This Data Processing Addendum ("**DPA**") is incorporated into and supplements the Devyce Terms and Conditions ("**Terms**"), as updated from time to time (together, the "**Agreement")**, between the Customer (referred to as **"you"** or "**Customer**" in the Terms and "**Customer**" or "**Controller**" in this DPA) and Devyce (referred to as "**we", "us" or** "**Devyce**" in the Terms and as **"Devyce"** or "**Processor**" in this DPA).

This DPA only applies if and to the extent Devyce processes Personal Data on behalf of a Customer that qualifies as a Controller with respect to Personal Data under Data Protection Laws.

DEFINITIONS	
Parties' relationship	Controller to Processor
Parties' roles	Customer will act as the Controller (as defined in Section 1 of this DPA) Deyvce will act as the Processor (as defined in Section 1 of this DPA)
Term	This DPA will commence on the Commencement Date as set out in the Terms and will continue for the Total Subscription Term as set out in the Terms.
Breach Notification Period	Without undue delay and no later than 72 hours after becoming aware of a personal data breach.
Sub-processor Notification Period	A reasonable timeframe before the new sub-processor is granted access to Personal Data.
Liability Cap	Each party's aggregate liability under this DPA will not exceed the liability caps as per the Terms.
Governing Law and Jurisdiction	As per the Terms.
Data Protection Laws	All laws, regulations and court orders which apply to the processing of Personal Data in the United Kingdom (**UK**). This includes UK GDPR and the Data Protection Act 2018 each as amended from time to time.
Services	As described in the Terms.
Duration of processing	For the Term of this DPA.
Nature and purpose of processing	Collection, storage and deletion for the purposes of providing the Services under the Terms.
Personal Data	The types of personal data processed are: ● Contact details: name, address, email address, phone number and billing address. ● Financial data: card details ● Call data: call metadata, caller ID, audio recordings of incoming and outgoing calls, transcript of calls and voicemails, call summaries. ● Message data: SMS content, SMS logs, MMS content, MMS logs. ● CRM data: Customer information synced from the CRM, such as names and phone numbers, as well as any other data relating to a third party subject stored within the Customer CRM.
Data subjects	The individuals whose Personal Data will be processed are determined and controlled by the Customer in its sole discretion but includes (without limitation)**:** ● Customer ● Employees of Customer

	● Customer's end-users of the services: (callers, message recipients)
Special provisions	None.
Transfer Mechanism	The parties will use appropriate and lawful mechanisms for international transfers of Personal Data, including but not limited to Standard Contractual Clauses (SCCs) approved by the European Commission, the UK International Data Transfer Agreement (IDTA), or adequacy decisions, as required by applicable laws.

ANNEX 1	
Security measures. Technical and organisational measures to ensure the security of Personal Data	● Physical access controls: managed by Azure which maintains SOC2 and ISO 27001 certifications. ● System access controls: authentication mechanisms. ● Data access controls. Users log in with individual accounts, and have different levels of permissions based on their role within the system. ● Data encryption: at rest. ● Transmission controls: data in transit is secured using TLS encryption. ● Input controls: Users log in with individual accounts and data is validated before it is accepted. ● Data backups: data is continuously backed up, with a hot-standby in a different data centre located in a separate region. ● Data segregation: Data is partitioned based on organisation.

ANNEX 2

Sub-processors. Current sub-processors

Devyce engages the following sub-processors in provision of the Services to the Customer:

Sub-processor	**Activity**	**Country**
Microsoft Azure	Cloud services	UK, EU
Twilio	Voice connectivity, SMS services, call recording and call flow management	US, EU
Telnyx	Voice connectivity and SMS services	US, EU
Stour Marine	Voice connectivity and SMS services	UK
Deepgram	Call transcription	US, EU
OpenAI	Call summarisation, call coaching and feedback	US
Posthog	Caller ID analytics	EU
Hyperdoc Inc.	Video call recording	US

TERMS

1. What is this agreement about?

1.1 **Purpose**. The parties are entering into this Data Processing Agreement (**DPA**) for the purpose of processing Personal Data (as defined above).

1.2 **Definitions.** Under this DPA:

(a) **adequate country** means a country or territory that is recognised under Data Protection Laws from time to time as providing adequate protection for processing Personal Data, and

(b) **Controller**, **data subject**, **personal data breach**, **process/processing, Processor** and **supervisory authority** have the same meanings as in the Data Protection Laws, and

(c) **Sub-Processor** means another processor engaged by the Processor to carry out specific processing activities with Personal Data.

2. What are each party's obligations?

2.1 **Controller obligations.** Controller instructs Processor to process Personal Data in accordance with this DPA, and is responsible for providing all notices and obtaining all consents, licences and legal bases required to allow Processor to process Personal Data.

2.2 **Processor obligations.** Processor will:

(a) only process Personal Data in accordance with this DPA and Controller's instructions (unless legally required to do otherwise),

(b) not sell, retain or use any Personal Data for any purpose other than as permitted by this DPA and the Terms,

(c) inform Controller immediately if (in its opinion) any instructions infringe Data Protection Laws,

(d) use the technical and organisational measures described in Annex 1 when processing Personal Data to ensure a level of security appropriate to the risk involved,

(e) notify Controller of a personal data breach within the Breach Notification Period and provide assistance to Controller as required under Data Protection Laws in responding to it,

(f) ensure that anyone authorised to process Personal Data is committed to confidentiality obligations,

(g) without undue delay, provide Controller with reasonable assistance with:

(i) data protection impact assessments,

(ii) responses to data subjects' requests to exercise their rights under Data Protection Laws, and

(iii) engagement with supervisory authorities,

(h) if requested, provide Controller with information necessary to demonstrate its compliance with obligations under Data Protection Laws and this DPA,

(i) allow for audits at Controller's reasonable request, provided that audits are limited to once a year and during business hours except in the event of a personal data breach, and

(j) return Personal Data upon Processor's written request or delete Personal Data by the end of the Term, unless retention is legally required.

2.3 **Warranties**. The parties warrant that they and any staff and/or subcontractors will comply with their respective obligations under Data Protection Laws for the Term.

3. Sub-processing

3.1 **Use of sub-processors.** Controller authorises Processor to engage other processors (referred to in this section as **sub-processors**) when processing Personal Data. Processor's existing sub-processors are listed in Annex 2.

3.2 **Sub-processor requirements.** Processor will:

(a) require its sub-processors to comply with equivalent terms as Processor's obligations in this DPA,

(b) ensure appropriate safeguards are in place before internationally transferring Personal Data to its sub-processor, and
(c) be liable for any acts, errors or omissions of its sub-processors as if they were a party to this DPA.

3.3 **Approvals.** Processor may appoint new sub-processors provided that they notify Controller in writing in accordance with the Sub-processor Notification Period.

3.4 **Objections.** Controller may reasonably object in writing to any future sub-processor. If the parties cannot agree on a solution within a reasonable time, either party may terminate this DPA.

4. International personal data transfers

4.1 **Instructions.** Processor will transfer Personal Data outside the UK, the EEA or an adequate country only on documented instructions from Controller, unless otherwise required by law.

4.2 **Transfer mechanism.** Where a party is located outside the UK, the EEA or an adequate country and receives Personal Data:
(a) that party will act as the **data importer**,
(b) the other party is the **data exporter**, and
(c) the relevant Transfer Mechanism will apply.

4.3 **Additional measures.** If the Transfer Mechanism is insufficient to safeguard the transferred Personal Data, the data importer will promptly implement supplementary measures to ensure Personal Data is protected to the same standard as required under Data Protection Laws.

4.4 **Disclosures.** Subject to terms of the relevant Transfer Mechanism, if the data importer receives a request from a public authority to access Personal Data, it will (if legally allowed):
(a) challenge the request and promptly notify the data exporter about it, and
(b) only disclose to the public authority the minimum amount of Personal Data required and keep a record of the disclosure.

5. Other important information

5.1 **Survival.** Any provision of this DPA which is intended to survive the Term will remain in full force.

5.2 **Order of precedence.** In case of a conflict between this DPA and other relevant agreements, they will take priority in this order:
(a) Transfer Mechanism,
(b) DPA,
(c) Terms.

5.3 **Notices.** Formal notices under this DPA must be in writing and sent to the Contact on the DPA's front page as may be updated by a party to the other in writing.

5.4 **Third parties.** Except for affiliates, no one other than a party to this DPA has the right to enforce any of its terms.

5.5 **Entire agreement.** This DPA supersedes all prior discussions and agreements and constitutes the entire agreement between the parties with respect to its subject matter and neither party has relied on any statement or representation of any person in entering into this DPA.

5.6 **Amendments.** Any amendments to this DPA must be agreed in writing.

5.7 **Assignment.** Neither party can assign this DPA to anyone else without the other party's consent.

5.8 **Waiver.** If a party fails to enforce a right under this DPA, that is not a waiver of that right at any time.

5.9 **Governing law and jurisdiction.** The Governing Law applies to this DPA and all disputes will only be litigated in the courts of the Jurisdiction.

This version of the DPA is in force from 2026-08-21