NOTICE: If you are a Jasper for Business Customer and would like to receive a DocuSign of this DPA for countersignature, please fill out the request form here .

DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "DPA") constitutes an integral part of all agreements between Customer (as defined in the Master Subscription Agreement or otherwise identified on the signature block below) and Jasper AI, Inc. (the "Processor" or "Jasper") a Delaware corporation with offices at 3001 Bee Caves Road, Suite 100 B, Rollingwood, Texas 78746, including the Master Subscription Agreement or under any services agreement or similar agreement (collectively "Agreement"), and reflects the Parties' agreement with respect to the Processing of Controller Data.

In providing the Services to Customer pursuant to the Agreement, Jasper may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith. This DPA supplements the Agreement and in the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA prevail with regard to the specific subject matter of this DPA. This DPA is effective on the date that it, or the Agreement that references and incorporates it, has been duly executed by both Parties ("Effective Date"), and amends, supersedes and replaces any prior agreement relating to data processing and/or data protection entered into by the Parties.

1. DEFINITIONS

Any capitalized terms used but not defined in this DPA has the meaning provided to it in the Agreement,

(a) "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. Control, for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

(b) "Applicable Data Protection Law" means (a) all data protection laws and regulations applicable to the European Economic Area and Switzerland, including (i) the General Data Protection Regulation 2016/679 ("GDPR"), and EU Member State laws supplementing the GDPR; (b) the UK Data Protection Act of 2018, and the UK GDPR (collectively "UK Data Protection Laws"); and (c) any other laws and regulations applicable to Processor's Processing of Controller Data under the Agreement.

(c) "Authorized Affiliate" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Customer, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

(d) "California Privacy Law" means the California Consumer Privacy Act until January 1, 2023, and thereafter will refer to the California Privacy Rights Act.

(e) "Controller" as used in this DPA, means Customer.

(f) "Controller Data" means any Personal Data Processed by Processor on behalf of Customer pursuant to or in connection with the Agreement.

(g) "Customer" means the entity which determines the purposes and means of the Processing of Personal Data and includes any Authorized Affiliates of the Customer, and to the extent applicable includes a "Business" as defined under California Privacy Law.

(h) "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Controller Data transmitted, stored or otherwise processed by Processor.

(i) "Permitted Purpose" means the use of the Controller Data to the extent necessary for provision of the Services by Processor to the Controller.

(j) "Personal Data" means any information relating to an identified or identifiable natural person that relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular natural person.

(k) "Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, sharing, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(l) "Processor" means Jasper AI, Inc. and any Jasper entities, including its Affiliates, which Processes Personal Data on behalf of the Customer, and to the extent applicable, includes a "Service Provider" as defined under the California Privacy Law.

(m) "Regulator" means any supervisory authority with authority under Applicable Data Protection Law over all or any part of the provision or receipt of the Services or the Processing of Personal Data.

(n) "Restricted Transfer" means: (i) where the EU GDPR applies, transferring Personal Data from the EEA to a country outside the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, transferring Personal Data from the United Kingdom to any other country which is not subject based on adequacy regulations under Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss Federal Act on Data Protection of June 19, 1992 ('Swiss DPA") applies, transferring Personal Data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

(o) "Services" means the products and services that are ordered by Controller through a link or via an Order pursuant to the Agreement and made available online by Processor.

(p) "Sub-processor" means any third-party data processor engaged by Processor, who receives Personal Data from Processor for processing on behalf of Controller and in accordance with Controller's instructions (as communicated by Processor) and the terms of its written subcontract.

(q) The terms, "Commission", "Data Subject", "Member State", and "Supervisory Authority" shall have the same meaning as in the Applicable Data Protection Laws, and their cognate terms shall be construed accordingly.

2. PURPOSE

2.1 Controller and Processor have entered into the Agreement pursuant to which Controller is granted a right to access and use the Services. In providing the Services, Processor will engage, on behalf of Controller, in the processing of Personal Data submitted to and stored within the Services by Controller.

2.2 The Parties are entering into this DPA to ensure that the Processing by Processor of Controller Data, within the Services by Controller and/or on its behalf, is done in a manner compliant with Applicable Data Protection Law and its requirements regarding the collection, use and retention of Personal Data of Data Subjects.

3. AUTHORITY

3.1 Roles of the Parties

(a) To the extent the GDPR or UK Data Protection Laws apply to the Controller Data, the Parties acknowledge and agree that Customer is a Controller and Jasper is a Processor acting on behalf of Customer. When Customer is acting as a Processor of Controller Data, Jasper is a sub-processor of the Customer.

(b) For purposes of California Privacy Law, Jasper will act as a Service Provider in its performance of its obligations under the Agreement. Jasper (i) will only use Controller Data to provide the Services under the Agreement; (ii) will not collect, retain, use, sell, disclose or otherwise process any Controller Data, for any purpose other than providing the Services under the Agreement, or as otherwise permitted. Notwithstanding anything to the contrary in the Agreement (including this DPA), Controller acknowledges that Processor shall have a right to Process Personal Data in relation to the support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. Jasper understands the restrictions in this Section 3.1(b) and certifies that it understands its obligations under the California Privacy Law and will comply with them.

3.2 Controller's Instructions. Customer represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including Applicable Data Protection Law, in respect of its Processing of Controller Data and any Processing instructions it issues to Processor; and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Applicable Data Protection Law for Processor to process Controller Data for the purposes described in the Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Controller Data and the means by which Customer acquired the Controller Data. Controller specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the California Privacy Law.

3.3 Purpose Limitation. Processor shall process Controller Data only in accordance with Customer's documented lawful instructions as set forth in this DPA, for Permitted Purposes, as necessary to comply with applicable law, or as otherwise agreed to in writing. The Parties agree that the Agreement and this DPA set out Customer's complete and final instructions to Processor in relation to the processing of Controller Data, and processing outside the scope of these instructions (if any) shall require prior written agreement between the Parties.

3.4 Data Subject and Regulator Requests . Customer shall be responsible for communications and leading any efforts to comply with all requests made by Data Subjects under the Applicable Data Protection Law, and all communications from Regulators that relate to the Controller Data.

4. OBLIGATIONS OF PROCESSOR

4.1 **Confidentiality**. Processor will restrict access to the Controller Data to its personnel who need access to meet Processor's obligations under the Agreement. Processor shall take commercially reasonable steps to ensure the reliability of any Processor personnel engaged in the Processing of Controller Data.

4.2 **Disclosure to Third Parties**. Processor will not disclose Controller Data to third parties except as permitted by this DPA or the Agreement. If requested or required by a competent governmental authority to disclose Controller Data, to the extent legally permissible and practicable, Processor will provide Customer with sufficient prior written notice in order to permit Customer the opportunity to oppose any such disclosure.

4.3 **Retention**. Processor will retain Controller Data only for as long as the Customer deems it necessary for the Permitted Purpose, or as required by Applicable Data Protection Law. At the termination of this DPA, or upon Customer's written request, Processor will either destroy or return the Controller Data to Customer, unless legal obligations require storage of the Controller Data.

4.4 **Data Subject and Regulator Requests**. Processor shall, to the extent legally permitted, promptly notify Controller in writing of any complaints, questions or requests received from Data Subjects or Regulators regarding the Controller Data. In taking into account the nature of the Processing and to the extent reasonably possible, Processor will provide Controller with commercially reasonable assistance in relation to the handling of a Data Subject's request. To the extent Controller, in its use of the Services, does not have the ability to correct, block or delete Controller Data, Processor shall comply with any commercially reasonable request by Controller to facilitate such actions to the extent Processor is legally permitted to do so.

4.5 **Data Protection Impact Assessment**. To the extent required under the Applicable Data Protection Law, upon Customer's request, Processor will provide reasonable assistance to Customer necessary for Customer to fulfil its obligation under the Applicable Data Protection Law to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Processor.

4.6 **Security**. Processor will implement and maintain appropriate technical, physical and administrative measures to protect Controller Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access (a "Data Security Breach"), provided that such measures shall take into account 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, so as to ensure a level of security appropriate to the risks represented by the processing and the nature of the Controller Data to be protected.

(a) Customer acknowledges that the security measures are subject to technical progress and development and that Processor may update or modify the security measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services

purchased by Customer. Customer is responsible for reviewing the information made available by Processor relating to data security and making an independent determination as to whether the Services meet Controller's requirements and legal obligations under Applicable Data Protection Law.

(b) Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Controller Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Controller Data uploaded to the Services.

5. DATA BREACH

5.1 Data Breach. If Processor becomes aware of any Data Breach, Processor will promptly: notify Customer of the Data Breach, but in no event later than seventy-two (72) hours after Processor has confirmed a Data Breach impacting Controller Data; investigate the Data Breach and provide Customer with information about the Data Breach; and take reasonable steps to mitigate the effects and to minimize any damage resulting from the Data Breach. Processor's obligation to report or respond to a Data Breach under this Section is not and will not be construed as an acknowledgement by Processor of any fault or liability with respect to the Data Breach.

5.2 Coordination. Processor will provide reasonable assistance to Customer in fulfilling its obligations to notify Data Subjects and the relevant authorities in relation to a Data Breach, provided that nothing in this section shall prevent either party from complying with its obligations under the Applicable Data Protection Laws. The Parties agree to coordinate in good faith on developing the content of any related public statements.

5.3 Caused by Controller. The obligations in this section shall not apply to a Data Breach that is caused by Customer.

6. AUDITS

6.1 Customer may audit Processor's compliance with this DPA up to once per year, unless requested by a Supervisory Authority. Such an audit will be conducted by an independent third party ("Auditor") reasonably acceptable to Processor. Before the commencement of any such on-site audit, Customer must submit in writing a detailed proposed audit plan to Processor at least 30 business days in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration and date of the audit, as well as the proposed Auditor. Processor will review the proposed audit plan and provide Customer with any concerns or questions and will work cooperatively with Customer to agree on a final audit plan. Prior to the start of an audit, the Parties will agree to reasonable time, duration, place and manner conditions for the audit, and a reasonable reimbursement rate payable by Customer to Processor for Processor's audit expenses. The results of the audit and all information reviewed during such inspection will be deemed Processor's confidential information, and subject to the Confidentiality provisions in the Agreement. Notwithstanding any other terms, the Auditor may only disclose to the Customer any specific violations of the DPA, if any, and the basis for such findings, and shall not disclose to the Customer any of the records or information reviewed during the inspection.

7. USE OF SUB-PROCESSORS

7.1 **General Consent.** Customer acknowledges and agrees that Processor may appoint Sub-processors to assist it in providing the Service and Processing Controller Data provided that such Sub-processors agree to (a) act only on Processor's instructions when Processing the Controller Data (which instructions shall be consistent with Controller's processing instructions to Processor); and (b) protect the Controller Data to a standard consistent with the requirements of this DPA.

7.2 **Sub-processor List**. The names of all Sub-processors used as of the Effective Date for the processing of

Controller Data under this DPA is set forth on Schedule 3.

7.3 **Objection to New Sub-Processor.** Processor will provide 10 (ten) days' notice of a new sub-processor to Customer. Customer may object to Processor's appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is in writing and based on reasonable grounds relating to data protection, and such objection is made within 10 (ten) days after the notice of the new sub-processor provided by Processor. Any such written objection shall include Customer's specific reasons for its objection and proposed options to mitigate alleged risk, if any. In such an event, the Parties agree to discuss commercial reasonable alternative solutions in good faith. If the parties cannot reach a resolution within sixty (60) days from the date of Processor's receipt of Customer's written objection, Customer may discontinue the use of the affected Services by providing written notice to Processor. In the absence of timely and valid objection by Customer, such new Sub-processor may be commissioned to Process Controller Data.

7.4 **Liability**. Processor shall be liable for the acts and omissions of its Sub-processors use to provide the Services to the same extent Processor would be liable if performing the services of each Subprocessor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

8. INTERNATIONAL PROVISIONS

8.1 Jurisdiction Specific Terms. To the extent Processor Processes Controller Data originating from and protected by Applicable Data Protection Law in one of the jurisdictions listed in Schedule 4 (Jurisdiction Specific Terms) of this DPA, the terms specified in Schedule 5 with respect to the applicable jurisdiction(s) apply in addition to the terms of this DPA.

8.2 Restricted Transfers. To the extent Customer's use of the Services involves a Restricted Transfer of Controller Data, the terms set forth in Schedule 4 (Cross Border Transfer Mechanisms) will apply. In the event of any conflict or inconsistency between this DPA and the terms set forth in Schedule 4, the terms in Schedule 4 shall apply.

9. LIMITATION ON LIABILITY

9.1 In no event will either Party or their respective directors, officers, agents, or employees be liable to the other party for any reason, whether in contract or in tort for any claims or liability arising out of or based upon this DPA, excess of the amount actually paid by the Customer to Processor in the twelve months preceding the first incident out of which the liability arose, regardless of the form in which any legal or equitable action may be brought.

9.2 For the avoidance of doubt, Processor's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

10. MISCELLANEOUS

10.1 Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to that jurisdiction alone, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions hereof, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. The parties will attempt in good faith to agree upon a valid and enforceable provision that is a reasonable substitute and shall incorporate such substitute provision into this DPA.

10.2 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Law.

10.3 Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Law, in the name and on behalf of its Authorized Affiliates, if and to the extent Jasper processes Personal Data for which such Authorized Affiliates qualify as the Controller.

10.4 This DPA may not be amended or modified except by the mutual agreement of the Parties; provided, however, Customer will be notified thirty (30) days in advance of any amendments or modifications to this DPA, which shall take effect in the next billing cycle, and Customer's continued use of the Services shall constitute acceptance of such amendments and/or modifications. This DPA may be executed in counterparts. The terms and conditions of this DPA are confidential and each Party agrees and represents, on behalf of itself, its employees and agents to whom it is permitted to disclose such information that it will not disclose such information to any third party; provided, however, that each Party shall have the right to disclose such information to its officers, directors, employees, auditors, attorneys and third party contractors who are under an obligation to maintain the confidentiality thereof and further may disclose such information as necessary to comply with an order or subpoena of any administrative agency or court of competent jurisdiction or as reasonably necessary to comply with any applicable law or regulation. Controller may not, directly or indirectly, by operation of law or otherwise, assign all or any part of its rights under this DPA or delegate performance of its duties under this DPA without Processor's prior consent, which consent will not be unreasonably withheld. Processor may, without Controller's consent, assign this DPA to any affiliate or in connection with any merger or change of control of Processor or the sale of all or substantially all of its assets provided that any such successor agrees to fulfil its obligations pursuant to this DPA. Subject to the foregoing restrictions, this DPA will be fully binding upon, inure to the benefit of and be enforceable by the Parties and their respective successors and assigns.

Unless otherwise incorporated by reference in an Agreement, the Parties' authorized signatories have duly executed this DPA as of the Effective Date:

Jasper AI, Inc.	**Customer**
Signature: _____	Customer: _____
Print Name: _____	Signature: _____
Title: _____	Print Name: _____
	Title: _____

Schedule 1 – Details of Processing

1. Categories of Data Subjects

The personal data transferred concern the following categories of Data Subjects: The categories of data subjects are within the control of the Controller and may include individuals about whom data is provided to Processor by or at the direction of the Controller pursuant to the Agreement

2. Types of Personal Data Transferred

The personal data transferred concern the following categories of data: the categories of Personal Data are within the control of the Controller and may include data relating to individuals to the extent provided to Processor by or at the direction of the Controller pursuant to applicable terms of service between them.

3. Sensitive Data Transferred

The personal data transferred concern the following special categories of data: the categories of Personal Data are within the control of the Controller and may include data relating to individuals to the extent provided to Processor by or at the direction of the Controller pursuant to applicable terms of service between them.

4. Frequency of the Transfer.

Continuous.

5. Nature of Processing

The Personal Data transferred will be subject to the following basic processing activities: Processor will Process Controller Data as necessary to perform the Services pursuant to the Agreement, and as further instructed by Customer in its use of the Services. The processing operations are the Services that are used by the Controller.

6. Purpose of Processing

The purpose of the Processing of Controller Data by Processor is to provide Customer with the Services under the Agreement.

7. Duration of the Processing

The Term of the Agreement, plus the period from the expiry of such Term until deletion of all Controller Data by the Processor in accordance with the DPA.

Schedule 2 – Technical and Organisational Security Measures

Organization Security

Personnel

Security of the Jasper environment is the responsibility of all Jasper employees, contractors, and temporary workers who have access to Jasper information systems. All personnel are required to understand and follow program policies and processes.

Before access is granted, all personnel are required to review the employee handbook, sign a confidentiality agreement, and have security training. Training and agreements cover among other elements: privacy, information security, physical security, acceptable use, and incident reporting. Upon termination of employment or contract, all access is removed promptly.

Security and Awareness Training

During the onboarding process all employees are given information security and privacy training. They are also required to receive that training annually and acknowledge that they have read and understand Jasper information security policies.

Some technical teams require elevated access to information systems to perform their job duties. These teams receive annual specialized training specific to those roles and responsibilities. All employees are required to report potential security and privacy related issues to the appropriate internal teams. They acknowledge that failure to do so may result in disciplinary measures up to and including termination.

Complying with Laws and Regulations

Jasper works with legal representation that ensures the company and its employees identify and follow applicable laws, regulations, and contractual obligations. Jasper requires all personnel to behave ethically and to comply with the law.

SDLC

Jasper utilizes an effective secure software development lifecycle (SDLC) including requirements like code must be reviewed and approved before being pushed into production. This program covers feature enhancements, bug fixes, emergency changes, and

problem and incident management. The agile nature of the process allows for teams to follow their own release cycles and provides continuous improvement without having other teams creating a bottleneck.

All code is checked into a version control repository with role based access controls. The Jasper code repository is controlled by strong authentication, including MFA.

Penetration Testing

Jasper engages independent 3rd parties to conduct annual penetration tests. Results of these tests are shared with management. An overview of the results may be shared with customers upon request. The Jasper information security team reviews and prioritizes findings and tracks them to resolution. Customers are not allowed to conduct their own penetration tests of the Jasper environment. Any exceptions must have written approval from the Jasper VP of Engineering.

Technical Controls - Protecting Jasper Customer Data

Data Encryption

Jasper encrypts data at rest and in transit using industry best practices. All information transmitted to users is done via HTTPS using TLS 1.2 or higher with AES 256 SHA2 signatures (defaulting to TLS 1.3 based on client ability). Data at rest is encrypted at the storage level using AES256. Database connections are verified using TLS certificates, and encrypted in transit using SSL.

Password Security

Jasper uses industry leading services to securely authenticate users. Passwords are hashed and salted using BCrypt or equivalent (a one way hashing algorithm with high entropy) that is designed to be secure and mitigate against user database breach/theft. User passwords are never stored in plaintext.

Cloud Provider

Jasper utilizes serverless instances across multiple cloud providers to ensure High Availability of all services. Cloudflare CDN is used to provide faster access to Jasper's application as well as to help prevent DDOS attacks. Cloudflare WAF is used to protect against commonly known web application vulnerabilities.

Authorization

All access to Jasper systems is based on a least privilege model; meaning personnel are only granted the access that they need to

perform their current job responsibilities. Reviews of access are done on at least an annual basis. When personnel are terminated their access is removed immediately.

System Monitoring, Logging, and Alerting

Jasper has a centralized log management system which facilitates logging, correlation and monitoring of network, operating system, and database logs. Centralized logging is enabled for all production systems.

These logs are reviewed for indications of compromise and alerted upon when predetermined thresholds are met. The Information Security team is responsible for incident handling when monitoring and alerting thresholds are reached and tracks the security events through to remediation or escalation. Production infrastructure is also monitored to ensure availability. Jasper maintains an incident response plan to effectively respond to any deviation from normal system performance.

Endpoint Security

Jasper endpoints are managed by industry standard management tools to ensure policies are followed and systems stay up to date with all relevant security patches.

Vulnerability Management

Reported vulnerabilities are remediated promptly following industry best practices. Production systems are monitored for vulnerabilities, and operating systems are refreshed regularly to stay current.

Schedule 3 – Sub-processor List

The Customer has authorized the use of the Sub-processors located at legal.jasper.ai/#sub-processors.

Schedule 4 – Cross Border Transfer Mechanisms

1. Definitions

1. "EC" means the European Commission.
2. "EEA" means the European Economic Area.
3. "EEA Personal Data" is Controller Data collected from data subjects when they are located in the EEA.
4. "Standard Contractual Clauses" means (i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for transferring personal data to third countries under Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCC"); (ii) where the UK GDPR applies, the

   the International Data Transfer Agreement: Controller to Processor under Section 119A of the Data Protection Act 2018 ("UK SCC"); and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner ("Swiss SCC").

5. "Swiss Personal Data" means Controller Data collected from data subjects when they are located in Switzerland.
6. "UK Personal Data" means Controller Data collected from data subjects when they are located in the United Kingdom.

2. Cross-Border Data Transfer Mechanisms

2.1. EEA Personal Data. The Parties agree that the Standard Contractual Clauses will apply to Controller Data that is transferred via the Services from the EEA or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland that is: (a) not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for Personal Data. To the extent applicable, the Standard Contractual Clauses will be deemed entered into (and incorporated into this Addendum by this reference) and are deemed executed by each of the Parties acting on their own behalf and on behalf of their Affiliates (where applicable) without the need for any further signature from either party and completed as follows:

(a) Module Two (Controller to Processor) of the Standard Contractual Clauses will apply where Customer is a Controller of Controller Data and Jasper is Processing Controller Data.

(b) Module Three (Processor to Processor) of the Standard Contractual Clauses will apply where Customer is a Processor of Controller Data and Jasper is Processing Controller Data.

(c) For each Module, where applicable:

(i) in Clause 7 of Standard Contractual Clauses, the optional docking clause will not apply;

(ii) the audits described in Clause 8.9(c) and (d) of the SCC shall be carried out in accordance with Section 6 of the DPA

(iii) in Clause 9 of the Standard Contractual Clauses, Option 2 will apply and the time period for prior notice of sub-processor changes will be as set forth in the DPA;

(iii) in Clause 11 of the Standard Contractual Clauses, the optional language will not apply;

(iv) the liability described in Clause 12 shall in no event exceed the limitations set forth in the DPA, and that under no circumstances and under no legal theory (whether in contract, tort, negligence or otherwise) will either party to this DPA, or their Affiliates, officers, directors, employees, agents, service providers, suppliers, or licensors be liable to the other party or any third party for any lost profits, lost sales of business, lost data (being data lost in the course of transmission via Customer's systems or over the Internet through no fault of Supplier), business interruption, loss of goodwill, or for any type of indirect, incidental, special, exemplary, consequential or punitive loss or damages, regardless of whether such party has been advised of the possibility of or could have foreseen such damages. For the avoidance of doubt, this section shall not be construed as limiting the liability of either party with respect to claims brought by data subjects;

(v) the certification of deletion of Controller Data that is described in Clause 16(d) of the SCC shall be provided by Processor to Customer only upon Customer's request.

(vi) in Clause 17 (Option 1), the Standard Contractual Clauses will be governed by Irish law;

(vii) in Clause 18(b) of the Standard Contractual Clauses, disputes will be resolved before the courts of Ireland;

(viii) in Annex I, Part A of the Standard Contractual Clauses:

Data Exporter: Customer.

Contact details: See signature line of DPA.

Data Exporter Role: The Data Exporter's role is set forth in Section 3 (Relationship of the Parties) of this DPA.

Signature and Date: By entering into the DPA, Data Exporter is deemed to have signed these Standard Contractual Clauses

incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

Data Importer: Processor (Jasper)

Contact details: John Bullough, privacy@jasper.ai

Data Importer Role: The Data Importer's role is set forth in Section 3 (Relationship of the Parties) of this DPA.

Signature and Date: By entering into the DPA, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the DPA.

(ix) in Annex I, Part B of the Standard Contractual Clauses:

The categories of data subjects: see Schedule 1 (Details of Processing) of this DPA.

The Sensitive Data transferred: see Schedule 1 (Details of Processing) of this DPA.

The frequency of the transfer is a continuous basis for the duration of the Agreement.

The nature of the processing: see Schedule 1 (Details of Processing) of this DPA.

The purpose of the processing: see Schedule 1 (Details of Processing) of this DPA.

The period for which the Personal Data will be retained: see Schedule 1 (Details of Processing) of this DPA.

(viii) in Annex I, Part C of the Standard Contractual Clauses: The Irish Data Protection Commission will be the competent supervisory authority;

(ix) Schedule 2 (Technical and Organizational Security Measures) of this Addendum serves as Annex II of the Standard Contractual Clauses; and

(xii) In relation to Swiss Personal Data:

(a) For purposes of Annex I.C under Clause 13 of Standard Contractual Clauses insofar as the data transfer is governed by the

Switzerland Federal Act on Data Protection of 19 June 1992 (SR 235.1; FADP) or the FADP's revised 25 September 2020 version, the Supervisory Authority shall be Switzerland's Federal Data Protection and Information Commissioner (FDPIC);

(b) The term "member state" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in Switzerland in accordance with Clause 18(c) of the Standard Contractual Clauses. The Standard Contractual Clauses shall also protect the data of Switzerland legal entities until the entry into force of the 25 September 2020 revised version of the Federal Act on Data Protection (revised FADP). Any references in the Standard Contractual Clauses to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA.

2.3 UK Personal Data. The parties agree that the Information Commissioner's Office's International Data Transfer Agreement, referred to hereafter as Standard Contractual Clauses, will apply to UK Personal Data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside the United Kingdom that is not recognized by the ICO as providing an adequate level of protection for Personal Data. To the extent applicable, the Standard Contractual Clauses will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

PART 1: TABLES

Table 1: Parties

Start Date	*See Effective Date of the DPA*	
The Parties	**Data Exporter (Controller)**	**Jasper - Data Importer (Processor)**
Parties' details	*See Section 2.1(c)(viii), above.*	*See Section 2.1(c)(viii), above.*
Key Contact	*See Section 2.1(c)(viii), above.*	*See Section 2.1(c)(viii), above.*

Table 2: Transfer Details

UK country's law that governs the IDTA:	☒ England and Wales ☐ Northern Ireland ☐ Scotland
Primary place for legal claims to be made by the	☒ England and Wales ☐ Northern Ireland

Parties	☐ Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: ☒ Exporter is a Controller ☐ Exporter is a Processor or Sub-Processor
The status of the Importer	In relation to the Processing of the Transferred Data: ☐ Importer is a Controller ☒ Importer is the Exporter's Processor or Sub-Processor ☐ Importer is **not** the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)
Whether UK GDPR applies to the Importer	☒ UK GDPR applies to the Importer's Processing of the Transferred Data ☐ UK GDPR does not apply to the Importer's Processing of the Transferred Data
Linked Agreement	**If the Importer is the Exporter's Processor or Sub-Processor** – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data: Name of agreement: DPA to which this Schedule 4 is attached. Date of agreement: Same as above. Parties to the agreement: Same as above. Reference (if any): None. **If the Exporter is a Processor or Sub-Processor** – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data: (*complete if applicable otherwise put N/A*) Name of agreement: Date of agreement: Parties to the agreement: Reference (if any):
Term	The Importer may Process the Transferred Data for the following time period: ☒ the period for which the Linked Agreement is in force ☐ time period: ☐ (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.
Ending the IDTA before the end of the Term	See Termination provision in the DPA to which this Schedule 4 is attached.
Ending the IDTA when the Approved IDTA changes	See Termination provision in the DPA to which this Schedule 4 is attached.
Can the Importer make further transfers of the Transferred Data?	☐ The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data). ☒ The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).
Specific restrictions when the Importer may	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1: ☒ if the Exporter tells it in writing that it may do so.

transfer on the Transferred Data	☐ to: ☐ to the authorised receivers (or the categories of authorised receivers) set out in: ☐ there are no specific restrictions.
Review Dates	☐ No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data First review date: The Parties must review the Security Requirements at least once: ☐ each month(s) ☐ each quarter ☐ each 6 months ☒ each year ☐ each year(s) ☐ each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment

Table 3: Transferred Data

Transferred Data	See Schedule 1 of the DPA to which this Schedule 4 is attached.
Special Categories of Personal Data	See Schedule 1 of the DPA to which this Schedule 4 is attached.
Relevant Data Subjects	See Schedule 1 of the DPA to which this Schedule 4 is attached.
Purpose	See Schedule 1 of the DPA to which this Schedule 4 is attached.

Table 4: Security Requirements

Security of Transmission	See Schedule 2 of the DPA to which this Schedule 4 is attached.
Security of Storage	See Schedule 2 of the DPA to which this Schedule 4 is attached.
Security of Processing	See Schedule 2 of the DPA to which this Schedule 4 is attached.
Organisational security measures	See Schedule 2 of the DPA to which this Schedule 4 is attached.

Technical security minimum requirements	See Schedule 2 of the DPA to which this Schedule 4 is attached.
Updates to the Security Requirements	☒ The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. ☐ The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

PART 2: EXTRA PROTECTION CLAUSES

Extra Protection Clauses:	
(i) Extra technical security protections	N/A
(ii) Extra organisational protections	N/A
(iii) Extra contractual protections	N/A

PART 3: COMMERCIAL CLAUSES

Commercial Clauses	See Agreement to which the DPA is attached.

PART 4: MANDATORY CLAUSES

The template IDTA A1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4. By entering into the DPA, the parties are deemed to have signed the IDTA, incorporated herein by reference, as of the Effective Date of the Agreement.

Schedule 5 – Jurisdiction Specific Terms

1. Australia

1.1 The definition of “Applicable Data Protection Law” includes the Australian Privacy Principles and the Australian Privacy Act (1988).

1.2 The definition of “Personal Data” includes “Personal Information” as defined under Applicable Data Protection Law.

2. Brazil

2.1 The definition of “Applicable Data Protection Law” includes the Lei Geral de Proteção de Dados (LGPD).

2.2 The definition of “Data Breach” includes a security incident that may result in any relevant risk or damage to data subjects.

2.3 The definition of “Processor” includes “operator” as defined under Applicable Data Protection Law.

3. Canada

3.1 The definition of “Applicable Data Protection Law” includes the Federal Personal Information Protection and Electronic Documents Act (PIPEDA).

4. European Economic Area (EEA)

4.1 The definition of “Applicable Data Protection Law” includes the General Data Protection Regulation (EU 2016/679) (“GDPR”).

4.2 Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

5. Israel

5.1 The definition of "Applicable Data Protection Law" includes the Protection of Privacy Law (PPL).

5.2 The definition of "controller" includes "Database Owner" as defined under Applicable Data Protection Law.

5.3 The definition of "processor" includes "Holder" as defined under Applicable Data Protection Law.

6. **Japan**

6.1 The definition of "Applicable Data Protection Law" includes the Act on the Protection of Personal Information (APPI).

6.2 The definition of "Personal Data" includes "Personal Information" as defined under Applicable Data Protection Law.

6.3 The definition of "Controller" includes "Business Operator" as defined under Applicable Data Protection Law.

6.4 The definition of "Processor" includes a business operator entrusted by the Business Operator with the handling of Controller Data in whole or in part (also a "trustee"), as described under Applicable Data Protection Law. As a trustee, Processor will ensure that the use of the Controller Data is securely controlled.

7. Singapore

7.1 The definition of "Applicable Data Protection Law" includes the Personal Data Protection Act 2012 (PDPA).

8. Switzerland

8.1 The definition of "Applicable Data Protection Law" includes the Swiss Federal Act on Data Protection.

9. United Kingdom (UK):

9.1 References in this Addendum to GDPR will to that extent be deemed to be references to the corresponding laws of the United Kingdom (including the UK GDPR and Data Protection Act 2018).

9.2 Notwithstanding anything to the contrary in this Addendum or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any UK GDPR fines issued or levied under Article 83 of the UK GDPR

against the other party by a regulatory authority or governmental body in connection with such other party's violation of the UK GDPR.