

Version date: 16 September 2022

PARTIES

| | |
|--|---|
| <p>Juralio Technology Ltd ('JTL' or 'Processor')</p> <p>A Scottish limited company with company number SC571514 and registered office is at Unit 8, 20 Greenmarket, Dundee DD1 4QB, Scotland.</p> | <p>An individual or organisation who has signed up to use the Juralio software product via JTL's website, Juralio.com ('You' or 'Controller')</p> |
|--|---|

VARIABLES

| | | |
|--|--|--|
| Parties' relationship | Controller to Processor. | |
| Parties' roles | JTL is the data processor and you are the data controller. | |
| Contacts | JTL / Processor | You / Controller |
| | Chief Operating Officer info@juralio.com | Any of the email addresses associated with organisation administrator accounts in Customer's Juralio organisation as defined in the Main Agreement |
| Main Agreement | <p>Product terms of use published on JTL's Juralio.com website, including any subsequent amendments in effect at the relevant time.</p> <p>Note: this document is the Data Protection Agreement mentioned in the Main Agreement.</p> | |
| Term | <p>Start date: on you signing up to use Juralio via JTL's Juralio.com website and indicating agreement to this Data Processing Agreement</p> <p>End date: when the Main Agreement has been terminated and personal data is no longer being processed by JTL as envisaged by that agreement.</p> <p>Note: this data protection agreement may be amended or replaced during its term by the procedure stated in the Main Agreement.</p> | |
| Breach Notification Period | 24 hours | |
| Sub-processor Notification Period | At least 14 days before the new sub-processor takes effect. | |
| Liability Cap | Each party's aggregate liability will not exceed the liability cap specified in the Main Agreement. | |
| Governing Law and Jurisdiction | As in the Main Agreement. The arbitration provision there prevails over clause 5.9 of this Data Protection Agreement. | |
| Data Protection Laws | <p>The laws of the United Kingdom and European Union on processing of personal data, including</p> <ul style="list-style-type: none"> ● UK: Data Protection Act 2018 and the UK GDPR ● EU: GDPR (Regulation 2016/67) | |
| Services related to processing | <ul style="list-style-type: none"> ● Provision by JTL to you of access to the Juralio software product under the Main Agreement | |

| | |
|---|--|
| | <ul style="list-style-type: none"> Any related services which may be provided by JTL to you under the Main Agreement or a separate agreement. |
| Duration of processing | <p>During the effective period of the Main Agreement and, following its termination, until any personal data associated with your Juralio organisation has been deleted.</p> <p>In the context of clause 2.2(k), please note that the Main Agreement provides for data to be</p> <ul style="list-style-type: none"> retained by JTL for 90 days after termination of the Main Agreement, and available for return to you if requested; then deleted no longer than 180 days after termination of the Main Agreement unless retention is legally required. |
| Nature and purpose of processing | Performing the Main Agreement. |
| Types of personal data | <ul style="list-style-type: none"> Names Email addresses, phone numbers, home addresses and other contact information CVs Identification numbers (e.g. for employees) IP addresses Any other personal data added to the instance of the Juralio software to which the Main Agreement relates by you or by individuals for whom you have responsibility under the Main Agreement |
| Data subjects | <p>Anyone about whom personal data has been added to the Juralio instance to which the Main Agreement relates.</p> <p>This may include:</p> <ul style="list-style-type: none"> You, if you are an individual, Individuals associated directly or indirectly with <ul style="list-style-type: none"> you (for example, your colleagues, employees, directors, consultants, secondees, volunteers, agents, friends and family); or your counterparties, advisers, clients, consultants, experts, shareholders, suppliers, providers, complainants, correspondents, enquirers, relatives, guardians, associates, Any other individual about whom personal data is added to your organisation in the Juralio software. |
| Special provisions | <p>1. Costs. For the purpose of clause 2.2(h)(ii), where requests are excessive, in particular because of their repetitive character or are otherwise manifestly unfounded or excessive, JTL may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on</p> |

| | |
|----------------------------------|--|
| | <p>the request.</p> <ol style="list-style-type: none"> 2. Deletion and return of data. Please see the Duration of processing section above for how JTL meets the return and deletion requirements of clause 2.2(k). 3. Privacy notices. Please note that, as data controller, legal responsibility rests with you to provide any applicable privacy notices to data subjects in connection with the processing of personal data envisaged by this data protection agreement. 4. No special category data. At this time, Juralio is not intended for the processing of special category data. As such, you must not add such data to Juralio or provide any such data to JTL. You must also take reasonable steps to ensure that individuals for whose conduct you are responsible under the Main Agreement do not do these things. If this nevertheless occurs, you must promptly remove such data upon becoming aware of it. <p>Note: the UK legal definition of special category data is:</p> <ul style="list-style-type: none"> ● personal data revealing racial or ethnic origin; ● personal data revealing political opinions; ● personal data revealing religious or philosophical beliefs; ● personal data revealing trade union membership; ● genetic data; ● biometric data (where used for identification purposes); ● data concerning health; ● data concerning a person's sex life; and ● data concerning a person's sexual orientation. <p>Further information is available on the UK ICO website.</p> |
| <p>Transfer mechanism</p> | <p>Where Customer transfers personal data from the UK or EEA to a jurisdiction which is not considered 'adequate' under UK or EEA laws, JTL will implement appropriate protections to meet international transfers of personal data requirements under applicable Data Protection Laws.</p> <p>This includes implementing the following, where relevant:</p> <ul style="list-style-type: none"> ● For transfers from the EEA: the SCCs - that is, the standard contractual clauses approved by the European Commission, in the version applicable at the relevant time. ● For transfers from the UK: the IDTA - that is, the international data transfer agreement and related addendum issued by the UK ICO, in the version applicable at the relevant time. <p>Note: the UK IDTA is effective from 21 March 2022 but with transitional periods in which the EU SCCs may be used instead for transfers out of the UK (i) up to 21 September 2022 for existing contracts and (ii) up to 21 March 2024 for new contracts.</p> |

ANNEX 1

Security measures. Technical and organisational measures to ensure the security of the data

- JTL's parent company Juralio Ltd maintains an information security management system (ISMS) consistent with that company's ISO 27001 certification. That ISMS is designed to maintain the confidentiality, integrity and availability of information, including that held on the Juralio software.
- JTL operates consistently with that certification and system and will continue to do so.
- JTL will promptly
 - notify you of any loss of ISO 27001 certification by Juralio Ltd,
 - notify you of any material reduction in the level of assurance provided by the ISMS,
 - notify you of any information security incident which JTL or Juralio Ltd know or ought to know about which jeopardises the confidentiality, integrity or availability of information relevant to you;
 - provide reasonable assistance and co-operation to help you understand and mitigate any material harm or risk resulting from such a loss, reduction or incident.

ANNEX 2

Sub-processors. Current sub-processors

Amazon Web Services (aws.amazon.com) (aka AWS)

Activity: hosting the Juralio software, database and the associated data processing.

Data hosted in: UK

Conva Ventures Inc (usefathom.com) (product: Fathom)

Activity: analytics of how the Juralio product and website are being used, for the purpose of improving them and identifying any problems.

Data hosted in: EEA

Not So Big Tech Ltd (sheety.com) (product: Sheety)

Activity: processing of information entered into forms by individual within our product to inform us about their needs, roles and use cases. This product is used to transfer such information into a Google Sheet for review.

Data hosted in: EEA

Google (workspace.google.com) (product: Google Workspace)

Activity: processing the information mentioned above (in relation to use of sheety.com) in Google Sheets.

Data hosted in: EEA

Help Scout PBC (helpscout.com)

Activity: handling end user support inquiries. This service processes the name and email address of the user, their IP address and the content of their query and our response.

Data hosted in: **United States** and anywhere else in the world where Help Scout, its affiliates or its sub-processors maintain data processing operations.

- In the event of transfers of personal data from the UK or EEA to Helpscout, the EU SCCs apply as set out in Helpscout's data processing agreement - <https://www.helpscout.com/company/legal/dpa/>
- Please see the Transfer mechanism section above for the transitional applicability of EU SCCs to UK transfers.

Stripe, Inc, Stripe Payments Europe, Limited and Stripe Payments UK, Ltd (stripe.com)

Activity: payment and invoice processing. This service processes the name and email address of the user, their IP address, payment card details (including number, expiration date and CVC), invoicing address and payment history. It also processes other personal information described at <https://stripe.com/gb/privacy-center/legal>

Data hosted in: **Ireland, the United States** and anywhere else in the world where Stripe, its affiliates or its sub-processors maintain data processing operations.

- In the event of transfers of personal data from the UK or EEA to Helpscout, the EU SCCs apply, as indicated on Stripe's website-
- [https://support.stripe.com/questions/does-stripe-offer-the-new-uk-addendum-to-the-standard-contractual-clauses-\(sccs\)?local_e=en-GB](https://support.stripe.com/questions/does-stripe-offer-the-new-uk-addendum-to-the-standard-contractual-clauses-(sccs)?local_e=en-GB)
- Please see the Transfer mechanism section above for the transitional applicability of EU SCCs to UK transfers.

Unsplash Inc (unsplash.com)

Activity: provision of images for templates in Juralio via the Unsplash API. This service processes the IP address of the user but section 6 of the [Unsplash API Terms](#) states that Unsplash does not link it to other personal information.

Data hosted in: the data transfer section of the [Unsplash Privacy Policy](#) states that it may store data in any country but, if applicable, will comply with GDPR requirements on transfer from the EU/EEA.

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.

CONTROLLER-PROCESSOR RELATIONSHIP

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 Main Agreement,
 - (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 Controller'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 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.** 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) Main Agreement.
- 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.