

Murmurly Data Processing Addendum

Effective date: 23 september 2026 · Version 1.0

This Data Processing Addendum (“**DPA**”) forms part of the Agreement between Murmurly B.V. (“**Murmurly**”) and Customer.

Murmurly and Customer are each a “**Party**” and together the “**Parties**”.

1. Definitions

For purposes of this DPA:

“**Agreement**” means the agreement between Murmurly and Customer governing Customer’s access to and use of the Services, including the applicable General Terms and Conditions, Subscription Agreement, this DPA and any other documents expressly incorporated into the contractual relationship between Murmurly and Customer.

“**Customer**” means the business, organization or other person acting in the course of a business or professional activity that has entered into the Agreement with Murmurly.

“**Murmurly**” means Murmurly B.V., a private company with limited liability incorporated under the laws of the Netherlands, having its registered office in Alkmaar, the Netherlands, registered with the Dutch Chamber of Commerce under number 42165731

“**AI Features**” means artificial intelligence and machine learning functionality made available through the Services, including conversational AI, generative text functionality, automated summarisation, content and template generation, information extraction, semantic search, voice functionality and AI-assisted actions.

“**Applicable Data Protection Law**” means all laws and regulations relating to privacy, data protection or the Processing of Personal Data that apply to the Processing of Customer Personal Data under the Agreement, including, where applicable, the General Data Protection Regulation (EU) 2016/679 (“**GDPR**”), applicable implementing or supplementary laws of the European Economic Area, and applicable United States federal and state privacy laws.

“**Customer Personal Data**” means Personal Data Processed by Murmurly on behalf of Customer in connection with the Services, including Personal Data submitted to, stored in, generated through, or otherwise Processed by the Services on Customer’s behalf.

“**Data Subject**” means an identified or identifiable natural person to whom Personal Data relates.

“Optional Integration” means a third-party integration or connection that Customer may independently elect to activate through the Services and that is not required for Murmurly to provide the core Services.

“Personal Data”, “Processing”, “Controller”, “Processor” and “Personal Data Breach” shall have the meanings given to those terms under Applicable Data Protection Law.

“Services” means the software, platform, features, integrations, AI functionality and related services provided by Murmurly to Customer under the Agreement.

“Sub-processor” means any third party engaged by Murmurly to Process Customer Personal Data on behalf of Customer.

Capitalised terms used but not defined in this DPA have the meanings given to them in the Agreement.

2. Scope and Roles

2.1 In respect of Customer Personal Data Processed by Murmurly on behalf of Customer in connection with the Services, Customer acts as the Controller and Murmurly acts as the Processor, or each Party acts in the equivalent role under Applicable Data Protection Law. Any jurisdiction-specific terms applicable to such roles shall apply as set out in this DPA.

2.2 The subject matter, duration, nature and purposes of the Processing, the categories of Personal Data and the categories of Data Subjects are described in Schedule 1.

2.3 Murmurly shall Process Customer Personal Data only on documented instructions from Customer, including as set out in the Agreement, this DPA and Customer's use and configuration of the Services, unless Murmurly is required to Process such Customer Personal Data by applicable law to which Murmurly is subject.

Where Applicable Data Protection Law requires Murmurly to do so, Murmurly shall inform Customer of such legal requirement before the Processing, unless the applicable law prohibits such information on important grounds of public interest.

2.4 Customer's documented instructions include, to the extent applicable:

- a. Customer's use and configuration of the Services and Workspace;
- b. Customer's configuration and use of AI Features;
- c. Customer's activation and use of Optional Integrations;
- d. requests for support, troubleshooting or other Services made by or on behalf of Customer;
- and e. other written instructions provided by Customer and accepted by Murmurly,

in each case to the extent necessary to provide the Services in accordance with the Agreement and this DPA.

2.5 If Murmurly reasonably believes that an instruction from Customer infringes Applicable Data Protection Law, Murmurly shall inform Customer without undue delay. Where required by Applicable Data Protection Law, including Article 28(3) GDPR, Murmurly shall provide such information immediately. Murmurly may suspend the affected Processing to the extent reasonably necessary while the Parties seek to resolve the matter.

2.6 To the extent Murmurly Processes Personal Data for purposes for which Murmurly independently determines the purposes and means of Processing, including account administration, billing, security, fraud prevention, service integrity or compliance with Murmurly's own legal obligations, Murmurly acts as an independent Controller in respect of that Processing. Such Personal Data is not Customer Personal Data for purposes of this DPA, and Murmurly shall Process it in accordance with Applicable Data Protection Law and its applicable Privacy Policy.

3. Customer Responsibilities

3.1 Customer is responsible for determining the purposes of the Processing of Customer Personal Data and for ensuring that its collection, use, disclosure and other Processing of Customer Personal Data through the Services complies with Applicable Data Protection Law, including establishing any legal basis or other authority required for such Processing.

3.2 Customer is responsible for providing any notices to Data Subjects and obtaining any consents, permissions or other authorisations required under Applicable Data Protection Law in connection with Customer's use of the Services and Murmurly's Processing of Customer Personal Data on Customer's behalf.

3.3 Customer is responsible for the Customer Personal Data it submits to, imports into or otherwise makes available through the Services, including Personal Data entered into custom fields, notes, event records, contact records, communications and other Customer-configured areas of the Services. Customer shall ensure that it has the rights and authority necessary to provide such Customer Personal Data to Murmurly for Processing in accordance with the Agreement and this DPA.

3.4 Customer shall not instruct Murmurly to Process Customer Personal Data in a manner that violates Applicable Data Protection Law.

3.5 The Services are not specifically designed for the Processing of special categories of Personal Data under Article 9 GDPR or other sensitive Personal Data subject to heightened protection under Applicable Data Protection Law. Where Customer chooses to Process such data through the Services, Customer is responsible for determining whether such

Processing is permitted and for satisfying any applicable legal basis, consent, notice, security or other requirements.

3.6 Customer is responsible for configuring and using the Services, including AI Features and Optional Integrations, in accordance with Applicable Data Protection Law and Customer's own legal, regulatory and internal requirements.

4. Murmurly's Obligations

4.1 Murmurly shall:

- a. Process Customer Personal Data only in accordance with Section 2 of this DPA and Customer's documented instructions;
- b. ensure that persons authorised to Process Customer Personal Data have committed themselves to confidentiality or are subject to an appropriate statutory obligation of confidentiality;
- c. implement and maintain appropriate technical and organizational measures required under Applicable Data Protection Law to protect Customer Personal Data, taking into account the nature, scope, context and purposes of the Processing and the risks to the rights and freedoms of Data Subjects, as further described in Schedule 2;
- d. taking into account the nature of the Processing, assist Customer by appropriate technical and organizational measures, insofar as this is possible, in fulfilling Customer's obligations to respond to requests from Data Subjects exercising their rights under Applicable Data Protection Law;
- e. assist Customer in ensuring compliance with applicable obligations relating to security of Processing, Personal Data Breaches, data protection impact assessments and prior consultations with supervisory authorities, taking into account the nature of the Processing and the information available to Murmurly;
- f. maintain records and documentation concerning its Processing activities to the extent required by Applicable Data Protection Law; and
- g. make available to Customer information necessary to demonstrate Murmurly's compliance with its obligations as a Processor under Applicable Data Protection Law and this DPA, and allow for and contribute to audits in accordance with Section 11.

4.2 The assistance obligations under Sections 4.1(d) and 4.1(e) apply to the extent required by Applicable Data Protection Law and do not transfer to Murmurly any responsibility that Applicable Data Protection Law places on Customer in its capacity as Controller or equivalent role.

4.3 Where assistance requested by Customer under this Section 4 requires substantial additional work beyond the ordinary functionality of the Services or Murmurly's ordinary compliance activities, Murmurly may charge Customer its reasonable costs for such additional assistance, to the extent permitted by Applicable Data Protection Law, provided that Murmurly informs Customer of such costs in advance.

5. Confidentiality

5.1 Murmurly shall treat Customer Personal Data as confidential and shall not disclose Customer Personal Data to any third party except:

- a. in accordance with Customer's documented instructions, the Agreement or this DPA;
- b. to an authorised Sub-processor to the extent necessary for the provision of the Services;
- c. where Customer has otherwise authorised the disclosure; or
- d. where disclosure is required by applicable law, a binding court order or a competent governmental or regulatory authority, subject to any applicable notification obligations under Section 2.3.

5.2 Murmurly shall ensure that persons authorised to Process Customer Personal Data are subject to appropriate confidentiality obligations.

5.3 The confidentiality obligations under this Section 5 shall survive expiration or termination of the Agreement for so long as Murmurly retains Customer Personal Data.

6. Sub-processors

6.1 Customer provides Murmurly with general written authorisation to engage Sub-processors to Process Customer Personal Data on Customer's behalf in connection with the Services, subject to this Section 6 and Applicable Data Protection Law. Customer authorises the Sub-processors identified on the Sub-processor List as of the effective date of the Agreement.

6.2 Murmurly shall enter into a written agreement or other binding arrangement with each Sub-processor that imposes, in substance, the same data protection obligations as those applicable to Murmurly under this DPA, to the extent relevant to the Processing performed by that Sub-processor, including obligations to implement appropriate technical and organizational measures.

6.3 Murmurly shall remain responsible to Customer for the performance of the applicable data protection obligations of its Sub-processors to the extent required by Applicable Data Protection Law.

6.4 Murmurly shall maintain an up-to-date list of its Sub-processors at <https://murmurly.io/subprocessors> (the "Sub-processor List"). The Sub-processor List shall identify each Sub-processor and provide information concerning its processing location and the nature and purpose of the Processing it performs. Upon Customer's reasonable request, Murmurly shall provide additional information reasonably necessary for Customer to assess the relevant Sub-processor's data protection safeguards, subject to appropriate confidentiality restrictions.

6.5 Murmurly may appoint new Sub-processors or replace existing Sub-processors from time to time. Murmurly shall notify Customer in writing of any intended addition or replacement at least fourteen (14) days before the relevant Sub-processor is authorised to Process Customer Personal Data, thereby giving Customer an opportunity to object before such Processing begins.

6.6 Customer may object to an intended addition or replacement of a Sub-processor on reasonable grounds relating to the protection of Customer Personal Data by notifying Murmurly in writing within fourteen (14) days after receiving the notice under Section 6.5 and providing reasonable details of the grounds for its objection.

6.7 Where Customer objects in accordance with Section 6.6, Murmurly and Customer shall work in good faith to resolve the objection. Murmurly may, where reasonably available:

- a. elect not to use the relevant Sub-processor for Customer;
- b. take reasonable steps to address the grounds for Customer's objection; or
- c. provide a commercially reasonable alternative that avoids the Processing of Customer Personal Data by the relevant Sub-processor.

If no such solution is reasonably available and Murmurly intends to proceed with the relevant Sub-processor, Customer may terminate the affected Services by written notice before the Sub-processor begins Processing Customer Personal Data. Any fees, refunds or other consequences of such termination shall be governed by the Agreement, except to the extent otherwise required by Applicable Data Protection Law.

6.8 Where Customer independently elects to activate an Optional Integration, the third-party provider of that Optional Integration shall be treated as a Sub-processor under this DPA only to the extent that the provider Processes Customer Personal Data on behalf of Murmurly in connection with the Services. To the extent that such provider Processes Personal Data under a direct relationship with Customer or otherwise does not act as a Sub-processor of Murmurly, Customer is responsible for reviewing and complying with the applicable terms and data protection arrangements governing that provider. Customer's activation and use of an Optional Integration constitutes an instruction to Murmurly to enable the data flows reasonably necessary for that integration.

7. International Data Transfers

7.1 Murmurly shall ensure that any international transfer of Customer Personal Data that is subject to transfer restrictions under Applicable Data Protection Law is carried out in accordance with such law and, where required, is subject to a valid transfer mechanism.

7.2 Where Chapter V of the GDPR applies to a transfer of Customer Personal Data by Murmurly to a recipient outside the EEA, Murmurly may rely, as applicable, on:

- a. an adequacy decision adopted by the European Commission;
- b. the European Commission's Standard Contractual Clauses for transfers of Personal Data to third countries adopted by Commission Implementing Decision (EU) 2021/914 (the "SCCs"); or
- c. another lawful transfer mechanism permitted under Applicable Data Protection Law.

7.3 Where Murmurly transfers Customer Personal Data as a Processor to a Sub-processor located outside the EEA and the SCCs are required for that transfer, Murmurly shall enter into the processor-to-processor provisions of the SCCs (Module Three) with the relevant Sub-processor and shall complete the applicable annexes using the information relevant to that transfer.

7.4 Where Applicable Data Protection Law requires additional safeguards or assessments in connection with an international transfer, Murmurly shall implement or undertake such measures to the extent required by that law.

7.5 If a transfer mechanism relied upon by Murmurly is amended, replaced, invalidated or otherwise ceases to provide a lawful basis for the relevant transfer, Murmurly may rely on another valid transfer mechanism permitted under Applicable Data Protection Law without requiring an amendment to this DPA.

7.6 Information regarding the countries or regions in which Sub-processors Process Customer Personal Data and the applicable transfer mechanisms shall be made available through Murmurly's Sub-processor List or otherwise upon Customer's reasonable request.

8. Personal Data Breaches

8.1 Murmurly shall notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data.

8.2 To the extent known and reasonably available to Murmurly, the notification under Section

8.1 shall include:

- a. a description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
- b. the likely consequences of the Personal Data Breach;
- c. the measures taken or proposed to be taken by Murmurly to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects; and
- d. a contact point from which further information can be obtained.

Where it is not possible to provide all such information at the same time, Murmurly may provide the information then available and provide further information in phases as it becomes available, without undue further delay.

8.3 Murmurly shall reasonably cooperate with Customer and provide assistance required under Applicable Data Protection Law in connection with Customer's investigation, assessment, containment and remediation of a Personal Data Breach and Customer's applicable notification or communication obligations, taking into account the nature of the Processing and the information available to Murmurly.

8.4 Customer remains responsible for determining whether a Personal Data Breach must be notified to a supervisory or governmental authority, Data Subjects or any other person, except to the extent Applicable Data Protection Law places such responsibility directly on Murmurly.

8.5 Murmurly shall not notify any supervisory or governmental authority or Data Subject of a Personal Data Breach on Customer's behalf unless Customer instructs Murmurly to do so and Murmurly agrees to such instruction, or unless Murmurly is independently required to make such notification under applicable law.

8.6 Notification or assistance under this Section 8 shall not be construed as an admission by Murmurly of fault or liability.

8.7 Murmurly shall maintain processes for identifying, investigating, containing and remediating security incidents and Personal Data Breaches affecting Customer Personal Data. Security incidents that do not constitute a Personal Data Breach are not subject to the notification obligation under Section 8.1, except to the extent notification is otherwise required by Applicable Data Protection Law.

8.8 Customer shall ensure that it maintains up-to-date contact details for privacy and security notifications under the Agreement. Unless Customer has designated another contact for such notifications, Murmurly may send notifications under this Section 8 to the contact details associated with Customer's account or otherwise designated under the Agreement. Customer may contact Murmurly regarding Personal Data Breaches at legal@murmurly.io.

9. Data Subject Rights

9.1 Taking into account the nature of the Processing, Murmurly shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, in fulfilling Customer's obligations to respond to requests from Data Subjects exercising their rights under Applicable Data Protection Law.

9.2 If Murmurly receives a request directly from a Data Subject relating to Customer Personal Data, Murmurly shall, to the extent reasonably possible, promptly notify Customer and may direct the Data Subject to Customer. Murmurly shall not independently fulfil such request directly with the Data Subject except on Customer's documented instructions and where Murmurly has agreed to do so on Customer's behalf, or where Murmurly is required to do so under applicable law.

9.3 Assistance under this Section 9 may include, as appropriate and taking into account the nature and functionality of the Services:

- a. providing Customer with access to or copies of relevant Customer Personal Data;
- b. correcting or deleting Customer Personal Data;
- c. restricting or otherwise limiting Processing where applicable;

d. facilitating portability of Customer Personal Data where required under Applicable Data Protection Law; and

e. providing information reasonably necessary for Customer to respond to the relevant request.

9.4 Customer remains responsible for determining whether and how a request from a Data Subject should be fulfilled and for responding to the Data Subject within the periods required by Applicable Data Protection Law. Any costs for additional assistance under this Section 9 shall be governed by Section 4.3.

10. Data Retention, Return and Deletion

10.1 Murmurly shall retain Customer Personal Data only for as long as necessary to provide the Services and perform its obligations under the Agreement and this DPA, or as otherwise required or permitted under Applicable Data Protection Law.

10.2 Upon termination or expiration of the Services involving the Processing of Customer Personal Data, Customer may instruct Murmurly to:

a. return the relevant Customer Personal Data to Customer and subsequently delete the Customer Personal Data and existing copies; or

b. delete the relevant Customer Personal Data and existing copies without return, in each case in accordance with this Section 10, except to the extent applicable law requires Murmurly to retain the relevant Customer Personal Data.

10.3 Customer may provide the instruction referred to in Section 10.2 before termination or expiration or during any post-termination data retrieval period made available under the Agreement. Unless Customer instructs Murmurly otherwise, Murmurly may treat deletion in accordance with Section 10.4 as Customer's default instruction.

10.4 Unless an earlier deletion is requested by Customer or required by Applicable Data Protection Law or an applicable EU Data Act Addendum, Murmurly shall make Customer Personal Data available for return or retrieval for up to sixty (60) days following termination or expiration of the applicable Services and shall thereafter delete the Customer Personal Data from its active systems.

10.5 Where Customer elects to receive a return of Customer Personal Data, Murmurly shall provide the relevant Customer Personal Data in a reasonably accessible and commonly used format, taking into account the nature and functionality of the Services. Any additional export or switching rights applicable under an EU Data Act Addendum shall be governed by that addendum.

10.6 Customer Personal Data that remains in backup or disaster recovery systems after deletion from active systems shall remain protected in accordance with this DPA, shall not be restored or otherwise Processed except as necessary for backup restoration, disaster

recovery, security or other legitimate technical purposes, and shall be deleted or overwritten in accordance with Murmurly's applicable backup retention procedures and Applicable Data Protection Law.

10.7 Where applicable law requires Murmurly to retain Customer Personal Data beyond the period otherwise permitted under this Section 10, Murmurly shall retain only the Customer Personal Data required by that law, protect it in accordance with this DPA and Process it only for the purpose for which continued retention is required.

10.8 Upon Customer's reasonable written request, Murmurly shall confirm completion of the deletion required under this Section 10, to the extent required by Applicable Data Protection Law.

11. Audits and Compliance Information

11.1 Upon Customer's reasonable written request, Murmurly shall make available to Customer all information necessary to demonstrate Murmurly's compliance with its obligations as a Processor under Applicable Data Protection Law and this DPA.

11.2 Customer shall, where reasonably appropriate, first review any relevant compliance documentation made available by Murmurly, including independent audit reports, certifications, penetration test summaries or other relevant third-party assurance materials. Where such information does not reasonably enable Customer to verify Murmurly's compliance, or where an audit is otherwise required under Applicable Data Protection Law, Customer may conduct an audit of Murmurly's Processing of Customer Personal Data or appoint an auditor to conduct such audit on its behalf.

11.3 Customer shall provide at least thirty (30) days' prior written notice of an audit, unless a shorter notice period is reasonably necessary due to a Personal Data Breach, a specific requirement of a competent supervisory or governmental authority, reasonable documented grounds to suspect a material breach of this DPA, or where otherwise required by Applicable Data Protection Law.

11.4 Customer may conduct no more than one audit in any twelve-month period, unless an additional audit is:

- a. required by Applicable Data Protection Law or a competent supervisory or governmental authority;
- b. reasonably necessary following a Personal Data Breach affecting Customer Personal Data; or
- c. reasonably necessary based on documented grounds to suspect a material breach by Murmurly of its obligations under this DPA.

11.5 Any audit shall be limited to information, systems, facilities and Processing activities relevant to Customer Personal Data and Murmurly's obligations under this DPA. Audits shall be conducted during normal business hours and in a manner that does not unreasonably

interfere with Murmurly's business operations or compromise the security, confidentiality or rights of Murmurly, its other customers or third parties.

11.6 Where Customer appoints a third-party auditor, Customer shall ensure that the auditor is subject to appropriate confidentiality obligations and complies with reasonable security and access requirements communicated by Murmurly. Customer and its auditor shall not access Customer Personal Data relating to another Murmurly customer or information that Murmurly is legally or contractually prohibited from disclosing.

11.7 Before an audit is conducted, Customer and Murmurly shall establish a reasonable audit plan specifying the scope, timing and method of the audit and the information, systems or facilities to be reviewed. Murmurly may require reasonable safeguards to protect the security and confidentiality of its systems and information, including supervised access and reasonable restrictions on copying, photographing, recording or retaining confidential information. Any such safeguards shall not prevent Customer from exercising an audit or inspection right required under Applicable Data Protection Law.

11.8 Customer shall bear its own costs and expenses associated with an audit. Where an audit requires substantial additional work by Murmurly beyond its ordinary compliance activities, Murmurly may charge Customer its reasonable costs for such additional work, to the extent permitted by Applicable Data Protection Law, provided that Murmurly informs Customer of such costs in advance. Any such costs shall not be disproportionate or have the effect of preventing Customer from exercising a mandatory audit right under Applicable Data Protection Law.

12. Liability

12.1 The exclusions and limitations of liability set out in the Agreement shall apply to all claims arising out of or in connection with this DPA. Any liability arising under or in connection with this DPA shall form part of, and shall not be in addition to, any aggregate liability cap applicable under the Agreement.

12.2 Nothing in this Section 12 shall exclude or limit liability to the extent such liability cannot lawfully be excluded or limited. For clarity, nothing in this Section 12 limits or restricts any rights of Data Subjects or powers of supervisory authorities under Applicable Data Protection Law.

13. AI Features

13.1 Murmurly may make AI Features available as part of the Services. Customer's use of AI Features is subject to the settings, permissions, functionality and configurations made available through the Services and selected or configured by Customer.

13.2 Where Customer's use of AI Features requires Customer Personal Data to be Processed by a third-party AI service provider acting as a Sub-processor of Murmurly, Murmurly may disclose the relevant Customer Personal Data to that provider in accordance with Sections 6 and 7 of this DPA.

13.3 Depending on the AI Feature used and the configuration selected by Customer, Customer Personal Data Processed through an AI Feature may include prompts, messages, notes, contextual information, audio, information retrieved from Customer's Workspace and other Customer Personal Data made available to or through the relevant AI Feature.

13.4 Murmurly configures its third-party AI services, where supported, so that Customer Personal Data submitted through the Services is not used by the applicable AI service provider to train or improve its general-purpose AI models. Murmurly may rely on the contractual commitments, technical controls and configurations made available by the applicable AI service provider in relation to such use.

13.5 Where Customer, through functionality made available by Murmurly, connects to or uses an AI service under Customer's own account or licence, or under a direct contractual relationship between Customer and the relevant AI service provider, the role and responsibilities of that AI service provider shall be determined in accordance with Section

6.8. Customer remains responsible for any direct data protection arrangements applicable between Customer and that provider.

13.6 Customer is responsible for reviewing and evaluating AI-generated or AI-assisted output before relying on or acting upon such output where it concerns or may affect Data Subjects.

13.7 Customer is responsible for determining whether its configuration or use of AI Features involves automated decision-making or profiling subject to specific requirements under Applicable Data Protection Law and, where applicable, for complying with the obligations applicable to Customer in its capacity as Controller or equivalent role.

13.8 Customer remains responsible for determining whether, and on what basis, AI-generated or AI-assisted outputs, recommendations or actions are used in decisions concerning Data Subjects. Murmurly does not independently determine Customer's purposes for such decisions merely by providing the AI Features. Nothing in this Section

13.8 limits Murmurly's obligations under this DPA or Applicable Data Protection Law.

13.9 Murmurly shall apply the technical and organizational measures described in Schedule 2 to Customer Personal Data Processed through AI Features.

14. Governing Law and Jurisdiction

14.1 Unless the Parties expressly agree otherwise in writing, this DPA shall be governed by and construed in accordance with the laws of the Netherlands.

14.2 Unless the Parties expressly agree otherwise in writing, any dispute arising out of or in connection with this DPA shall be submitted to the exclusive jurisdiction of the competent court in Amsterdam, the Netherlands.

14.3 Nothing in Sections 14.1 or 14.2 shall limit any right of a Party or Data Subject, or any power of a supervisory or governmental authority, that cannot lawfully be restricted under Applicable Data Protection Law. Where the SCCs apply, the governing law and jurisdiction provisions of the SCCs shall apply to the extent required by those clauses.

15. Order of Precedence

15.1 In the event of a conflict between this DPA and any other document forming part of the Agreement with respect to the Processing of Customer Personal Data, this DPA shall prevail to the extent of the conflict.

15.2 Notwithstanding Section 15.1, the Parties may expressly agree in writing to modify a specific provision of this DPA, provided that the agreement expressly identifies the provision being modified and any such modification complies with Applicable Data Protection Law.

15.3 Where the SCCs apply to a transfer of Customer Personal Data, the SCCs shall prevail over this DPA and any other document forming part of the Agreement to the extent of any conflict concerning matters governed by the SCCs.

15.4 Where a Schedule or addendum to this DPA contains jurisdiction-specific data protection terms, those terms shall prevail over conflicting provisions of the main body of this DPA solely to the extent necessary to give effect to the Applicable Data Protection Law addressed by that Schedule or addendum.

16. Amendments

16.1 Murmurly may propose amendments to this DPA from time to time where reasonably necessary to reflect changes in the Services, Applicable Data Protection Law, security practices, technical developments or other relevant circumstances. Any amendment that materially changes the rights or obligations of the Parties under this DPA shall require the agreement of the Parties.

16.2 Murmurly shall provide Customer with reasonable prior notice of a proposed material amendment, unless an earlier change is reasonably necessary to comply with Applicable Data Protection Law or a binding requirement of a competent authority. Where Customer's approval is required, such approval may be provided through the execution or acceptance of an updated DPA, Subscription Agreement or other written or electronic mechanism made available by Murmurly.

16.3 Murmurly may make non-material administrative or technical updates to this DPA without Customer's separate approval, including corrections of errors, changes to contact details or URLs, and other changes that do not materially alter the Processing of Customer Personal Data or the rights or obligations of either Party. Murmurly shall make the current version of this DPA available to Customer.

16.4 Changes concerning the addition or replacement of Sub-processors shall be governed by Section 6 and shall not require a separate amendment to this DPA.

16.5 No amendment to this DPA shall reduce the level of protection required by Applicable Data Protection Law or limit any obligation that cannot lawfully be modified by agreement.

17. Notices

17.1 Notices and other communications under this DPA shall be made in writing and may be delivered by email or by another method expressly permitted under the Agreement or this DPA.

17.2 Notices to Murmurly concerning this DPA shall be sent to legal@murmurly.io, unless Murmurly designates another contact address in accordance with this DPA.

17.3 Notices to Customer shall be sent to the contact details or email address designated by Customer under the Agreement or in its Murmurly account. Customer is responsible for keeping such contact details up to date.

17.4 Notices concerning Sub-processors, Personal Data Breaches and amendments to this DPA shall be provided in accordance with Sections 6, 8 and 16 respectively.

17.5 Delivery of a notice under this Section 17 shall not, by itself, constitute Customer's agreement to an amendment or other matter where this DPA expressly requires Customer's agreement or approval.

18. General

18.1 If any provision of this DPA is held to be invalid, illegal or unenforceable, the remaining provisions shall remain in full force and effect. The affected provision shall, to the extent possible, be interpreted or modified only to the minimum extent necessary to make it valid and enforceable while preserving its intended effect.

18.2 No failure or delay by either Party in exercising any right or remedy under this DPA shall constitute a waiver of that right or remedy, nor shall any single or partial exercise of a right or remedy prevent its further exercise.

18.3 This DPA forms part of the Agreement and shall remain effective for so long as Murmurly Processes Customer Personal Data on behalf of Customer, including after expiration or termination of the Agreement to the extent Murmurly continues to retain or Process Customer Personal Data in accordance with this DPA.

18.4 The Schedules to this DPA form an integral part of this DPA.

Schedule 1 — Processing Details

1. Subject Matter

The Processing of Customer Personal Data by Murmurly on behalf of Customer in connection with the provision of the Services, including event planning and management, contact and company management, invitations and RSVP management, communications, collaboration, task and workflow management, Customer-authorised integrations, AI Features and related support and administrative functionality.

2. Duration

Murmurly shall Process Customer Personal Data on behalf of Customer for the duration of the applicable Services and thereafter only for such period as Customer Personal Data is retained or Processed in accordance with this DPA, including Section 10.

3. Nature and Purposes of the Processing

Depending on Customer's use and configuration of the Services, Murmurly may Process Customer Personal Data on Customer's behalf for the following purposes:

- a. creating, organising and managing events;
- b. creating and maintaining records relating to persons, companies, groups and other Customer-defined information;
- c. sending invitations, emails and other communications at Customer's direction;
- d. collecting and managing invitations, RSVPs, attendance and other event participation information;
- e. creating and managing agendas, notes, comments, tasks, proposals and workflows;
- f. enabling collaboration and access between persons authorised by Customer to use or interact with the Services;
- g. managing Workspace membership, roles, permissions and other Customer-configured access controls;
- h. providing AI Features, including conversational AI, summarisation, content generation, information retrieval, voice functionality and administrative or workflow assistance;
- i. enabling Optional Integrations and other Customer-authorised connections with third-party services;
- j. providing Customer-requested support, troubleshooting and technical assistance;
- k. providing functionality relating to the security, integrity, availability and administration of Customer's Workspace and Customer Personal Data; and

I. otherwise Processing Customer Personal Data in accordance with Customer's documented instructions as described in Sections 2.3 and 2.4 of this DPA.

4. Categories of Data Subjects

Depending on Customer's use of the Services, Data Subjects may include:

- a. Customer's employees, personnel, contractors and other persons authorised by Customer to use or interact with the Services;
- b. Customer's customers, clients, prospects and business contacts;
- c. event attendees, invitees, speakers, hosts, organisers and other event participants;
- d. representatives, employees and other personnel of companies and organizations with which Customer interacts;
- e. Customer's suppliers, partners, service providers and other professional contacts; and
- f. other individuals whose Personal Data Customer chooses to Process through the Services.

5. Categories of Customer Personal Data

Depending on Customer's use and configuration of the Services, Customer Personal Data may include:

- a. identity and contact information, including names, email addresses, telephone numbers and other contact details;
- b. professional and organizational information, including job titles, roles, company affiliations and other business-related information;
- c. event-related information, including invitations, RSVP responses, attendance, participation information, agendas, scheduling information and related event records;
- d. communications and correspondence, including email content and associated information where made available through an Optional Integration or other Customer-authorised functionality;
- e. notes, comments, tasks, proposals, workflow information and other content entered, submitted or generated through the Services;
- f. Customer-defined attributes, custom fields and other information stored in Customer-managed records;
- g. calendar and scheduling information made available through Customer-authorised calendar functionality or integrations;

- h. Personal Data obtained from or made available through Optional Integrations or other third-party services at Customer's direction;
- i. Workspace membership information, user or member identifiers, roles, permissions and other Customer-configured access information;
- j. AI-related information, including prompts, messages, contextual information, information retrieved from a Workspace, AI-generated or AI-assisted outputs and other information Processed through AI Features;
- k. audio, speech and related information where Customer enables AI-powered voice functionality;
- l. audit, activity, security and technical information to the extent such information is Processed by Murmurly on Customer's behalf in connection with the administration, security or operation of Customer's Workspace; and m. any other Personal Data that Customer chooses to submit to or Process through the Services.

6. Special Categories and Other Sensitive Personal Data

The Services are not specifically designed for the Processing of special categories of Personal Data under Article 9 GDPR or other Personal Data subject to heightened protection under Applicable Data Protection Law.

Where Customer chooses to Process such data through the Services, the Processing shall remain subject to this DPA and Customer shall be responsible for satisfying the requirements described in Section 3.5.

7. Technical, Usage and Operational Data

Technical, usage and operational information generated in connection with the Services may include device and browser information, login timestamps, Workspace and user identifiers, feature and page usage, actions performed within the Services, AI usage information, API activity, error and crash information, audit and security logs and performance information.

To the extent Murmurly Processes such information on Customer's behalf for purposes relating to Customer's Workspace, Customer administration, Customer-requested functionality or Customer Personal Data, such information constitutes Customer Personal Data and is subject to this DPA.

To the extent Murmurly independently determines the purposes and means of Processing such information for its own account administration, billing, fraud prevention, service integrity, security, legal compliance or other purposes described in Section 2.6, Murmurly acts as an independent Controller and such Processing falls outside the scope of this Schedule 1.

8. Customer's Instructions

Customer's documented instructions for the Processing described in this Schedule 1 are set out in Sections 2.3 and 2.4 of this DPA and include the Processing necessary to provide the Services in accordance with the Agreement and Customer's use and configuration of the Services.

Schedule 2 — Technical and Organizational Measures

Murmurly implements and maintains appropriate technical and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Data.

The measures described in this Schedule may be updated from time to time to reflect changes in the Services, technology, security practices and applicable risks, provided that such updates do not materially reduce the overall level of protection of Customer Personal Data during the applicable Services.

1. Access Control

Murmurly implements access controls designed to restrict access to Customer Personal Data to authorised persons and systems.

Such measures include:

- a. Workspace-level role-based access controls and configurable permissions;
- b. access to Customer Personal Data based on Workspace membership, roles and permissions;
- c. authentication mechanisms supported by the Services, including email-based authentication, Passkey, and supported single sign-on mechanisms, where applicable;
- d. support for multi-factor authentication where made available through the Services; and
- e. access controls restricting access to Murmurly's backend and infrastructure systems to authorised personnel.

2. Workspace Isolation

Customer Workspaces are logically segregated from other Customer Workspaces.

Murmurly applies access controls designed to prevent users from accessing Customer Personal Data in a Workspace unless they have been granted the relevant access to that Workspace.

3. Encryption

Murmurly uses encryption to protect Customer Personal Data in transit and at rest, as applicable to the relevant systems and services.

- a. Data transmitted between Customer clients and Murmurly backend services is protected using TLS 1.2 or higher and secure WebSockets (WSS), where applicable.
- b. Customer Personal Data stored within cloud infrastructure used by Murmurly is encrypted at rest using encryption mechanisms provided by the applicable infrastructure provider.
- c. Backups and snapshots containing Customer Personal Data are subject to the applicable encryption mechanisms of the infrastructure provider.

4. Infrastructure and Service Security

Murmurly uses cloud infrastructure and service providers with security controls appropriate to the services they provide.

Murmurly applies technical and organizational measures designed to maintain the confidentiality, integrity and availability of the Services and Customer Personal Data.

Relevant infrastructure and application components are monitored for availability, errors and security-relevant events.

5. Logging and Monitoring

Murmurly maintains technical, operational and security logs as appropriate for the operation, administration and security of the Services.

Such logs may include authentication events, Workspace and administrative activity, security and audit events, API activity, errors, crashes, performance information and information reasonably necessary to investigate security incidents.

Access to security and operational logs is restricted to authorised persons and systems.

6. Vulnerability Management

Murmurly maintains processes designed to identify and address vulnerabilities affecting the software and infrastructure used to provide the Services.

These measures include vulnerability and dependency scanning and appropriate review of identified security issues.

Murmurly may conduct additional security assessments, including penetration testing, where appropriate to the nature, risk and maturity of the Services.

7. Production and Customer Data Access

Access to production systems and Customer Personal Data is restricted to authorised personnel and is permitted only where reasonably necessary for a legitimate purpose related to the provision, maintenance, security or support of the Services.

Such purposes may include troubleshooting, maintenance, security investigations, incident response or Customer-requested support.

Access is subject to appropriate authentication, authorisation and access controls and shall be limited to the extent reasonably necessary for the relevant purpose.

8. Development and Testing

Murmurly does not intentionally use Customer Personal Data for software development or testing purposes except where reasonably necessary for troubleshooting or another authorised purpose and subject to appropriate safeguards.

Production systems are logically separated from development and testing environments as appropriate to the architecture of the Services.

9. Availability, Backup and Recovery

Murmurly uses backup and recovery mechanisms designed to support the availability and recovery of relevant production data and Services following technical failures or other incidents.

Backups are maintained in accordance with the applicable backup, retention and recovery mechanisms of Murmurly's infrastructure providers and are subject to applicable access-control and encryption measures.

Customer Personal Data contained in backups is handled in accordance with Section 10 of this DPA.

10. Incident Response

Murmurly maintains processes for identifying, investigating, assessing, containing and remediating security incidents and Personal Data Breaches.

Such processes include escalation and assessment procedures for determining whether an incident affects Customer Personal Data and whether the notification obligations under Section 8 of this DPA apply.

11. Confidentiality and Personnel

Persons authorised to Process Customer Personal Data on behalf of Murmurly are subject to appropriate confidentiality obligations.

Murmurly takes reasonable measures to ensure that persons with access to Customer Personal Data are informed of their applicable security, confidentiality and privacy responsibilities.

Access is granted based on the relevant person's responsibilities and legitimate need for access.

12. Sub-processor Security

Murmurly assesses relevant third-party service providers that Process Customer Personal Data on Murmurly's behalf and requires contractual and security safeguards in accordance with Section 6 of this DPA and Applicable Data Protection Law.

13. Data Minimisation

Murmurly limits Customer Personal Data disclosed or transmitted to third-party service providers to the information reasonably necessary for the applicable functionality or Processing purpose.

Where Murmurly retrieves information from Optional Integrations or other third-party services for Processing within the Services, Murmurly does not intentionally retain raw source data beyond what is reasonably necessary for the relevant functionality, except where otherwise instructed by Customer or required by applicable law.

14. AI Security

Customer Personal Data Processed through AI Features remains subject to applicable Workspace-level access controls and the other security measures described in this Schedule.

Credentials used by Murmurly to access third-party AI services are protected against unauthorised access and are not intentionally exposed to Customer clients except where a secure, limited-purpose credential or session mechanism is required for the applicable functionality.

Where real-time AI functionality requires a client connection to a third-party AI service, Murmurly uses limited-purpose or short-lived credentials or other access-control mechanisms designed to restrict access to the authorised AI functionality.

15. Security Review

Murmurly periodically reviews the technical and organizational measures relevant to the security of the Services and Customer Personal Data and may update those measures in response to identified risks, vulnerabilities, changes in the Services or developments in security practices.

Schedule 3 — Sub-processors

1. General

Murmurly may engage Sub-processors to Process Customer Personal Data on behalf of Customer in accordance with Section 6 of this DPA.

The Sub-processors authorised as of the effective date of the Agreement are identified below. Certain Sub-processors, services or Processing locations may apply only where Customer enables or receives the functionality for which they are used. Processing locations may also vary depending on Customer's configured deployment region, including where an EU or United States data residency option applies.

Murmurly maintains an up-to-date list of its current Sub-processors, including information concerning their Processing purposes and locations, at <https://murmurly.io/subprocessors> (the "Sub-processor List").

Changes to Murmurly's Sub-processors shall be governed by Section 6 of this DPA.

2. Core Sub-processors

Sub-processor	Purpose of Processing	Categories of Personal Data	Processing Location
Convex	Application backend, database, data storage and processing	Customer Personal Data stored in or processed through the Murmurly platform	EU or United States, depending on Customer's configured deployment region; current location as identified on the Sub-processor List
Amazon Web Services (AWS)	Cloud infrastructure, storage, content delivery, email delivery and related infrastructure services	Customer Personal Data processed through the applicable AWS services, including communications and related delivery information where applicable	EU or United States depending on Customer's configured deployment region and the applicable AWS service; additional service-dependent processing locations may apply as identified on the Sub-processor List
Google Cloud	AI processing, including generative and conversational AI, embeddings, summarisation and real-time speech functionality	Prompts, messages, notes, contextual information, Customer Personal Data made available to AI Features, audio, speech and related data	EU or United States, depending on Customer's configured deployment region and the applicable AI functionality. For EU-configured deployments, server-side text-based AI and embeddings are processed using EU-configured Google Cloud infrastructure. Real-time speech functionality uses a direct client connection to Google Cloud and is not subject to a specific data residency commitment by Murmurly; such Processing may occur outside the EU. Current applicable processing locations and configurations are identified on the Sub-processor List.

3. Optional Integrations

Customer may independently elect to connect the Services to Optional Integrations provided by third parties.

A provider of an Optional Integration is not a Sub-processor solely because Customer chooses to connect or use that integration. To the extent Murmurly engages an Optional Integration provider to Process Customer Personal Data on Murmurly's behalf, that provider

shall be treated as a Sub-processor and shall be subject to Section 6 of this DPA.

Where an Optional Integration provider Processes Personal Data under a direct relationship with Customer or otherwise does not act as a Sub-processor of Murmurly, the Processing by that provider shall be governed by the applicable relationship between Customer and that provider.

Information concerning Optional Integrations currently supported by Murmurly may be made available separately from the Sub-processor List.

Schedule 4 — International Data Transfers

1. Application

International transfers of Customer Personal Data by Murmurly shall be governed by Section 7 of this DPA.

This Schedule 4 provides additional information concerning the implementation of the transfer mechanisms referred to in Section 7.

2. Transfers to Sub-processors

Where Murmurly transfers Customer Personal Data to a Sub-processor in a manner that is subject to international data transfer restrictions under Applicable Data Protection Law, Murmurly shall ensure that an applicable transfer mechanism is in place in accordance with Section 7.

Where the SCCs are required for a transfer by Murmurly as a Processor to a Sub-processor, Murmurly shall enter into the applicable processor-to-processor provisions of the SCCs with the relevant Sub-processor.

3. Transfer Information

Information concerning the countries or regions in which Murmurly's Sub-processors Process Customer Personal Data and, where applicable, the transfer mechanisms relied upon by Murmurly shall be made available through the Sub-processor List or upon Customer's reasonable request.

Where a Sub-processor provides different services or Processing locations depending on Customer's configuration or use of the Services, the applicable Processing locations and transfer arrangements may differ accordingly.

4. Additional Safeguards

Where Applicable Data Protection Law requires Murmurly to assess an international transfer or implement supplementary safeguards in addition to the applicable transfer mechanism, Murmurly shall undertake such assessment and implement such safeguards to the extent

required by Applicable Data Protection Law.

Schedule 5 — United States Privacy Terms

1. Application and Definitions

1.1 This Schedule 5 applies to the Processing of Customer Personal Data to the extent that such Processing is subject to an applicable United States federal or state privacy or data protection law that imposes obligations on a processor, service provider, contractor or equivalent person Processing Personal Data on behalf of another person (“**US Privacy Law**”).

1.2 For purposes of this Schedule 5, references to a “Controller” include a “business” or other equivalent role under applicable US Privacy Law, and references to a “Processor” include a “service provider”, “contractor” or equivalent role, in each case to the extent applicable to the relevant Processing.

1.3 Terms defined under an applicable US Privacy Law shall have the meaning assigned to them by that law where used in relation to Processing subject to that law. In the event of a conflict between definitions under different US Privacy Laws, the definition applicable to the relevant Processing shall apply.

2. Roles and Processing Instructions

2.1 Where Customer determines the purposes and means of Processing Customer Personal Data and Murmurly Processes such Customer Personal Data on Customer’s behalf, Customer acts as the Controller and Murmurly acts as the Processor, or each Party acts in the equivalent role under applicable US Privacy Law.

2.2 Murmurly shall Process Customer Personal Data only in accordance with Customer’s documented instructions and for the purposes described in the Agreement, this DPA and Schedule 1, except as otherwise permitted or required by applicable US Privacy Law.

2.3 Schedule 1 sets out the Processing instructions, nature and purposes of the Processing, categories of Customer Personal Data, categories of Data Subjects and duration of Processing for purposes of applicable US Privacy Laws.

3. General US Processor Obligations

3.1 To the extent required by applicable US Privacy Law, Murmurly shall:

- a. Process Customer Personal Data only on behalf of and in accordance with the documented instructions of Customer;
- b. ensure that persons authorised to Process Customer Personal Data are subject to appropriate confidentiality obligations;

- c. maintain reasonable administrative, technical and organizational safeguards appropriate to the nature of the Customer Personal Data, as further described in Schedule 2;
- d. assist Customer, taking into account the nature of the Processing and the information available to Murmurly, in responding to applicable consumer or Data Subject rights requests;
- e. provide reasonable assistance and information required for Customer to conduct data protection, privacy or other assessments required by applicable US Privacy Law;
- f. at Customer's direction, return or delete Customer Personal Data in accordance with Section 10 of the DPA, except where retention is required or permitted by applicable law;
- g. make available information and permit assessments or audits to the extent required by applicable US Privacy Law and in accordance with Section 11 of the DPA;
- h. engage Sub-processors in accordance with Section 6 of the DPA and require applicable Sub-processors to be bound by written obligations that provide the level of protection required by applicable US Privacy Law; and
- i. not sell Customer Personal Data or Process Customer Personal Data for Murmurly's own targeted advertising or other purposes inconsistent with Murmurly's role as Processor.

3.2 Where assistance requested by Customer under this Schedule 5 requires substantial additional work beyond the ordinary functionality of the Services or Murmurly's ordinary compliance activities, Murmurly may charge Customer its reasonable costs for such additional assistance, to the extent permitted by applicable US Privacy Law, provided that Murmurly informs Customer of such costs in advance. Nothing in this Section 3.2 limits any assistance that Murmurly is required to provide without charge under applicable US Privacy Law.

4. California Privacy Terms

4.1 This Section 4 applies to the extent that Customer Personal Data constitutes "personal information" subject to the California Consumer Privacy Act of 2018, as amended, and its implementing regulations (the "**CCPA**"), and Customer is a "business" and Murmurly acts as a "service provider" or "contractor" with respect to such personal information.

4.2 The specific business purposes for which Murmurly Processes such personal information are the applicable purposes described in Schedule 1. Customer discloses or makes personal information available to Murmurly solely for those limited and specified business purposes.

4.3 Murmurly shall not:

- a. sell or share personal information received from or on behalf of Customer;
- b. retain, use or disclose such personal information for any purpose other than the business purposes specified in the Agreement, this DPA and Schedule 1, or as otherwise permitted by the CCPA;

c. retain, use or disclose such personal information outside the direct business relationship between Murmurly and Customer, except as permitted by the CCPA; or

d. combine such personal information with Personal Data received from or on behalf of another person or collected from Murmurly's own interaction with a consumer, except to the extent expressly permitted by the CCPA.

4.4 Murmurly shall comply with the obligations applicable to it as a service provider or contractor under the CCPA and, with respect to personal information Processed in that capacity, shall provide the level of privacy protection required by the CCPA and its implementing regulations to the extent applicable to Murmurly in such capacity.

4.5 To the extent Murmurly acts as a “contractor” within the meaning of the CCPA, Murmurly certifies that it understands the restrictions applicable to contractors under the CCPA, including the restrictions set out in Section 4.3, and will comply with them.

4.6 Taking into account the nature of the Processing and the information available to Murmurly, Murmurly shall reasonably cooperate with Customer to the extent required by the CCPA in:

a. responding to and complying with consumer requests;

b. completing a cybersecurity audit where Customer is required to conduct such audit under the CCPA;

c. conducting a risk assessment where Customer is required to conduct such assessment under the CCPA; and

d. complying with obligations relating to automated decisionmaking technology to the extent Murmurly's Processing of Customer Personal Data is relevant to Customer's applicable obligations.

4.7 Customer may take reasonable and appropriate steps to verify that Murmurly Processes personal information received from or on behalf of Customer in a manner consistent with Customer's obligations under the CCPA. Any assessment or audit shall be conducted in accordance with Section 11, except to the extent the CCPA requires otherwise.

4.8 If Murmurly determines that it can no longer meet its applicable obligations under the CCPA with respect to Customer Personal Data, Murmurly shall notify Customer without undue delay.

4.9 Upon notice from Customer of an unauthorised use of personal information by Murmurly, Murmurly shall take reasonable and appropriate steps to stop and remediate such unauthorised use to the extent required by the CCPA.

4.10 Where Murmurly engages a Sub-processor to Process personal information subject to this Section 4, Murmurly shall ensure that its written agreement with the Sub-processor includes the contractual protections required by the CCPA and its implementing regulations to the extent applicable to the relevant Processing.

5. Consumer Requests

5.1 Where Murmurly receives a request directly from a consumer relating to Customer Personal Data, Murmurly shall handle the request in accordance with Section 9 of this DPA and applicable US Privacy Law.

5.2 Customer remains responsible for determining the validity of, and responding to, consumer requests except to the extent applicable US Privacy Law places an obligation directly on Murmurly.

6. Sensitive Personal Data

6.1 The Services are not specifically designed for the Processing of sensitive Personal Data subject to heightened protection under applicable US Privacy Law. Where Customer chooses to Process such data through the Services, Customer remains responsible for determining whether such Processing is permitted and for satisfying any applicable consent, authorisation, notice, opt-in or other legal requirements, in accordance with Section 3.5 of the DPA.

6.2 To the extent Customer chooses to submit sensitive Personal Data through functionality supported by the Services, Murmurly shall Process such data in accordance with the Agreement, this DPA and Customer's documented instructions as provided in Section 2. Nothing in this Schedule requires Murmurly to accept any additional instruction, enable any functionality, or Process any category of sensitive Personal Data that is not supported by the Services or agreed by Murmurly.

7. Additional Mandatory Requirements

7.1 Mandatory requirements of applicable US Privacy Law shall apply to each Party only to the extent they apply to that Party by operation of law and in its actual role with respect to the relevant Processing. Nothing in this Schedule shall be construed as Murmurly voluntarily assuming any statutory obligation that would not otherwise apply to Murmurly. Where applicable US Privacy Law requires additional contractual terms not otherwise contained in this DPA, the Parties shall implement such terms to the extent required by law in accordance with Section 16 of the DPA.

7.2 Nothing in this Schedule requires Murmurly to assume obligations applicable to a Controller, business or other person independently determining the purposes and means of Processing except to the extent Murmurly actually acts in such role with respect to the relevant Processing.

8. Sector-Specific Laws

This Schedule does not, by itself, constitute a business associate agreement under the Health Insurance Portability and Accountability Act ("HIPAA") or any other agreement required under a sector-specific US privacy or data protection law.

Where Customer requires Murmurly to Process Personal Data subject to sector-specific contractual requirements not otherwise addressed by this DPA, such requirements shall apply only where expressly agreed by Murmurly in writing.

9. Liability

9.1 The exclusions and limitations of liability set out in Section 12 of the DPA and the Agreement apply to this Schedule 5. Any contractual liability arising out of or in connection with this Schedule 5 shall form part of, and shall not be in addition to, the aggregate liability cap applicable under the Agreement.

9.2 Nothing in this Schedule 5 creates any separate or additional indemnity, contractual penalty, liquidated damages obligation or uncapped liability. Any claim between the Parties arising out of or in connection with a breach of this Schedule 5 shall be subject to Section

9.1. Nothing in this Schedule creates a private statutory right of action that does not otherwise exist by operation of applicable law.

9.3 Sections 9.1 and 9.2 apply to the fullest extent permitted by applicable law. They do not limit liability, regulatory enforcement powers or statutory rights only to the extent that applicable law expressly prohibits such limitation by contract.