CAPDESK - DATA PROCESSING AGREEMENT

Appendices to the Processing Agreement

Appendix 1	Categories of personal data
Appendix 2	Technical and organisational security safeguards
Appendix 3	Documentation for compliance with obligations
Appendix 4	Controller's obligations
Appendix 5	Sub-processors

1. The Agreement And The Parties

1.1 This Data Processing Agreement (the “Processing Agreement”) and underlying appendices is an agreement between Vauban Technologies Limited, with offices at 186 Shoreditch High Street, Fora - Montacute Yards, London, E1 6HU, (“the Processor”, “we” or “Capdesk”) and you or the entity you represent (“the Controller”, or “you”), collectively referred to as the Parties and individually as a Party.

1.2 The Parties have agreed to the provision of certain services from the Processor to the Controller, as described in more detail in the Parties' separate agreement to this effect, the Controller’s Customer Agreement with Capdesk, and possibly further service specific appendices. This Processing Agreement governs the Controller’s usage of the Capdesk-provided services, such as usage of the Capdesk web application (the “Application”) and the controller’s consumption of services in relation hereto, hereafter referred to as the "Primary Services".

1.3 In this connection, the Processor processes personal data on behalf of the Controller, and for that purpose, the Parties have entered into this Processing Agreement.

1.4 You enter into this Processing Agreement when you enter into the Customer Agreement and this Processing Agreement is incorporated in and forms part of the Customer Agreement between Capdesk and you.

2. Changes To This Agreement

2.1 You agree that Capdesk may modify this Processing Agreement at any time in its sole discretion and without prior notice to you. Any changes will be published online and will be effective upon such publishing. We will notify you directly in case of any changes to this Processing Agreement. We encourage you to review this Processing Agreement periodically to ensure familiarity with its then-current terms and conditions. Your continued use of the Services shall constitute your acceptance of this Processing Agreement and your continued use of the Services following any modification of this Processing Agreement shall constitute your acceptance to the Processing Agreement, as amended.

You may object to any substantial change to this Processing Agreement by terminating the Processing Agreement for cause immediately upon notice, on condition that you provide such notice within 90 days of being informed of the change to this Processing Agreement. This termination right is your sole and exclusive remedy if you object to any change in the Processing Agreement.

2.2 This Processing Agreement was last updated on 6 April 2023.

3. Purpose

3.1 The purpose of the Processing Agreement is to ensure that the Processor complies with all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, and the UK, applicable to the Processing of Personal Data under the Agreement in force as may be amended from time to time.

4. Scope

4.1 The Processor is authorised to process personal data on behalf of the Controller on the terms and conditions set out in the Processing Agreement.

4.2 The Processor may only process personal data subject to documented instructions from the Controller ("Instructions"). This Processing Agreement, including appendices, constitutes the Instructions at the date of agreement.

4.2.1 The Processor may process any personal data provided by the Controller as part of consuming the Primary Services. Restrictions apply to what categories of personal data the Controller may provide, cf. Appendix 4.

4.2.2 The personal data provided by the Controller is kept by the Processor until the Controller requests its deletion as part of termination of this Processing Agreement, cf. clause 14.5.

4.2.3 The Processor can optimize the quality and usefulness of the Primary Services, as well as its communication to the Controller, by internally registering and analysing how the Controller and representatives of the Controller consume the Primary Services. To the extent that any personal data is part of such internal data processing, the processing of that data adheres to the obligations set out in this Processing Agreement.

4.3 The Instructions may be changed or concretised at any time by the Controller, pursuant to the Change of Instruction process outlined in clause 11.

4.4 If at any time the Instructions are regarded by the Processor as unlawful (in breach of GDPR, other EU personal data protection regulation, or UK or EU member state national personal data protection regulation), the Processor shall notify the Controller without undue delay.

4.5 Unless explicitly agreed otherwise in writing, the Processor may use all relevant technical and non-technical aids, including IT systems, subject to their appropriate security level (for instance fulfilment of GDPR article 32).

4.6 Regardless of the termination of the Processing Agreement, clauses 14.4 (termination window for processing) and 15 (dispute resolution) will remain in force after termination of the Processing Agreement.

5. Duration

5.1 The Processing Agreement applies until termination of the agreement(s) on provision of the Primary Services.

6. Processor's obligations

6.1 Technical and organisational security measures

6.1.1 The Processor is responsible for implementing necessary (a) technical and (b) organisational measures to ensure an appropriate security level to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access. The measures must be implemented with due regard to the current state of the art, costs of implementation and the nature, scope, context and purposes of the processing and the risk of varying likelihood and severity to the rights and freedoms of natural persons. The Processor shall take the category of personal data described in Appendix 1 into consideration in the determination of such measures.

6.1.2 Notwithstanding clause 6.1.1, the Processor shall implement the technical and organisational security measures as specified in Appendix 2 to this Processing Agreement.

6.1.3 The Processor shall implement suitable technical and organisational measures in such a manner that the processing by the Processor of personal data meets the requirements of the personal data regulation in force from time to the time of processing by the Processor.

6.1.4 The Parties agree that the provided safeguards as specified in Appendix 2 are adequate at the date of conclusion of this Processing Agreement. The Processor shall, at own cost and initiative, maintain and elaborate on its technical and organizational measures as described in this clause 6, as time passes, industry practice changes, and supervisory authorities issue opinions.

6.2 Employee conditions

6.2.1 The Processor shall ensure that employees who process personal data for the Processor have undertaken to observe confidentiality or are subject to an appropriate statutory duty of confidentiality.

6.2.2 The Processor shall ensure that access to the personal data is limited to those employees for whom it is necessary to process personal data in order to meet their obligations to the Controller.

6.2.3 The Processor shall ensure that employees processing personal data for the Processor only process such data in accordance with the Instructions.

6.3 Documentation for compliance with obligations

6.3.1 Upon written request, the Processor shall document to the Controller that the Processor:

a) meets its obligations under this Processing Agreement and the Instructions.

b) meets the provisions of the personal data regulation in force from time to time, in respect of the personal data processed on behalf of the Controller.

6.3.2 The Processor's documentation must be provided within reasonable time.

6.3.3 The specific content of the obligations under clause 6.3.1 is described in Appendix 3 to this Processing Agreement.

6.4 Security breach

6.4.1 The Processor shall notify the Controller of any known personal data breach which may potentially lead to accidental or unlawful destruction, alteration, unauthorised disclosure of, or access to, personal data processed for the Controller ("Security Breach").

6.4.2 Security Breaches must be reported to the Controller without undue delay. A Security Breach report shall, to the extent this is possible at the time of reporting, provide the Controller with

a) information about the nature of the Security Breach, including the categories and volumes of personal data affected,

b) information about the potential consequences of the Security Breach,

c) contact information of a Processor representative where further information can be obtained,

d) a description of measures undertaken or planned by the Processor, if any, to mitigate consequences of the Security Breach.

In case of complex situations, the Processor may inform the Controller in steps, as more become known about the Security Breach, and in such situations, the Processor will report regularly to the Controller until all necessary information that can possibly and realistically be obtained regarding the Security Breach has been provided.

6.5 Assistance

6.5.1 The Processor shall to the necessary and reasonable extent assist the Controller in the performance of its obligations in the processing of the personal data covered by this Processing Agreement, including in connection with:

a) responses to data subjects on exercise of their rights; (basic operations and support for performing such operations are available as part of the Services at no cost),

b) Security Breaches;

c) impact assessments; and

d) prior consultation of the supervisory authorities.

6.5.2 In this connection, the Processor shall obtain the information to be included in a notification to the supervisory authority provided that the Processor is best suited to do so.

6.5.3 The Processor may assist with any extra tasks as agreed in writing between the Processor and the Controller.

6.5.4 The Processor is entitled to payment for time spent (at an hourly rate of £100 – 150 ex. VAT, depending on the type of assistance) and materials consumed for assistance pursuant to this clause 6.5; however, to the extent assistance pursuant to 6.5.1 a) and b) is required by GDPR or other applicable law, such assistance will not entitle Processor to any payments.

7. Controller's obligations

7.1 The obligations of the Controller are set out in Appendix 4.

8. Sub-Processors

8.1 As part of the Processor's delivery of the Primary Services, the Processor may use a third party for the processing of personal data for the Controller (a "Sub-Processor"). This Processing Agreement constitutes the Processor's prior general and specific consent to the Processor's use of Sub-Processors.

8.2 The Processor will ensure that each Sub-Processor adheres to an equivalent level of data protection obligations towards the Processor as those adhered to by the Processor towards the Controller (including in pursuance of this Processing Agreement).

8.3 Moreover, the Sub-Processor also acts only under the Instructions of the Processor.

8.4 The Processor is directly responsible for the Sub-Processor's processing of personal data in the same manner as had the processing been carried out by the Processor.

8.5 Upon request, the Processor shall provide the Controller with documentation of what Sub-Processors are used by the Processor. A list of Sub-Processors as of the Effective Date is included as an appendix to this Processing Agreement.

9. Transfer to third countries and international organisations

9.1 The Processor may only transfer personal data to countries outside UK or EU, or international organisations, to the extent specified in:

a) Clause 9.3 of this Processing Agreement; or

b) Instructions from the Controller; or

c) prior written consent from Controller.

9.2 In any case, personal data may only be transferred to the extent permitted under the Personal Data Regulation in force from time to time - and the Processor shall ensure that the Sub-Processor at any time is subject to a Supervisory Authority (i.e. the Information Commissioner's Office) or EU Commission approved third country transfer legal mechanism. To the extent that the transfer mechanism is the EU Model Clauses (otherwise referred to as the Standard Contractual Clauses), the Controller and Sub-Processor shall execute an unedited version of the EU Model Clauses, for it to be considered a valid third country transfer mechanism.

9.3 The Controller approves that the Processor, without further or prior notice, may transfer personal data to third countries as long as such transfers are part of data transfers to and from approved Sub-Processors and pursuant to the conditions in clause 9.2.

9.4 Based on the adequacy decision adopted by the EU Commission on 28 June 2021, the Processor will continue to consider the UK a secure country with respect to data processing, and will therefore allow customer data to flow between and be processed in both the UK and the EU without requiring a third country transfer mechanism.

10. Data processing outside the scope of the Instructions

10.1 The Processor may process personal data outside the scope of the Instructions in cases where required by EU law or national law to which the Processor is subject.

10.2 If personal data are processed outside the scope of the Instructions, the Processor shall notify the Controller of the reason. The notification must be made before processing is carried out and must include a reference to the legal requirements forming the basis of the processing.

10.3 Notification should not be made if such notification would be contrary to EU law or national law.

11. Change of Instructions

11.1 Before any changes are made to the Instructions, the Parties shall to the widest possible extent discuss and, if possible agree on, the implementation of the changes, including time and costs of implementation.

11.2 Unless otherwise agreed, the following applies:

- Fundamental processing instructions such as access to, deletion of, or correction of data, or suspension of data processing, shall not be subject to discussion and require the Processor's response without undue delay, cf. also Section 6.5.
- The Processor shall, without undue delay, execute implementation of changes to the Instructions and ensure that such changes are implemented without undue delay in relation to the nature and scope of the change.
- Subject to exclusions and limitations of payment of fees for assistance stipulated in other sections of this Processing Agreement, The Processor is entitled to payment of all costs directly related to changes to the Instructions, including costs of implementation and increased costs for the delivery of the Primary Services.
- An indicative estimate of the time and cost of implementation must be communicated to the Controller without undue delay.
- The changes to the Instructions are only considered to apply once the changes have been implemented, provided that the implementation is carried out in accordance with this clause 11.2 and unless the Controller explicitly communicates a deviation from this clause.
- Processors are exempt from liability for failure to deliver the Primary Services if (including in terms of time) delivery of the Primary Services would be contrary to the changed Instructions or delivery in accordance with the changed Instructions is not possible. This may be the case (i) where the changes cannot be technically, practically or legally implemented, (ii) where the Controller explicitly communicates that the changes have to apply before implementation is possible or (iii) during the period until the parties have made any necessary changes to the agreement(s) in accordance with the change procedures herein. Notwithstanding aforementioned, the Processor is never exempt from liability for failure to deliver the Primary Services if the changed Instructions relate to the implementation of appropriate technical and organizational measures as applicable from time to time arising out of law applicable to Processor.

12. Breach

12.1 The regulation of breach in the Customer Agreement on delivery of the Primary Services also applies to this Processing Agreement as were this

Processing Agreement an integral part thereof. If this is not considered in the Customer Agreement on delivery of the Primary Services, the general remedies for breach laid down in applicable law will apply to this Processing Agreement.

13. Limitation Of Liability

13.1 For the avoidance of doubt, each Party’s liability, taken together in the aggregate, arising out of or related to these terms, whether in contract, tort or under any other theory of liability, is subject to the limitations and exclusions of liability contained within the Customer Agreement, and any reference to the liability of a Party means the aggregate liability of that Party under the Customer Agreement and this Processing Agreement together.

14. Force Majeure

14.1 The regulation of force majeure in the agreement(s) on delivery of the Primary Services also applies to this **Processing Agreement** as were this **Processing Agreement** an integral part thereof.

15. Termination

15.1 Termination for cause or breach or without cause

15.1.1 The Processing Agreement may only be terminated according to the provisions on termination in the agreement(s) on delivery of the Primary Services.

15.2 Effects of termination

15.3 The Processor's authority to process personal data on behalf of the Controller lapses on termination of the Processing Agreement for whatever reason.

15.4 The Processor may continue to store personal data for up to three months and process personal data for up to one month after the termination of the Processing Agreement to the extent that this is necessary to take the required statutory measures. During the same period, the Processor is entitled to let the personal data be included in the Processor's usual backup procedure. The processing by the Processor during this period is assumed to comply with the Instructions.

15.5 The Processor and any Sub-Processors shall return all personal data processed by the Processor under this Processing Agreement to the Controller on termination of the Processing Agreement; if the Controller is already in possession of aforementioned personal data, the Parties may agree to skip this procedure. Then, the Processor will without undue delay delete all personal data from the Controller, and the Controller may request adequate documentation about such deletion, except where such a deletion contradicts record-keeping or other lawful obligations on the Processor in force from time to time.

16. Disputes

16.1 The regulation of dispute resolution, including governing law and venue, in the agreement(s) on delivery of the Primary Services also applies to this Processing Agreement as were this Processing Agreement an integral part thereof.

17. Precedence

17.1 In the event of any discrepancies between this Processing Agreement and the agreement(s) on delivery of the Primary Services, this Processing Agreement takes precedence.

18. Contact And Notice

18.1 The contact information of the Parties and the regulation of notice in the agreement(s) on delivery of the Primary Services also applies to this Processing Agreement as were this Processing Agreement an integral part thereof.

APPENDIX 1
CATEGORIES OF PERSONAL DATA

1. Categories of Personal Data

1.1 The categories of personal data considered in the context of this Processing Agreement:

a) General Personal Data, including any data about an identified or identifiable data subject, except for those mentioned in point b) and c), also including civil/social registration numbers. Examples of such data include, but are not limited to, first name, middle names, last name, title, emails, phone numbers, addresses, IP-addresses, un-hashed cookies, civil/social security numbers, other personal identifiers, birthday, sex.

b) Sensitive Personal Data, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning health or sex life or sexual orientation, genetic data and biometric data.

c) Other Personal Data, relating to criminal offences and serious social problems.

2. Categories Of Personal Data Processed

2.1 According to The Instructions, the Processor will process General Personal Data (see 1.1.a above) provided by the Controller, including contact information, financial data and social security numbers. The Processor does not process Sensitive Personal Data or Other Personal Data as described in 1.1.b and 1.1.c above.

3. Categories Of Registered Data Subjects Processed

3.1 According to The Instructions, the Processor may process personal data for the Controller concerning the following categories of registered data subjects:

a) the Controller's and its affiliated companies' end users, if any,

b) the Controller's and its affiliated companies' employees,

c) the Controller's and its affiliated companies' contact persons,

d) the Controller's and its affiliated companies' direction and board,

e) the Controller's and its affiliated companies' shareholders, optionholders, warrantholders, debtholders, and other stakeholder with a commercial, financial or other interest in or relation to the Controller,

f) the Controller's and its affiliated companies' customers and customers' end users,

g) the Controller's and its affiliated companies' customers' employees,

h) the Controller's and its affiliated companies' customers' contact persons,

i) other.

APPENDIX 2

TECHNICAL AND ORGANISATIONAL SECURITY SAFEGUARDS

1. Specific technical and organisational security Safeguards:

1.1 The following specific safeguards are made for the Processor's physical security:

a) Access control to physical facilities,

b) Password-protection of physical equipment and outsourced systems (including databases) by suitably strong passwords, specifically, passwords no less than 10 characters and of at least alphanumerical symbol variance,

c) Only authenticated, encrypted traffic for administrative access to systems (including databases),

d) Data center redundancy of all critical infrastructure, eliminating physical risks to equipment such as fire, power failure, or similar,

e) Periodical monitoring for known vulnerabilities, e.g. scans against OWASP top 10, and established process(es) for addressing such vulnerabilities without undue delay.

1.2 The following specific safeguards are made for the Processor's technical security:

a) at an application-level, the Application requires authentication via user / password combination and has a fine-grained access and authorization engine for controlling resource access,

b) on a network communication level, any communication with the Application is encrypted, as is application-database traffic,

c) as for data storage, the Application uses state of the art data centres for storage of database data and documents, which means that data is safe, encrypted at rest, backed up, and roll-backable in case of incidents,

d) data center redundancy, backups (including at least daily backups of Controller’s data), deployment and rollout methods and contingency plans enable suitable and timely recovery of the entire Application (in case of a major incident),

e) all Application activity (including database activity) is logged for accountability,

f) the Processor’s internal data networks are secured by expert third parties.

1.3 The following specific safeguards are made for the Processor's organisational security:

a) All relevant Processor employees are briefed regularly on the Processor’s security matters and how to respond to security incidents,

b) All the Processor’s employees follow the Processor’s internal Employee Code of Conduct, which spells out relevant best practice employee security behaviour, such as keeping passwords personal, strong and secret.

c) The Processor undertakes regular security reviews to secure a constantly sufficient level of security and develops and implements its business using the principles of privacy by design and privacy by default.

1.4 The following specific safeguards are made for the Processor's deletion of personal data:

a) The Processor keeps a digital record of what personal data is stored where on behalf the Controller, so when deleting data is mandated, The Processor knows which data to delete,

b) The Processor maintains a standard procedure to delete such data,

c) The Processor has procedures to identify personal data that must be deleted due to age.

1.5 The Processor shall ensure that Sub-Processors will implement the appropriate technical and organisational measures in such a way that the processing meets the requirements of the General Data Protection Regulation.

APPENDIX 3
DOCUMENTATION FOR COMPLIANCE WITH OBLIGATIONS

As part of the Processor's demonstration to the Controller of compliance with its obligations according to clause 6.3 of the Processing Agreement, the following points must be completed and observed.

1. General documentation to the Controller

1.1 Upon written request, the Processor is obliged to submit the following general documentation to the Controller:

a) A declaration from the Processor's management specifying that, during the processing of personal data on behalf of the Controller, the Processor continuously ensures compliance with its obligations under this Processing Agreement.

b) A description of the practical measures, both technical and organisational, implemented by the Processor to ensure compliance with its obligations under the Processing Agreement. The description may include a presentation of established and implemented management systems for information security and for processing of personal data as well as a description of other initiatives taken. As part thereof, the Processor is also obliged to participate in follow-up meetings with the Controller.

A description of the control measures taken and implemented by the Processor for measurement and control of the effect of the established management system for information security and processing of personal data and performance measurements thereof.

1.2 Upon written request, the Processor will further assist with non-general documentation, documenting any other measures and controls as the Controller may request.

1.3 The general documentation must be provided no later than 14 working days after the Controller has made its written request to the Processor, or such shorter notice as required by the government. The Processor shall prepare general documentation for its own account; preparation of non-general documentation and participation in meetings may be subjected to a separate payment of a fee to the Processor, as agreed on a request by request basis and negotiated between the Parties.

2. Statement of assurance

2.1 Upon request and against separate payment of a fee, the Processor shall arrange for the preparation and submission of statements of assurance regarding the Processor's information security level and the measures taken by the Processor. Scope and payment of such undertakings shall be agreed in more detail on a request by request basis.

3. Physical meeting

Upon request, the Processor shall participate in a physical meeting at the premises of the Processor or the Controller. At the meeting the Processor must be able to give an account of compliance and how compliance is ensured. A request for a meeting must be made subject to at least 14 working days' notice. Scope and payment related to preparation, execution and follow-up shall be agreed in more detail on a request by request basis.

4. Audit

4.1 Upon written request, the Processor shall contribute to and give access to audit.

4.2 The Processor is entitled to payment for time spent and materials consumed for assistance pursuant to this clause 4; the hourly rate for time spent is set to £100 - £150 ex. VAT, depending on the nature of the assistance.

4.3 The Processor is not entitled to payments if an audit shows substantial non-compliance with the obligations under this Processing Agreement or Data Protection Regulations.

5. Other conditions

5.1 The above points should not be considered exhaustive, and the Processor therefore undertakes to take any such actions and measures as are necessary for the demonstration of the Processor's obligation under clause 6 of the Processing Agreement.

5.2 The Processor is not obliged to follow a request from the Controller according to this Appendix 3 if the request is in violation of the personal data regulation. The Processor shall notify the Controller if the Processor finds that this is the case.

APPENDIX 4
CONTROLLER'S OBLIGATIONS

1. OBLIGATIONS

1.1 The Controller has the following obligations

a) To ensure that any personal data provided to the Processor is controlled by the Controller on a lawful basis, and are kept accurate, minimized, complete, and up-to-date,

b) Ensure that any obligations towards data subjects relating the right to be informed about the Controller's controlling of that data subjects' data are met,

c) To not provide the Processor with any personal data that are not General Personal Data as defined in Appendix 1 (thus excluding the disclosure or provision of any Sensitive Personal Data, or data relating to criminal offences, or data relating to serious social problems).

d) To ensure that the Instructions are lawful in relation to the personal data regulation in force from time to time.

2. OTHER CONDITIONS

2.1 By agreeing to the Processing Agreement, the Controller agrees that the Processor has given sufficient and relevant guarantees regarding the technical and organisational safeguards related to securing the registered data subject's rights and personal data, at the time of signing this Processing Agreement. Notwithstanding aforementioned, Controller and Processor agree that the Processor is expected to implement changes that will be required to meet what is considered "appropriate technological and organizational measures", as technology evolves, implementation cost of technology changes, and/or directions from supervisory authorities change.

APPENDIX 5
SUB-PROCESSORS

1. THIRD PARTIES

1.1 The Processor and its affiliates engage the following third-party entities to assist them in connection with delivering the Primary Services. This list of sub-processors is subject to change at the Processors discretion. The

Processor will inform the Controller of any changes to the list of sub-processors.

1.2 APPLICATION AND DATA STORAGE

These third party sub-processors provide us with virtual application infrastructure and data storage:

1.2.1 **Salesforce.com EMEA Limited** (London, England). Provides us with a cloud application platform (Heroku) for running the Application and leveraging platform extensions for error analysis, mail sending, and more. Data processing in UK, EU and USA.

1.2.2 **Amazon Web Services, Inc.** (Seattle, USA)**.** File storage for Application file data (AWS), backups of system data, and backup of general company data. Data processing in EU and USA.

1.2.3 **ConvertIO** (Larncac, Cyprus). File conversion service used when assisting customers with onboarding. Data processing in EU.

1.2.4 **DocuSign** (San Francisco, USA). Electronic signing of documents. Data processing in EU and USA.

1.2.5 **Sentry** (San Francisco, USA). Cloud-based application and error monitoring platform. Data processing in taking place on the Google Cloud platform, which is located in both Americas, Europe, Middle east and Asia Pacific.

1.2.6 **Datadog** (New York, USA). Cloud based for application and error monitoring. Data processing in EU and USA.

1.2.7 **Snowflake** (Bozeman, USA). Provides a cloud data warehouse to store and transform data for use in business analytics. Data processing in EU and USA.

1.2.8 **Fivetran** (Oakland, USA). Cloud based application to extract data from source data systems and load into Snowflake. Data processing in UK, EU and USA.

1.2.9 **dbt** (Philadelphia, USA). Application for modelling, testing and documenting internal data. Data processing in EU and USA.

1.2.10 **Looker** (Santa Cruz, USA). Provides data visualisation services for business analytics. Data processing in EU and USA.

1.2.11 **FullStory** (Atlanta, USA). Product analytics used when developing new features and services. Data processing in USA and the EU.

1.2.12 **LaunchDarkly** (Oakland, USA). Feature manager used when launching new features in the services. Data processing in USA.

1.2.13 **SendSafely** (Remote, USA). File encryption service. Data processing in USA and EU.

1.3 CUSTOMER SERVICE

These third-party sub-processors provide systems that allows us to provide customer support and to help us onboard customers and deliver the Primary Services generally.

1.3.1 **Google LLC** (California, USA)**.** Provides a cloud-based file system (G Suite), where we store customer data as necessary to deliver the Primary Services, such as to assist with onboarding. Data processing in the UK, EU and USA.

1.3.2 **HubSpot Ireland Ltd.** (Dublin, Ireland). Provides a cloud-based customer relationship management system, where we store customer contact data as necessary to deliver and improve the Primary Services. Data processing in the European Economic Area ("EEA"), Switzerland and USA, and as necessary to provide services in specific cases, third countries for which the European Commission has issued an adequacy decision or for which Hubspot ensures that a legal mechanism achieving adequacy is in place.

1.3.3 **Slack** (San Francisco, USA). Provides a cloud-based collaboration system), where we may reference customer data as necessary to deliver and improve the Primary Services. Data processing in EU and USA.

1.3.4 **Atlassian** (Sydney, Australia) Provides a cloud-based bug tracking system, where we may process end user data to the extent necessary to reproduce and fix bugs, and in general as necessary to deliver and improve the Primary Services. Data processing in the EU, USA, Singapore, and Australia

1.3.5 **Intercom** (San Francisco, USA) Provides a cloud-based user support and engagement platform, where we store customer contact and product interaction data as necessary to deliver and improve the Primary Services. Data processing in EU and USA.

1.3.6 **Notion** (San Francisco, USA) Provides a cloud-based internal collaboration system, much like an intranet, where we may reference customer data as necessary to deliver and improve the Primary Services. Data processing in EU and USA.

1.3.7 **Totango** (Redwood City, USA). Customer success management software. Data processing in EU and USA.

1.4 PAYMENTS AND KYC

These third-party sub-processors provide systems that allows us to handle customer subscriptions and card payments.

1.4.1 **Stripe** (San Francisco, USA). Handling of subscriptions, email invoicing and credit card payments. Data processing in the European Economic Area ("EEA"), Switzerland and USA, and as necessary to provide services in specific cases, third countries for which the

European Commission has issued an adequacy decision or for which Stripe ensures that a legal mechanism achieving adequacy is in place.