UK Addendum will continue to apply as a fallback, so that they

govern the transfer if that mechanism ceases to be valid or does not apply. Skedda may notify Client of any such mechanism by updating the Trust Center. Client will take any reasonable steps needed to give it effect.

## 8. US, Canadian and Australian Privacy Laws

8.1 US State Privacy Laws. To the extent Skedda Processes Personal Data on Client's behalf and that Personal Data is subject to US State Privacy Laws, Skedda acts as Client's service provider, contractor or Processor, as applicable, and:

- (a) will not sell or share Personal Data, including for cross-context behavioral advertising or targeted advertising;
- (b) will not retain, use or disclose Personal Data for any purpose other than the business purposes set out in the Agreement and this DPA. Those purposes are: providing the Services, including account provisioning and authentication, management of resources, bookings and visitors, Client-configured notifications and communications, and Client-enabled integrations with Third-Party Platforms; providing customer support; securing the Services, detecting security incidents and preventing fraud; maintaining the reliability and availability of the Services; improving the quality of the Services (but not building profiles for use in providing services to another business); and any other use that US State Privacy Laws permit. Skedda will not retain, use or disclose Personal Data outside the direct business relationship between Skedda and Client;
- (c) will not combine Personal Data with personal information that Skedda receives from or on behalf of others, or collects from its own interactions with consumers, except as US State Privacy Laws permit;
- (d) will comply with the obligations that US State Privacy Laws impose on it and provide the same level of privacy protection those laws require. Skedda will notify Client if it determines that it can no longer meet those obligations, and Client may then take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data;
- (e) where Skedda creates de-identified data from Personal Data, will, to the extent US State Privacy Laws require for that data to be treated as de-identified, take reasonable measures to ensure it cannot be linked to an individual or household, publicly commit

to maintaining it in de-identified form, not attempt to re-identify it (except to test its de-identification processes), and contractually require any recipient of it to comply with these restrictions; and

(f) certifies that it understands and will comply with this Section 8.1.

8.2 Canada. To the extent Personal Data is subject to Canadian privacy laws, the parties intend this DPA to provide a level of protection comparable to that required by those laws, and Skedda will use that Personal Data only for the purposes of the Agreement. Where Quebec's Act respecting the protection of personal information in the private sector applies, Skedda will also notify Client without undue delay of any violation, or attempted violation, of its confidentiality obligations under this DPA of which it becomes aware. Client may verify Skedda's compliance with those obligations in accordance with Section 9, and Section 10 applies at the end of the Agreement.

8.3 Australia. To the extent Personal Data is subject to the Privacy Act 1988 (Cth), Skedda will not handle that Personal Data in a way that would breach Australian Privacy Principle 6, 8 or 11 if Skedda were bound by them in relation to that Personal Data.

## 9. Demonstrating Compliance and Audits

9.1 Independent Audits. Skedda's security program is audited by an independent third-party auditor (currently annually, under the AICPA SOC 2 Type II framework). Skedda makes its current audit reports, penetration-test summaries, security policies and related documentation available through the Trust Center, subject to confidentiality terms.

9.2 Information Requests. No more than once in any 12-month period, unless there are reasonable indications of non-compliance or a supervisory authority requires otherwise, Skedda will respond in writing to Client's reasonable written information requests, including security questionnaires, to the extent needed to confirm Skedda's compliance with this DPA. Skedda may respond by referring Client to materials on the Trust Center or to Skedda's standard responses.

9.3 Audits. The information made available under Sections 9.1 and 9.2 is the default means of auditing Skedda's compliance with this DPA. Client may conduct any further audit, including by inspection, that is reasonably necessary to verify Skedda's compliance with this DPA. Any such audit must: (a) be requested at least 30 days in advance, with a scope, timing

and duration agreed in advance, with neither party unreasonably withholding or delaying agreement; (b) be conducted remotely where practicable, and otherwise during normal business hours without unreasonably disrupting Skedda's operations or compromising the security or confidentiality of other customers' data; (c) be conducted by Client or an independent auditor that is not a Skedda competitor and is bound by confidentiality obligations; and (d) take place no more than once in any 12-month period, unless there are reasonable indications of non-compliance or a supervisory authority requires otherwise. Client will bear its own costs and reimburse Skedda's reasonable costs of any further audit, unless the audit is required by a supervisory authority, follows a Personal Data Breach or reasonable indications of non-compliance, or reveals a material breach of this DPA by Skedda. Audits do not extend to Sub-Processors' facilities; for those, Client will rely on the Sub-Processors' independent audit reports or certifications, which Skedda will make available on request to the extent it is permitted to do so. The procedures in this Section 9 (including notice, scope, conduct, auditor, confidentiality and cost) apply to every audit and information right under this DPA and, where they apply, the SCCs. The parties agree that they are reasonable conditions for audits under Clause 8.9 of the SCCs.

9.4 Confidentiality of Results. All information made available under this Section 9, including audit results, is Skedda's Confidential Information. Client may use it only to assess Skedda's compliance with this DPA and to meet Client's own regulatory obligations, and may share it with a competent supervisory authority on request, and with its professional advisers and auditors who are bound by confidentiality obligations.

## 10. Return and Deletion of Personal Data

Client may export and delete Personal Data at any time before the Agreement ends using the Services' features, as described in the Documentation. Making Personal Data available through the Services' standard export functionality is how Skedda returns Personal Data, and Client is responsible for exporting any Personal Data it wishes to keep before the Agreement ends. Skedda is not required to provide access to the Services, exports or migration assistance after the Agreement ends, but may agree to do so for a reasonable fee. After the Agreement ends, Skedda will delete Personal Data in accordance with the retention periods described in the Documentation and the Privacy Policy, or sooner if Client asks. On Client's written request after deletion is complete, Skedda will provide written confirmation of deletion. Skedda may retain Personal Data where applicable law requires it

or where retention is necessary to resolve a dispute between the parties. Copies in backups and system logs are removed under Skedda's documented routine schedules; until then they remain protected under this DPA and are used only for restoration and security purposes.

## 11. Liability

Nothing in this DPA or the Agreement limits either party's liability to the extent a limitation is prohibited by the SCCs, the UK Addendum or applicable law. Subject to that, each party's total liability arising out of or relating to this DPA, the SCCs and the UK Addendum, whether in contract, tort or any other theory, is subject to the limitations and exclusions of liability in the Agreement, and counts toward, and does not add to, that party's aggregate liability under the Agreement.

## 12. General

12.1 Term. This DPA remains in effect for as long as Skedda Processes Personal Data on Client's behalf under the Agreement, and then terminates automatically.

12.2 Cost of Assistance. Except where Data Protection Laws prohibit it, Skedda may charge Client its reasonable costs for assistance under Sections 4.6, 5 and 9 that goes beyond the Services' self-service features and the materials available on the Trust Center.

12.3 Governing Law. This DPA is governed by the law that governs the Agreement, except where the SCCs or Data Protection Laws require otherwise.

12.4 Updates. Updates to Skedda's published DPA apply prospectively: to DPAs signed after the update and, where this DPA applies automatically, as the Agreement provides. A signed DPA may be amended only by written agreement of the parties, except to the extent a change is required by applicable law, in which case Skedda will give Client at least 30 days' notice where practicable. No update will modify the SCCs or the UK Addendum.

12.5 Prior DPAs. If the parties have signed an earlier data processing addendum for the Services, that addendum continues to govern the Agreement to which it relates unless the parties agree in writing to replace it with this DPA.

12.6 Notices. Skedda will send notices under this DPA to the Client Notification Email Address in the Agreement or, if the Agreement does not specify one, to the primary contact email address associated with the Client Account (or another address Client designates in writing). Client will send notices under this DPA to dpo@skedda.com.

12.7 Severability; Counterparts. If any provision of this DPA is held invalid or unenforceable, the remaining provisions remain in effect. This DPA may be executed electronically and in counterparts.

Except where the Agreement provides that this DPA applies automatically, this DPA takes effect only when signed by both parties' authorized representatives.

**SKEDDA, INC.**

**CLIENT**

**Signature:**

---

**Name: Mark Gentry**

**Title: Chief Executive Officer**

**Date:**

**Signature:**

---

**Name:**

**Title:**

**Date:**

**Client legal entity name:**

---

# Annex 1 – Details of Processing

## A. List of Parties

Data exporter: Client, as identified in the Agreement. Contact details are those in the Agreement or the Client Account. Role: Controller (or Processor on behalf of a third-party Controller).

Data importer: Skedda, Inc., PMB 2510, 3839 McKinney Ave., Suite 155, Dallas, TX 75204, USA. Contact: Skedda Data Protection Officer, dpo@skedda.com. Role: Processor (or Sub-Processor).

Activities: Processing of Personal Data in connection with Client's use of the Services under the Agreement.

EU and UK representatives: Skedda's representatives under Article 27 of the GDPR and the UK GDPR are identified in Skedda's Privacy Policy (<https://support.skedda.com/legal/privacy-policy-for-venues>).

## B. Description of Processing and Transfer

Categories of Data Subjects: Users of the Client Account, such as Client's employees, contractors, members, customers and guests, and any other individuals whose Personal Data Client or its Users submit to the Services, such as visitors or attendees named in a booking. These may include minors, where Client's use of the Services involves them.

Categories of Personal Data: Identification and contact data (such as name, email address, telephone number and organization); account data (such as login credentials, external-service authentication identifiers and profile photo); booking and usage data (such as resources booked, dates, times, attendees and check-ins); technical data (such as IP address, browser and device information); payment and transaction records (such as amounts, dates and payment status; full payment-card details are collected by the payment provider and not stored by Skedda); and any Personal Data Client or its Users include in free-text fields such as booking notes.

Sensitive data: None intended. Client may not submit Sensitive Personal Information (or, where the Agreement does not define that term, special categories of personal data) unless

the Agreement expressly permits it (Section 3.3). Any such data submitted in breach of that prohibition, for example in free-text fields, remains protected under this DPA, and Client is responsible for removing it.

Frequency of transfer: Continuous, for the duration of the Agreement.

Nature of the Processing: Collection, storage, organization, structuring, retrieval, use, disclosure by transmission, restriction, erasure and other Processing necessary to host, operate, secure, support and improve the Services.

Purpose of the Processing: Providing the Services to Client under the Agreement, and as further instructed by Client through its use and configuration of the Services.

Retention: For the duration of the Agreement, subject to Client's retention settings and to Section 10 of this DPA.

Transfers to Sub-Processors: As described in the Sub-Processor List. Each Sub-Processor Processes Personal Data for the function stated there, for the duration of the Agreement.

## C. Competent Supervisory Authority

The competent supervisory authority is determined as follows. Where Client is established in an EU Member State, it is the supervisory authority of that Member State. Where Client is not established in the EU but falls within Article 3(2) of the GDPR and has appointed an Article 27 representative, it is the supervisory authority of the Member State where that representative is established. Otherwise, it is the Irish Data Protection Commission. For the UK GDPR, it is the UK Information Commissioner's Office. For the FADP, it is the Swiss Federal Data Protection and Information Commissioner.

## Annex 2 – Technical and Organizational Security Measures

This Annex describes the minimum Security Measures in effect as of the version date of this DPA. Skedda may update them under Section 4.4. The Security Measures are independently audited as described in Section 9.1. More detail, including Skedda's audit reports and security policies, is available on the Trust Center (<https://trust.skedda.com>).

Governance and policies. Skedda maintains a documented information security program with designated security and compliance responsibility, including written policies on access control, cryptography, data management, asset management, physical security, human-resources security, incident response, and business continuity and disaster recovery. Security risks are assessed periodically as part of that program.

Hosting and physical security. The Services are hosted with cloud infrastructure providers whose data centers are independently audited (for example, against SOC 2 Type II and ISO/IEC 27001). Skedda does not operate its own data centers. Production environments are logically separated from Skedda's corporate systems.

Tenant isolation. Client Data is stored in multi-tenant systems and is logically separated by customer. Application-level authorization checks are designed to ensure that Users can access only the data and features permitted for their account and role. Users have no direct access to the underlying infrastructure.

Access control. Access to production systems and Client Data is limited to authorized personnel on a least-privilege, role basis and requires multi-factor authentication for privileged access. Access rights are reviewed periodically and removed promptly as part of Skedda's offboarding process. Skedda support personnel access Client Accounts only where needed to provide support, through a time-limited, multi-factor-authenticated and logged process.

Encryption. Data is encrypted in transit over public networks using TLS 1.2 or higher, and encrypted at rest using AES-256 or an equivalent industry-standard algorithm. User passwords are stored using industry-standard salted hashing.

Network and application security. Network access controls, including security groups and firewall rules, restrict traffic to required services and protocols, and a web application firewall protects public endpoints. The Services use rate limiting on key endpoints. Code changes are subject to code review and automated code analysis.

Vulnerability management and testing. Skedda maintains a vulnerability management program and remediates identified vulnerabilities on risk-based timelines. A qualified independent third party performs penetration testing of the Services' application and infrastructure layers at least annually.

Logging, monitoring and incident response. System, security and access logs are collected centrally, with automated alerting on anomalous activity. Skedda maintains and regularly tests a documented incident response plan, and records, investigates and remediates security incidents.

Availability and resilience. Client Data is replicated across multiple availability zones and backed up regularly. Skedda maintains and regularly tests business continuity and disaster recovery plans.

Personnel. Personnel sign confidentiality agreements and complete security awareness training on hire and periodically after that. Background checks are conducted where local law permits.

Vendor management. Sub-Processors are assessed for security and privacy before engagement and periodically after that, and are bound by written data protection terms.

Client-configurable controls. Depending on Client's plan, the Services let Client manage User roles and permissions, enable single sign-on, configure data-retention settings, and export or delete Client Data.

## Annex 3 – Sub-Processors

Skedda's current Sub-Processors, including each one's function and location, are listed on the Sub-Processor List at <https://trust.skedda.com/subprocessors>. The list forms part of this DPA and is updated in accordance with Section 6. Skedda subscribes Client's notice address to change notices as described in Section 6.3; Client can add other addresses through the Trust Center or by email to [dpo@skedda.com](mailto:dpo@skedda.com).