

# DATA PROCESSING ADDENDUM

## 1 APPLICATION OF THIS ADDENDUM

- 1.1 This Data Processing Addendum (**Addendum**) applies if the Processing (as defined below) of Data (as defined in our Terms and Conditions at <https://narrative.so/terms-and-conditions> (**Terms**)) is governed by the GDPR (as defined below).
- 1.2 If this Addendum applies, this Addendum forms part of the Terms between us and you (as defined in the Terms) and sets out the parties' agreement in relation to the processing of Data in accordance with the requirements of European Union data protection laws and regulations.
- 1.3 We are located in New Zealand, which the European Commission has determined provides adequate protection for the purposes of Article 45 of the GDPR. However, to provide you with additional assurance as to our data protection commitments, this Addendum also includes Standard Contractual Clauses (as defined below), which are pre-signed by us. If you would like to opt in to the Standard Contractual Clauses, please complete the necessary details, countersign the Standard Contractual Clauses, and return a counter-signed copy to us at **support@narrative.so**.
- 1.4 Except as varied in this Addendum (including the Standard Contractual Clauses, if applicable) all terms and conditions set out in the Terms continue to apply.

## 2 INTERPRETATION

- 2.1 Unless the context requires otherwise:
  - a capitalised terms used, but not defined, in this Addendum will have the meanings given to them in the GDPR (or, if not defined in the GDPR, the Terms);
  - b the rules of interpretation set out in the Terms apply to this Addendum; and
  - c references to *clauses* are references to the clauses in this Addendum.

- 2.2 In this Addendum:

*Applicable Data Protection Laws* means EU Data Protection Laws and any applicable data protection or privacy laws of any other country

*EEA* means the European Economic Area

*EU Data Protection Laws* means all laws and regulations, including laws and regulations of the European Union, the EEA and their member states and (if the United Kingdom ceases to be a member state) the United Kingdom, that apply to the Processing of Data under the Terms, including (where applicable) the GDPR

*GDPR* means the European Union General Data Protection Regulation 2016/679

*Instruction* means the instructions set out in clause 3.3 or agreed under clause 3.4

*Personal Data* means all Data which is personal data, personally identifiable information or personal information under Applicable Data Protection Laws (as applicable under those laws)

*Processing* means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. *Process* has a consistent meaning

*Standard Contractual Clauses* means the standard contractual clauses set out in Schedule 3, as may be amended under clause 12.1.

*Sub-Processor* means any person appointed by us or on our behalf to Process Personal Data on your behalf in connection with the Terms

- 2.3 If there is any conflict between any of the following, they will have precedence in the descending order of priority set out below:
- a the Standard Contractual Clauses;
  - b this Addendum; and
  - c the Terms.

### **3 PROCESSING OF PERSONAL DATA**

- 3.1 With respect to the Processing of Personal Data under the Terms:
- a you act as the Data Controller;
  - b we act as the Data Processor; and
  - c subject to clause 6, we may engage the Sub-Processors listed in Schedule 2.
- 3.2 We will comply with all Applicable Data Protection Laws that apply to our Processing of Personal Data on your behalf, including all EU Data Protection Laws that apply to Data Processors.
- 3.3 You must, when using the Service, comply with all Applicable Data Protection Laws that apply to your Processing of Personal Data, including all EU Data Protection Laws that apply to Data Controllers.
- 3.4 You instruct us to Process Personal Data and in particular, subject to clause 6, transfer Personal Data to any country or territory:
- a as reasonably necessary to provide the Service in accordance with the Terms;

- b as initiated through the use of the Service by you, your Personnel and other end users you allow to use the Service; and
  - c to comply with any further instruction from you (including by email or through our support channels) that is consistent with the Terms and this Addendum.
- 3.5 This Addendum and the Terms are your complete and final instructions for the Processing of Personal Data as at the time this Addendum takes effect. Any additional or alternate instructions must be agreed between us and you separately in writing.
- 3.6 We will not Process Personal Data other than on your Instructions unless required by any law to which we are subject, in which case we will to the extent permitted by applicable law inform you of that legal requirement before we Process that Personal Data.
- 3.7 As required by article 28(3) of the GDPR (and, if applicable, equivalent requirements of other Applicable Data Protection Laws), the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this Addendum are set out in Schedule 1. We may amend Schedule 1 from time to time on written notice to you as we reasonably consider necessary to meet the requirements of the GDPR (and applicable equivalent requirements of other Applicable Data Protection Laws).
- 3.8 The duration of Processing is limited to the duration of the Terms. Our obligations in relation to Processing will continue until the Personal Data has been properly deleted or returned to you in accordance with clause 11 of this Addendum.
- 3.9 You are solely responsible for ensuring that your Instructions comply with Applicable Data Protection Laws. It is also your responsibility to enter into data processing agreements with other relevant Data Controllers in order to allow us and our Sub-Processors to Process Personal Data in accordance with this Addendum.
- 3.10 If, in our reasonable opinion, an Instruction infringes Applicable Data Protection Laws, we will notify you as soon as reasonably practicable.

#### **4 DATA SUBJECT REQUESTS**

- 4.1 To the extent permitted by law, we will notify you promptly if we receive a request from a Data Subject to exercise the Data Subject's rights under Applicable Data Protection Laws relating to any Personal Data (**Data Subject Request**).
- 4.2 Taking into account the nature of the Processing, we will assist you by implementing appropriate technical and organisational measures, to the extent possible, to fulfil your obligation to respond to a Data Subject Request under Applicable Data Protection Laws.
- 4.3 To the extent you do not have the ability to address a Data Subject Request, we will, on your written request, provide reasonable assistance in accordance with Applicable Data Protection Laws to facilitate that Data Subject Request. You will reimburse us for the costs arising from this assistance.

4.4 We will not respond to a Data Subject Request except on your written request or if required by applicable law.

## **5 OUR PERSONNEL**

5.1 We will:

- a take reasonable steps to ensure the reliability of any of our Personnel engaged in the Processing of Personal Data;
- b ensure that access to Personal Data is limited to our Personnel who require that access as strictly necessary for the purposes of exercising our rights and performing our obligations under the Terms;
- c ensure that our Personnel engaged in Processing Personal Data are subject to confidentiality undertakings or professional or statutory obligations of confidentiality; and
- d ensure that our Personnel engaged in Processing Personal Data are informed of the confidential nature of the Personal Data and receive appropriate training on their responsibilities.

5.2 We have appointed a data protection officer who can be contacted at **support@narrative.so**.

## **6 SUBPROCESSESORS**

6.1 You acknowledge and agree that we may engage third party Sub-Processors in connection with the provision of the Service.

6.2 We have entered into (and will, for any new Sub-Processor, enter into) written agreements with each Sub-Processor containing data protection obligations which offer at least the same level of protection for Personal Data as set out in this Addendum and that meet the requirements of Article 28(3) of the GDPR, as applicable to the nature of the services provided by that Sub-Processor.

6.3 You may request copies of our written agreements with Sub-Processors (which may be redacted to remove confidential information not relevant to this Addendum).

6.4 A list of current Sub-Processors for the Services as at 5 November 2020 is set out in Schedule 2. We may update the list of Sub-Processors from time to time and, subject to clause 6.5, we will give at least 30 days' written notice of any new Sub-Processor.

6.5 We may engage Sub-Processors as needed to serve as an Emergency Replacement to maintain and support the Services. *Emergency Replacement* means a sudden replacement of a Sub-Processor where a change is outside our reasonable control. In this case, we will inform you of the replacement Sub-Processor as soon as reasonably practicable.

- 6.6 If you object to any new Sub-Processor, you may, despite anything to the contrary in the Terms, terminate these Terms and your right to access and use the Service without penalty on written notice, provided (in the case of a new Sub-Processor notified under clause 6.4) your notice of termination is received by us before the effective date of our notice under clause 6.4 or (in the case of a new Sub-Processor notified under clause 6.5) your notice of termination is received by us within 30 days of our notice of the new Sub-Processor. If you do not terminate these Terms and your right to access and use the Service in accordance with this clause, you are deemed to have agreed to the new Sub-Processor.
- 6.7 We are liable for the acts and omissions of our Sub-Processors to the same extent we would be liable if performing the services of each Sub-Processor directly under the terms of this Addendum, except as otherwise set out in this Addendum.

## **7 SECURITY**

We will maintain technical and organisational measures to protect the confidentiality, integrity and security of Personal Data (including protection against unauthorised or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorised disclosure of, or access to, Personal Data), and to manage data security incidents affecting Personal Data, in accordance with Appendix 2 of the Standard Contractual Clauses.

## **8 SECURITY BREACH MANAGEMENT**

- 8.1 We will comply with all applicable laws requiring notification to you of any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data Processed by us or our Sub-Processors of which we become aware (**Breach Incident**).
- 8.2 We will make reasonable efforts to identify the cause of that Breach Incident, notify you within a timely manner to allow you to meet your obligations to report a Breach Incident, and take steps we consider necessary and reasonable to remediate the cause of the Breach Incident, to the extent remediation is within our reasonable control.

## **9 AUDIT AND COMPLIANCE**

Upon your written request, we will, at your cost, submit to your audits and inspections, and provide you all information necessary, to demonstrate that both you and we are complying with our respective obligations under Applicable Data Protection Laws (including our respective obligations under Article 28 of the GDPR).

## **10 DATA PROTECTION IMPACT ASSESSMENT**

Upon your written request, we will, at your cost, provide you with reasonable assistance needed to fulfil your obligation under the GDPR to carry out a data protection impact

assessment relating to your use of the Service, to the extent you do not otherwise have access to the relevant information.

## **11 RETURN AND DELETION OF PERSONAL DATA**

- 11.1 Subject to clauses 11.2 and 11.3, following termination of the Terms we will delete all Personal Data within a reasonable period from termination of the Terms.
- 11.2 Subject to clause 11.3, you may submit a written request to us within 10 working days of the termination of the Terms requiring us, within 20 working days of your written request, to:
- a return a complete copy of all Personal Data by secure file transfer in a common format; and
  - b delete all other copies of Personal Data Processed by us or any Sub-Processor.
- 11.3 We, or each Sub-Processor, may retain Personal Data to the extent that it is required by applicable laws, provided that we ensure the confidentiality of all such Personal Data and ensure that such Data is only processed as necessary for the purposes required under applicable laws requiring its Processing and for no other purpose.
- 11.4 If we cannot delete all Personal Data due to technical reasons, we will inform you as soon as reasonably practicable and will take reasonably necessary steps to:
- a come as close as possible to a complete and permanent deletion of the Personal Data;
  - b fully and effectively anonymise the remaining data; and
  - c make the remaining Personal Data which is not deleted or effectively anonymised unavailable for future Processing.

## **12 CHANGES IN DATA PROTECTION LAWS**

- 12.1 We may on at least 30 days' written notice to you from time to time, make any variations to this Addendum (including to the Standard Contractual Clauses), which we consider (acting reasonably) are required as a result of any change in, or decision of a competent authority under, Applicable Data Protection Law, to allow transfers and Processing of Personal Data to continue without breach of Applicable Data Protection Law.
- 12.2 If you object to any variation under clause 12.1, you may, despite anything to the contrary in the Terms, terminate these Terms and your right to access and use the Service without penalty on written notice, provided your notice of termination is received by us before the effective date of our notice. If you do not terminate these Terms and your right to access and use the Service in accordance with this clause, you are deemed to have agreed to the variation.

### **13 LIMITATION OF LIABILITY**

The liability of each party to the other party under or in connection with this Addendum is subject to the limitations and exclusions set out in the Terms, and any reference in the Terms to the liability of a party means the aggregate liability of that party under the Terms and this Addendum together.

### **14 GENERAL**

If any provision of this Addendum is, or becomes unenforceable, illegal or invalid for any reason, the relevant provision is deemed to be varied to the extent necessary to remedy the unenforceability, illegality or invalidity. If variation is not possible, the provision must be treated as severed from this Addendum without affecting any other provisions of this Addendum.

## **SCHEDULE 1**

### **DETAILS OF PROCESSING**

#### **Nature and Purpose of Processing**

We will Process Personal Data as necessary to provide the Service in accordance with the Terms, as further specified in our online documentation relating to the Services, and as further instructed by you and your Personnel and other end users you allow to use the Service through the use of the Service.

#### **Duration of Processing**

Subject to clause 11 of this Addendum, we will Process Personal Data for the duration of the Terms, unless otherwise agreed upon in writing.

#### **Categories of Data Subjects**

You may submit Personal Data to the Service, the extent of which is determined and controlled by you in your sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of data subjects:

- a our customers who are photographers, publishers or editors
- b our customers' clients who are natural persons, include people who they photograph
- c any other person who you invite to view or access a Select project, when you share their personal information with us.

#### **Type of Data**

You may submit Personal Data to the Service, the extent of which is determined and controlled by you in your sole discretion, and which may include, but is not limited to, the following categories of personal data:

- a first and last name
- b contact information (company, email, phone, physical business and billing addresses)
- c financial or billing information
- d photographs and their correlating metadata
- e information about the device you are using to access the Service.

## SCHEDULE 2

### LIST OF SUB-PROCESSORS AS AT 5 NOVEMBER 2020.

<b>Sub-processor</b>	<b>Location</b>	<b>Purpose</b>	<b>Policy pages</b>
AWS Amazon	USA	Data hosting	<a href="#">Privacy Policy</a>
Cloudflare	USA	CDN	<a href="#">Privacy Policy</a>
Github	USA	Software repository	<a href="#">Privacy Policy</a>
Slack	Ireland	Team communication platform	<a href="#">Privacy Policy</a>
Google Suite	USA	Cloud services and digital marketing	<a href="#">Privacy Policy</a>
Notion	USA	Internal documents	<a href="#">Privacy Policy</a>
Baremetrics	USA	CRM and financial reporting for company and users	<a href="#">Privacy Policy</a>
Intercom	USA	Customer support and CRM	<a href="#">Privacy Policy</a>
Stripe	USA	Billing, payments, subscription management and CRM	<a href="#">Privacy Policy</a>
First Promoter	USA	Affiliate and referral management and CRM	<a href="#">Privacy Policy</a>
Tapfiliate	The Netherlands	Affiliate and referral management and CRM	<a href="#">Privacy Policy</a>
Kickofflabs	USA	Affiliate and referral management and CRM	<a href="#">Privacy Policy</a>
Survicate	Poland	User surveys	<a href="#">Privacy Policy</a>



Clickup	USA	Internal planning	<a href="#">Privacy Policy</a>
Typeform	Spain	User surveys	<a href="#">Privacy Policy</a>
Drip	USA	EDM	<a href="#">Privacy Policy</a>
Datadog	USA	Security	<a href="#">Privacy Policy</a>
Saleshandy	USA	EDM	<a href="#">Privacy Policy</a>
Sentry	USA	Application monitoring platform	<a href="#">Privacy Policy</a>
CircleCI	USA	Continuous integration	<a href="#">Privacy Policy</a>
Inspectlet	USA	Website analytics	<a href="#">Privacy Policy</a>
Facebook Business	USA	Digital marketing	<a href="#">Privacy Policy</a>

### SCHEDULE 3

#### STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of Personal Data to Processors established in third countries which do not ensure an adequate level of data protection.

[Customer to complete the details below]

Name of the data exporting organisation: .....

Address: .....

Tel.: .....; fax: .....; e-mail: .....

Other information needed to identify the organisation

.....

(the **data exporter**)

And

Name of the data importing organisation: Software Limited

Address: Narrative – SPACES, 501 Karangahape Road, Central Auckland 1010

E-mail: support@narrative.so

Other information needed to identify the organisation:

a New Zealand company, company number 6304647

(the **data importer**)

each a **party**, together the **parties**

have agreed the following Standard Contractual Clauses (**Clauses**) in order to provide adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in Appendix 1 of this Schedule 3.

### **Clause 1: Definitions**

For the purposes of the Clauses:

- a *personal data, special categories of data, process/processing, controller, processor, data subject and supervisory authority* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- b the *data exporter* means the controller who transfers the personal data;
- c the *data importer* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- d the *subprocessor* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- e the *applicable data protection law* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- f *technical and organisational security measures* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

### **Clause 2: Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

### **Clause 3: Third-party beneficiary clause**

- 1 The data subject can enforce against the data exporter this Clause, Clause 4b to i, Clause 5a to e, and g to j, Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
- 2 The data subject can enforce against the data importer this Clause, Clause 5a to e and g, Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
- 3 The data subject can enforce against the subprocessor this Clause, Clause 5a to e and g, Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
- 4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

### **Clause 4: Obligations of the data exporter**

The data exporter agrees and warrants:

- a that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- b that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- c that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- d that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other

unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

- e that it will ensure compliance with the security measures;
- f that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- g to forward any notification received from the data importer or any subprocessor pursuant to Clause 5b and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- h to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- i that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- j that it will ensure compliance with Clause 4a to i.

#### **Clause 5: Obligations of the data importer**

The data importer agrees and warrants:

- a to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- b that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- c that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

- d that it will promptly notify the data exporter about:
  - i any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
  - ii any accidental or unauthorised access, and
  - iii any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- e to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- f at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- g to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- h that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- i that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- j to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

## **Clause 6: Liability**

- 1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
- 2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations

of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

- 3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

#### **Clause 7: Mediation and jurisdiction**

- 1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
  - a to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
  - b to refer the dispute to the courts in the Member State in which the data exporter is established.
- 2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

#### **Clause 8: Cooperation with supervisory authorities**

- 1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
- 2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
- 3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5b.

### **Clause 9: Governing Law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

### **Clause 10: Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

### **Clause 11: Subprocessing**

- 1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
- 2 The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
- 3 The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
- 4 The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5j, which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

### **Clause 12: Obligation after the termination of personal data processing services**

- 1 The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation

imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

- 2 The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**On behalf of the data exporter:**

[Customer to complete the details below]

Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any):  
.....

Signature.....

**On behalf of the data importer:**

Name: James Broadbent

Position: CEO

Address: Narrative – SPACES, 501 Karangahape Road, Central Auckland 1010

Other information necessary in order for the contract to be binding (if any):

Signature: *James Broadbent*



## APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

### Data exporter

The data exporter is:

[Customer to complete the details below]

Name: .....

(please specify briefly your activities relevant to the transfer):

.....

### Data importer

The data importer is:

Software Limited, a New Zealand company, company number 6304647

(please specify briefly your activities relevant to the transfer):

Software Limited provides a downloadable desktop and web based app (**Service**), that its customers can use to manage, edit, review and publish their photographs and other information. The provision of the Service is governed by the terms, including the Data Processing Addendum set out at <https://narrative.so/terms-and-conditions> (**Agreement**).

### Data subjects

The personal data transferred concern the following categories of data subjects:

As set out in Schedule 1 of the Data Processing Addendum to which these Clauses are attached.

### Categories of data

As set out in Schedule 1 of the Data Processing Addendum to which these Clauses are attached.

### Processing operations

The personal data transferred will be subject to the following basic processing activities:

The data importer will process personal data to exercise its rights and perform its obligations under the Agreement.

**DATA EXPORTER**

[Customer to complete the details below]	
Name:	.....
Signature	.....

**DATA IMPORTER**

Name: James Broadbent

Signature: *James Broadbent*

**APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES**

This Appendix forms part of the Clauses and must be completed and signed by the parties.

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4d and 5c:**

Data Storage - Our services operate in the cloud, specifically Amazon Web Services (AWS). AWS is the largest cloud compute and storage service provider and maintains strong security and data integrity policies. You can see more about AWS security [here](#). Our servers are physically located in the United States of America, specifically AWS Virginia (us-east-1), and Ohio (us-east-2). We maintain multiple databases to ensure our services operate correctly, and are continuously versioned, and backed up for recovery purposes. Finally, we use AWS Simple Storage Service (S3). We use S3 for storing all customer images, and other auxiliary assets.

Encryption - All traffic to any of our services are encrypted via HTTPS and protected with SSL certification.

Passwords - All user passwords are hash using Bcrypt hashing function. Passwords cannot be retrieved or changed without access to the associated user email address. Internal passwords are controlled and stored in 1Password, along with 2-Factor authentication where available. For all critical system access control is managed via Hashicorp Vault, with strict lease policies, and auto revoking. In most cases, certificates are issued rather than passwords.

Billing Data - We do not store your Credit Card details. All storage, payment processing, and fraud protection is managed by Stripe. Stripe is a secure PCI compliant company. You can see more about Stripe [here](#).

Segregation of Duties - Our employees do not have access to your data. The exception to this is when customer success teams, or engineers need to help, or debug an issue with your account. Access to data is controlled by department and role. Gaining access to data requires requesting access with our core service team. See our [Terms and Conditions](#) for more about how we use your data.

Reliability – We have multiple layers of redundancy and availability. Our services are designed to scale to demand as needed and protected via Cloudflare against DDoS attacks or other malicious activity. Our services are also monitored, with automatic notification services to signal potential issues.

Data Processing and Retention - See our [Terms and Conditions](#) and [Privacy Policy](#).

**DATA EXPORTER**

<i>[Customer to complete the details below]</i>	
Name:	.....
Signature	.....

**DATA IMPORTER**

Name: James Broadbent

Signature: *James Broadbent*

<b>TITLE</b>	PDF DPA for T&C update - please sign asap! :)
<b>FILE NAME</b>	Narrative DPA Nov 2020.pdf
<b>DOCUMENT ID</b>	9c2dfa06dd494a5a59b86068f0c2c511a9680d1a
<b>AUDIT TRAIL DATE FORMAT</b>	DD / MM / YYYY
<b>STATUS</b>	● Completed

---

## Document History



SENT

**04 / 11 / 2020**

13:17:39 UTC+12

Sent for signature to James Broadbent (james@narrative.so)  
 from kirstie.marsh@narrative.so  
 IP: 103.233.220.6



VIEWED

**04 / 11 / 2020**

13:20:36 UTC+12

Viewed by James Broadbent (james@narrative.so)  
 IP: 103.233.220.6



SIGNED

**04 / 11 / 2020**

13:21:04 UTC+12

Signed by James Broadbent (james@narrative.so)  
 IP: 103.233.220.6



COMPLETED

**04 / 11 / 2020**

13:21:04 UTC+12

The document has been completed.