DATA PROTECTION PROCEDURES

1. Definitions

1.1 In this Schedule 2 (including the Annexes), the following terms shall have the following meanings:

(a) "**Adequate Country**" means a country or territory recognised as providing an adequate level of protection for personal data transfers under an adequacy decision or regulations made from time to time by (as applicable) (i) the European Commission under the EU GDPR; or (ii) the UK Secretary of State under UK GDPR;

(b) "**Anonymized Data**" means personal data that has been processed in such a manner that it can no longer be attributed to an identified or identifiable natural person;

(c) "**Applicable Data Protection Law**" means all worldwide data protection and privacy laws and regulations applicable to the processing of personal data under the Agreement, including without limitation (where applicable) EU Data Protection Law and UK Data Protection Law;

(d) "**CPRA**" means the California Privacy Rights Act of 2020 Cal. Civil Code § 1798.100 et seq., as updated, amended or replaced from time to time (and including those sections of the California Consumer Privacy Act not amended by the CPRA).

(e) "**controller**", "**processor**", "**data subject**", "**personal data**", "**processing**" (and "**process**") and "**special categories of personal data**" shall have the meanings given in Applicable Data Protection Law;

(f) "**Client Personal Data**" means the personal data set out at Annex A processed by the Supplier for the Permitted Purpose;

(g) "**EEA**" means the European Economic Area;

(h) "**EU Data Protection Law**" means:

(i) all EU regulations or other legislation applicable (in whole or in part) to the processing of personal data (such as 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 (the "**GDPR**"));

(ii) the national laws of each EEA member state implementing any EU directive applicable (in whole or in part) to the processing of personal data (such as Directive 2002/58/EC); and

(iii) any other national laws of each EEA member state applicable (in whole or in part) to the processing of personal data,

as amended or superseded from time to time;

(i) "**EU Standard Contractual Clauses**" means the European Commission's implementing decision 2021/914/EU of 4 June 2021 on standard contractual clauses for the transfer of

personal data to third countries pursuant to the GDPR and currently available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en;

(j) **"Permitted Purpose"** means the purposes for which the Supplier processes Client Personal Data under this Agreement as set out at Annex A;

(k) "**Personal Information**" means personal information (as defined under the CPRA) provided by Client to Supplier (or indirectly by any third party) in respect of which Client is subject to the CPRA.

(l) "**UK Standard Contractual Clauses**" means the UK International Data Transfer Agreement dated 21 March 2022 issued under s119A(1) of the Data Protection Act 2018 and currently available at https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf.

(m) "**UK Addendum**" means the template Addenum B.1.0. dated 21 March 2022 issued under s119A(1) of the Data Protection Act 2018 and currently available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf.

(n) "**UK Data Protection Law**" means:

(i) the GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**");

(ii) the Data Protection Act 2018;

(iii) the Privacy and Electronic Communications (EC Directive) Regulations 2003 as they continue to have effect by virtue of section 2 of the European Union (Withdrawal) Act 2018; and

(iv) any other laws in force in the UK from time to time applicable (in whole or in part) to the processing of personal data,

as amended or superseded from time to time.

(o) "**US Privacy Law**" means the California Consumer Privacy Act of 2018 ("**CCPA**") and the CPRA and any other state or federal laws applicable to the processing of personal data relating to US data subjects.

Controller and Processor

2. Relationship of the parties

2.1 Client (the controller) appoints the Supplier as a processor to process Client Personal Data for the Permitted Purpose.

2.2 Client acknowledges that as Client (or Authorised Users) use the Services, the Supplier (as controller) may (i) process personal data to manage the relationship with Client (including for accounting and taxation purposes; and (ii) create and derive from processing under the Agreement, Anonymized Data for the purpose of product improvement and development purposes. Supplier may use and disclose Anonymized Data in any manner it deems useful, provided that any disclosure of Anonymized Data is

done in a manner that does not permit the identification of Client or Authorised Users in relation to such Anonymized Data.

2.3 Each party shall comply (and will procure that its personnel, and in the case of Client it's Authorised Users, comply and use commercially reasonable efforts to procure that its subprocessors comply) with the obligations that apply to it under Applicable Data Protection Law. As between the parties, Client shall have sole responsibility for the accuracy, quality and legality of personal data and the means by which Client acquired (or acquires) Client Personal Data and will ensure it provides any notices to, and obtains any consents from data subjects where required by Data Protection Laws.

2.4 In the event that the Supplier processes any Client Personal Data to which US Privacy Law applies, the terms of Annex C shall apply in addition in respect of such Client Personal Data.

Supplier processor obligations

3. Client Instructions

3.1 Supplier shall only process Client Personal Data (i) in accordance with this Schedule 2; and (ii) Client's written instructions. If the Supplier becomes aware that any Client instruction infringes Applicable Data Protection Law, it shall promptly inform Client.

3.2 In the unlikely event that applicable law requires Supplier to process Client Personal Data other than pursuant to Client's instructions, Supplier will notify Client (unless prohibited from so doing by applicable law).

4. Security

4.1 The Supplier shall:

4.1.1 implement and maintain appropriate technical and organisational measures to protect Client Personal Data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Client Personal Data (a "**Security Incident**"). Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons and shall include without limitation the security measures set out at https://www.doorway.io/security/; and

4.1.2 where required by Applicable Data Protection Law, provide other such reasonable cooperation and assistance to the Client (at Client's reasonable cost and expense) with respect to Client's obligations with respect to the security of processing.

5. Confidentiality

5.1 Supplier shall take reasonable steps to ensure that any person that it authorises to process Client Personal Data (including Supplier's staff, agents and subcontractors) (an "**Authorised Person**") shall be subject to a duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process Client Personal Data who is not under such a duty of confidentiality.

6. International transfers

6.1 The Supplier shall not transfer Client Personal Data (nor permit Client Personal Data to be transferred) outside of the EEA and/or the UK unless it takes such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) (i) transferring Client Personal Data to a recipient an Adequate Country; (ii) to a recipient that has achieved binding corporate rules authorisation in accordance with Applicable Data Protection Law; or (iii) to a recipient that has executed (a) EU Standard Contractual Clauses, adopted or approved

by the European Commission; or (b) for transfers from the UK, UK Standard Contractual Clauses or (c) the UK Addendum to the EU Standard Contractual Clauses approved by the Secretary of State; and as applicable, transferring Client Personal Data subject any reasonably appropriate supplementary safeguards in support of the above.

7. Subprocessing

7.1 The Client consents to the Supplier engaging the third party subprocessors listed in Annex B and any other subprocessors the Supplier may instruct to process Client Personal Data for the Permitted Purpose provided that: (i) the Supplier shall update the Client with details of any change in subprocessors; (ii) the Supplier imposes data protection terms on any subprocessor it appoints that require it to protect Client Personal Data to the standard required by Applicable Data Protection Law; and (iii) the Supplier remains liable for any breach of this paragraph 7 that is caused by an act, error or omission of its subprocessor. Client may object to the Supplier's appointment or replacement of a subprocessor within twenty-one (21) days of receiving the information, provided such objection is based on reasonable grounds relating to data protection. Should Client object, the parties shall work together in good faith to appoint an alternative sub-processor.

8. Cooperation and data subjects' rights

8.1 The Supplier shall provide reasonable assistance to Client (at Client's expense) to enable Client to respond to any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable).

9. Data Protection Impact Assessment

9.1 The Supplier shall provide reasonable cooperation to Client (at Client's expense) in connection with any data protection impact assessment or prior consultation with a regulatory authority that may be required under Applicable Data Protection Law for any data protection impact assessment conducted under this paragraph 9.

10. Return and Deletion

10.1 The Supplier shall unless otherwise required to comply with applicable law, delete or return to Client all personal data (including copies thereof) for which Supplier is the processor and that is processed pursuant to this Schedule 2 in accordance with the procedures and timeframes specified at clause 13.7 of the Agreement.

11. Security incidents

11.1 If Supplier becomes aware of a confirmed Security Incident, the Supplier shall inform Client without undue delay and shall provide reasonable information and cooperation to Client so that Client can fulfil any data breach reporting obligations it may have under (and in accordance with the timescales required by) Applicable Data Protection Law.

12. Audit and records

12.1 Client acknowledges that the Supplier is regularly audited by independent third party auditors. Upon request, the Supplier shall supply a summary copy of its audit report(s) to Client, and /or make available to Client (at Client's expense) such other information in Supplier's possession or control as Client may reasonably request with a view to demonstrating Supplier's compliance with the obligations of processors under Applicable Data Protection Law in relation to its processing of personal data under this Schedule which shall be subject to the confidentiality provisions of this Agreement.

13. Other information that we collect

13.1 Client acknowledges that, in using the Services, the Supplier may collect certain information automatically from an Authorised User's device. This information may be considered personal data under Applicable Data Protection Law.

13.2 Specifically, the information the Supplier collects automatically may include information like an Authorised User's IP address, device type, unique device identification numbers, other internal identifiers (integers), browser-type, broad geographic location (e.g. country or city-level location) and other technical information. The Supplier may also collect information about how an Authorised User's device has interacted with the Services.

13.3 Client acknowledges that collecting this information enables the Supplier to better understand the users of the Services, where they come from, and what content or functionality in the Services is of interest to them. The Supplier uses this information for its internal analytics purposes and to improve the quality and relevance of the Services to its users.

Annex A

Subject matter of processing
Supplier's provision of the Services to Client, including the use of Supplier's Software for the development and maintenance of virtual business cards.

Nature and purpose of processing
The collection, analysis (including improving Supplier's Software and Services) storage, duplication, deletion and disclosure of Personal Data as necessary to provide the Services, and as may be further instructed by Client in writing or as agreed in the Term Sheet.

Data subjects
The categories of data subject whose personal data that may be processed in order to provide the Services may include the Client's representatives and Authorised Users.

Categories of personal data
The categories of personal data that may be processed in order to provide the Services includes the first names, surnames, email addresses, telephone number, organisation and position of Client's representatives and Authorised Users.

Special categories of data (if applicable)
None.

Processing operations
Supplier may process Client Personal Data as necessary to perform the Services including hosting and storage; service change management; issue resolution; IT security purposes including incident management; maintenance and performance of technical support systems and IT infrastructure; and implementation, configuration and performance testing.

Duration of the processing
Supplier will process Client Personal Data for the Term of this Agreement, or until such data is no longer necessary for the purposes of either party performing its obligations under this Agreement (to the extent applicable), unless otherwise agreed between the parties in writing.

Annex B – Approved Subprocessors

Name	**Processing**	**Territory(ies)**
Amazon Web Services, Inc.	Cloud service provider	United States & EU
Heroku, Inc.	Clous service provider	United States & EU
Salesforce.com, Inc.	Cloud service provider	United States & EU
SendGrid, Inc.	Cloud-based notification services	United States
Twilio, Inc.	Cloud-based notification services	United States
Stripe, Inc.	Subscription data and payment information	United States & EU
CloudFlare, Inc.	Content delivery provider	United States
Hubspot, Inc.	Client relationship manager	United States
Alphabet, Inc.	Software service provider	United States

Mixpanel UK Limited	Software service provider	United States & EU
Hotjar Ltd	Software service provider	United States & EU

Annex C – US Privacy Laws

In this Annex C , **Business"** "**Collects**" (and "**collected**" and "**collection**"), "**Consumer**", "**Business Purpose**", "**Sell**" (and "**selling**", "**sale**", and "**sold**") and **"Service Provider"** are as defined under the CPRA.

1. Scope. This Annex C applies only where, and to the extent that, Supplier processes Personal Information that is subject to the CPRA on behalf of Client as a Service Provider in the course of providing the Services pursuant to the Agreement.

2. Service provider appointment: Client is a Business and appoints Supplier as its Service Provider to Collect and process the Personal Information for the Business Purpose. Supplier is responsible for its compliance with its obligations under this Annex C and for compliance with its obligations as a Service Provider under the CPRA. Client is responsible for compliance with its own obligations as a Business under the CPRA.

3. Business purpose: Supplier shall only Collect and process Personal Information as a Service Provider upon lawful documented instructions from Client, including those in the Agreement and this Annex C or as otherwise necessary to provide the Services (the **"Business Purpose"**). Supplier must not process the Personal Information for any purpose other than for the Business Purpose, except where and to the extent permitted by the CPRA.

4. Service provider certification: Supplier shall not: (a) Sell or Share any Personal Information; (b) retain, use, or disclose the Personal Information for any purpose other than for the Business Purpose, including to retain, use, or disclose the Personal Information for a commercial purpose other than providing its Services under the Agreement; (c) retain, use, or disclose the Personal Information outside of the direct business relationship between the Supplier and Client (other than to Supplier's own service providers); (d) combine Personal Information with any other data if and to the extent this would be inconsistent with the limitations on service providers under the CPRA. Supplier certifies that it understands the restrictions set out in this paragraph 4 and will comply with them.

5. Consumer's rights: Supplier will, upon Client's instructions (and at Client's expense): (a) use reasonable efforts to assist Client in deleting Personal Information in accordance with a Consumer's request (and shall instruct any service providers it has appointed to do the same) except where and to the extent permitted to retain the Personal Information pursuant to an exemption under the CPRA; and (b) use reasonable efforts to assist Client in responding to verified Consumer requests received by Client to provide information as it relates to the Collection of Personal Information for the Business Purpose.

6. Assistance: Supplier will, upon Client's instruction and upon proof of such a communication, provide reasonable assistance to Client to enable Client to respond to any correspondence, enquiry or complaint received from a Consumer or the California Attorney General and/or the Californian Privacy Protection Agency in connection with the Collection and processing of the Personal Information.