Company Customer DPA

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is between Company and Customer. This DPA amends and forms part of the Agreement. This DPA applies where Company Processes Customer Personal Data as a Processor on behalf of Customer, the Controller, in connection with providing the Services. This DPA will be effective as of the effective date of the Agreement. This DPA will terminate automatically upon termination of the Agreement or as earlier terminated pursuant to the terms of this DPA. Capitalized terms not defined in this DPA will have the meaning given those terms in the Agreement.

1. DATA PROCESSING AND PROTECTION

1.1. **Limitations on Use.** Company will Process Customer Personal Data for the Purpose and otherwise only: (a) pursuant to Customer's documented instructions as specified under Section 1.2 (Instructions), including with regard to transfers of Customer Personal Data to a third country; and (b) as otherwise required by applicable laws, provided that Company will inform Customer (unless prohibited by law) of the applicable legal requirement before such Processing. Company will not otherwise: (x) retain, use, or disclose the Customer Personal Data (i) outside of the direct business relationship between the parties or (ii) for any purpose other than for the Purpose; (y) sell or share (as defined by Data Protection Law) the Customer Personal Data; or (z) combine Customer Personal Data with Personal Data Company receives from individuals or other sources, except as permitted by Data Protection Law.

1.2. **Instructions**. Customer instructs Company to Process Customer Personal Data as necessary to provide the Services and as otherwise authorized or permitted under this DPA and the Agreement, including as specified in Attachment 2 (Scope of Processing). This DPA, the Agreement, and any instructions provided by Customer through configuration tools made available by Company are Customer's documented instructions regarding Company's Processing of Customer Personal Data. Additional instructions provided by Customer (if any) require prior written agreement by Customer and Company. Customer will not instruct Company to Process Customer Personal Data in violation of any Data Protection Law. Company may suspend Processing based upon any Customer instructions that Company reasonably suspects violate Data Protection Law, provided Company will promptly inform Customer if Company believes an instruction infringes Data Protection Law.

1.3. **Compliance.** Each party will comply with its obligations under Data Protection Law. Company shall promptly notify Customer if it determines that it cannot meet its obligations under Data Protection Law. Upon receiving written notice from Customer that Company has Processed Customer Personal Data without authorization, Company will take reasonable and appropriate steps to stop and remediate such Processing.

1.4. **Confidentiality.** Company will ensure that persons authorized by Company to Process any Customer Personal Data are subject to appropriate confidentiality obligations.

1.5. **Security.** Company will implement and maintain appropriate technical and organizational measures designed to protect Customer Personal Data against Security Incidents and provide the level of protection required by Data Protection Law in accordance with Attachment 3 (Data Security Exhibit). Company may amend the technical and organizational measures, provided the new measures do not reduce the level of security provided by Attachment 3 (Data Security Exhibit).

1.6. **Disposal.** At the choice of Customer, Company will (or will enable Customer via the Services to) delete (and will delete existing copies of) all Customer Personal Data after termination of the Agreement (unless Data Protection Law requires the storage of such Customer Personal Data by Company, in which case Company will only further retain and Process such Customer Personal Data for the limited duration and purposes required by such Data Protection Law). The certification of deletion contemplated by Section 8.5 of the SCCs shall be provided on Customers' written request.

1.7. **Deidentified Data**. Company may Process Deidentified Data to improve the Services. Company will (a) take reasonable measures to ensure the Deidentified Data cannot be associated with an individual and (b) publicly commit to maintain and use Deidentified Data in deidentified form and not attempt to reidentify Deidentified Data except as permitted by Data Protection Law.

2. DATA PROCESSING ASSISTANCE

2.1. **Data Subject Rights Assistance**. Customer shall be responsible for responding to requests from individuals to exercise rights under Data Protection Law relating to Customer Personal Data (each a "**Data Subject Request**"). Customer will inform Company of any Data Subject Request to which Company must comply and provide the information necessary for Company to comply with the request. Company will, to the extent permitted by Data Protection Law, notify Customer if Company receives a Data Subject Request. To the extent Customer, in its use of the Services, does not have the ability to address the Data Subject Request, Company will, on Customer's request, provide commercially reasonable assistance to Customer in responding to such Data Subject Request, to the extent the response to such Data Subject Request is required under Data Protection Law.

2.2. **Security Assistance.** Taking into account the nature of Processing and the information available to Company, Company will provide commercially reasonable efforts to assist Customer in Customer's efforts to comply with Customer's obligations to secure Customer Personal Data by providing the information and assistance described in Section 3 (Audits).

2.3. **Security Incident Notice and Assistance.** Company will notify Customer without undue delay after becoming aware of a Security Incident. Company will further take commercially reasonable steps to mitigate the effects and minimize any impact from the Security Incident and assist Customer in complying with any related notification obligations under Data Protection Law.

2.4. **Data Protection Impact Assessment ("DPIA") and Prior Consultation Assistance**. Taking into account the nature of Processing and the information available to Company, Company will provide commercially reasonable assistance to Customer in ensuring compliance with the obligations related to DPIAs and consulting with regulatory authorities.

3. AUDITS

3.1. **Company Audits**. Company may procure audits by third parties to assess Company's adherence to the following standards or requirements: (a) SOC 2 Type II; (b) ISO 27001; (c) PCI DSS Service Provider Level 1; and/or (d) certifications or other documentation evidencing compliance with alternative standards that are substantially equivalent to the foregoing (collectively, "**Audits**"). Subject to the confidentiality obligations set forth in the Agreement, Company will provide Customer with summaries of Company's then-current Audit reports ("**Reports**") on Customer's request. The Reports will be Company's Confidential Information.

3.2. **Customer Audits.** Customer will exercise its audit rights by first requesting the Reports as described in Section 3.1 (Company Audits). Customer may request additional information or an on-site audit of Company if the Reports do not reasonably demonstrate Company's compliance with this DPA and/or Data Protection Law. Except in the event of a Security Incident or regulatory investigation, Customer will provide no less than 30 days' advance notice of its request for an on-site audit and will cooperate in good faith with Company to schedule any such audit on a mutually agreeable date and time during Company's normal business hours. Any such on-site audit must be conducted by Customer or a nationally recognized independent auditor that has agreed to confidentiality provisions reasonably acceptable to Company. Customer is responsible for ensuring that the audit will comply with Company's applicable on-site policies and procedures and will not unreasonably interfere with Company's business activities. Customer will provide a written summary of any audit findings to Company, and the results of the audit will be Company's Confidential Information.

4. SUBPROCESSORS

4.1. **Appointment of Subprocessors.** Customer authorizes Company to use subcontractors to Process Customer Personal Data in connection with providing the Services (each, a "**Subprocessor**"). Customer specifically consents to Company's appointment of the Subprocessors identified on Attachment 4 (the "**Subprocessor List**").

4.2. **Objection Right for New Subprocessors.**

4.2.1. Company will notify Customer of its intent to update the Subprocessor List at least 15 days prior to engaging a new Subprocessor. Customer may object to Company's use of a new Subprocessor within 10 days of receiving such notice by sending an e-mail to hello@beambell.com clearly indicating its desire to object to any such change.

4.2.2. If Customer objects to the change in Subprocessors, Company and Customer will cooperate in good faith to resolve Customer's objection. If the parties are unable to resolve Customer's objection within 10 days, then either party may terminate the Agreement only with respect to those Services that Company indicates cannot be provided without the objected-to Subprocessor.

4.3. **Liability.** Company will impose data protection obligations upon any Subprocessor that are no less protective of Customer Personal Data than those included in this DPA. Company will be liable to Customer for any breach of such obligations by its Subprocessors as it would for its own acts and omissions.

5. DATA TRANSFERS

5.1. **Overview.** The parties will conduct any transfers of European Economic Area, the UK, and Swiss residents' Customer Personal Data to a country not subject to an adequacy decision (a "**Data Transfer**") pursuant to the SCCs, which are incorporated and deemed executed by this reference. If Company notifies Customer that Data Transfers can be conducted in compliance with Data Protection Law pursuant to an alternative transfer mechanism such as the Data Privacy Framework, the parties will rely on the alternative mechanism to legitimize Data Transfers instead of the provisions that follow.

5.2. **SCCs.** The parties agree to comply with the general clauses and with Module 2 (Controller to Processor) of the SCCs with Customer as the "data exporter" and Company as the "data importer."

5.3. **Transfers Subject to Swiss Data Protection Law.** If any Customer Personal Data subject to the Swiss Federal Act on Data Protection of September 25, 2020 (the "**FADP**") is subject to a Data Transfer, the parties will conduct such transfer pursuant to the SCCs with the following modifications: the competent supervisory authority in Annex I.C under Clause 13 shall be the Federal Data Protection and Information Commissioner; references to a "Member State" and "EU Member State" will not prevent individuals in Switzerland from suing for their rights in Switzerland; and references to "GDPR" in the SCCs will be understood as references to the FADP.

5.4. **Transfers Subject to the UK GDPR.** Any Customer Personal Data that is subject to the UK GDPR and a Data Transfer will be subject to the UK IDTA, which is incorporated and deemed executed by this reference.

6. LIMITATION OF LIABILITY

Each party's and all of its affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the limitation of liability in the Agreement. Nothing in this Section 6 is intended to restrict the rights of individuals under Data Protection Law.

7. MISCELLANEOUS

To the extent there is any conflict between the terms of this DPA, on the one hand, and the applicable SCCs or the UK IDTA, on the other hand, the SCCs or the UK IDTA, as appropriate, will control. Except as specifically amended and modified by this DPA, the terms and provisions of the Agreement remain unchanged and in full force and effect. Except as expressly stated in the SCCs and the UK IDTA, the governing law and forum selection provisions of the Agreement will apply to any disputes arising out of this DPA. No supplement, modification, or amendment of this DPA will be binding unless executed in writing by each party to this DPA.

Attachment 1: Definitions

For purposes of this DPA, the following terms will have the meaning ascribed below:

"**CCPA**" means the California Consumer Privacy Act of 2018, including (a) as amended by the California Privacy Rights Act of 2020 or otherwise and (b) any regulations promulgated thereunder.

"**Controller**" means "controller" and "business" (and analogous variations of such terms) under Data Protection Law.

"**Customer Personal Data**" means Personal Data that Company Processes on behalf of Customer in connection with providing the Services as described in Attachment 2.

"**Data Protection Law**" means the GDPR, the UK GDPR, the FADP, the CCPA, the Colorado Privacy Act, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring, the Virginia Consumer Data Protection Act, the Utah Consumer Privacy Act, and any other state, federal, or international data protection or privacy laws that apply to Company's Processing of Customer Personal Data.

"**Deidentified Data**" means information that cannot reasonably be linked to or associated with Customer or any Data Subject.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**Personal Data**" means "personal data" and "personal information" (and analogous variations of such terms) under Data Protection Law.

"**Process**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, extending further to such operation or operations under Data Protection Law.

"**Processor**" means "processor" and "service provider" (and analogous variations of such terms) under Data Protection Law.

"**Purpose**" means to provide, maintain, secure, and improve the Services.

"**SCCs**" means Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on SCCs for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance), available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914, as may be replaced or superseded by the European Commission. The parties make the following choices for implementing the SCCs:

- In Clause 7, the optional docking clause will apply.
- The audits contemplated by Section 8.9 shall be conducted according to the audit provisions of this DPA.
- In Clause 9, Option 2 will apply and the time period for notice of Subprocessor changes will be as set forth in this DPA.
- In Clause 11 the optional language will not apply to the SCCs or the UK IDTA.

- In Clause 17, the SCCs shall be governed by the laws of Ireland.
- In Clause 18(b), the parties agree to resolve disputes arising from the SCCs in the courts of Ireland.
- The information needed to complete Annex I of the SCCs is included in Attachment 2 to this DPA.
- The information needed to complete Annex II of the SCCs is included in Attachment 3 to this DPA.
- The information needed to complete Annex III of the SCCs is included in Attachment 4 to this DPA.

"**Security Incident**" means "personal data breach" and "security incident" (and analogous variations of such terms) under Data Protection Law.

"**Services**" means the services provided by Company pursuant to the Agreement.

"**UK GDPR**" means the GDPR as incorporated into the United Kingdom law by the Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 (each as amended, superseded, or replaced).

"**UK IDTA**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022, available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf. Neither party can terminate the UK IDTA pursuant to Table 4 and Section 19 thereof without the written consent of the other.

Attachment 2 - Scope of Processing

Data exporter

Customer

Data importer

Company

Subject-Matter and Duration of Processing

Company Processes Customer Personal Data in the course of providing the Services in accordance with the Agreement and until the Agreement terminates or expires.

Nature and Purpose of Processing

Company will Process Customer Personal Data in connection with and for the purpose of providing the Services to Customer pursuant to the Agreement. Specifically, the Customer Personal Data will be subject to storage and analysis, among other Processing activities.

Types of Customer Personal Data

Customer Personal Data may include, but is not limited to, the names, contact information, payment information, transactional and other information obtained from Customer's customer relationship management tool(s), and information derived from call transcripts.

Categories of Data Subjects

The data subjects will include Customer's clients or potential clients and Customer's employees, contractors, and other personnel.

Special Categories of Data (as applicable)

Company does not anticipate that Customer will submit special categories to the Services.

Frequency of Transfers

Company will import Customer Personal Data on a continuous basis.

Period of Data Retention

Company will retain the Personal Data until the termination of the Agreement, unless otherwise agreed to by the parties.

Attachment 3 - Data Security Exhibit

1. Program. Company will implement and maintain an information security program containing administrative, technical, and organizational safeguards that meet or exceed requirements under Data Protection Law.
2. Access Controls. Company will: (a) abide by the "principle of least privilege," pursuant to which Company will permit access to Personal Data by its personnel solely on a need-to-know basis; and (b) promptly terminate its personnel's access to Personal Data when such access is no longer required for performance under the Agreement.
3. Account Management. Company will effectively manage the creation, use, and deletion of all account credentials used to access the Company systems, including by implementing: (a) a segregated account with unique credentials for each User; and (b) strict management of administrative accounts.
4. Vulnerability Management. Company will: (a) use automated vulnerability scanning tools to scan its systems; (b) log vulnerability scan reports; (c) use patch management and software update tools for the Company systems; and (d) prioritize and remediate vulnerabilities by severity.
5. Security Segmentation. Company will monitor, detect and restrict the flow of information on a multilayered basis within its systems using tools such as firewalls, proxies, and network-based intrusion detection systems.
6. Data Loss Prevention. Company will use data loss prevention measures designed to identify, monitor and protect Personal Data in use, in transit, and at rest. Such data loss prevention processes and tools will include: (a) automated tools to identify attempts of data exfiltration; and (b) the secure and managed use of portable devices.
7. Encryption. Company will encrypt, using industry standard encryption tools, all Personal Data that Company: (a) transmits or sends wirelessly across public networks or within the Company systems; and (b) stores on laptops, portable devices or otherwise within the Company systems. Company will safeguard the security and confidentiality of all encryption keys associated with encrypted Personal Data.
8. Physical Safeguards. Company will maintain physical access controls designed to secure its systems.

Attachment 4 - Subprocessor List

Subprocessor Name	Services Performed
Twilio	Telephony and call routing
Deepgram	Speech-to-text transcription
Google (Gemini)	AI language model for response generation
ElevenLabs	Text-to-speech voice generation
Phorest	Salon management integration
Meevo	Salon management integration
Supabase	Database storage
Vercel	Web application hosting
Microsoft Azure	Cloud hosting for AI agents