Data Processing Agreement.

THIS AGREEMENT SHALL BE EFFECTIVE FROM THE DATE OF SIGNATURE OF THE MAIN CONTRACT, AND SHALL BE BETWEEN THE ELEMENT ENTITY ("ELEMENT") AND THE CUSTOMER ("CUSTOMER") REFERENCED IN THE MAIN CONTRACT

Each a "**party**", together the "**parties**".

BACKGROUND

This agreement (the "**Agreement**") describes the parties responsibilities and sets out the terms on which Element will process personal data on Customer's behalf.

1. Definitions

Controller, Processor, data subject, personal data, personal data breach, processing and appropriate technical measures: as defined in the Data Protection Legislation.

Data Protection Legislation: means all laws and regulations applicable to the processing of personal information under the agreement, including those of the United Kingdom, European Union, the European Economic Area and their member states, Switzerland and the United States and its states.

Standard Contractual Clauses: mean the applicable module of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council from June 4th 2021, as available here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj, or as such SCCs shall be amended by the EU Commission, or by any official data protection regulator mandated by data protection legislation and the ICO's International Data Transfer Agreement for the transfer of personal data from the UK and/or the ICO's International Data Transfer Addendum to EU Commission Standard Contractual Clauses in force as of the 21 March 2022.

EU GDPR: the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

GDPR: as applicable, the EU GDPR or the UK GDPR.

UK GDPR: the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

Main Contract: either i) the Element Software and Services License Agreement, or ii) the Element Master Services Agreement MSA, or iii) the Element Trial Terms and Conditions entered into between Element and the Customer (as applicable)

Sub-Processor means any person (including any third party but excluding an employee of Element) appointed by or on behalf of Element to Process Customer Personal Information.

Third Country: any country, organisation or territory not acknowledged by the European Union under Article 45 of GDPR as a safe country with an adequate level of data protection.

2. Data Protection Compliance

Both parties will comply with all applicable requirements of the Data Protection Legislation. This clause 2 is in addition to, and does not relieve, remove or replace, a party's obligations or rights under the Data Protection Legislation.

The processing of Customer's personal data shall take place exclusively in a member state of the European Union, in another state party to the Agreement on the European Economic Area, in the United Kingdom, or in a third country only in accordance with the requirements on data transfers in the GDPR, according to the Main Contract and the instructions of the Customer.

3. The Parties' Roles

The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and Element is the Processor. The table below sets out the scope, nature and purpose of processing by Element, the duration of the processing and the types of personal data and categories of data subject.

Data Processing Details	
Subject-matter	Element will process personal data as necessary to perform the services of the Main Contract.
Nature and purpose	For the delivery of the services of the Main Contract.
Duration	Data processing will occur for the duration of the Main Contract between the parties and on termination of this Agreement, the data will be deleted. Unless this data is required to comply with legal requirements.
Types of personal data	As per the Element Privacy Policy. Types of personal data processed may include contact details (address, email address) account details (MxID, unencrypted communications, room names, user profile pictures), mobile phone number (optional). Automatically collected personal data includes IP address, Device ID & agent.
Categories of Data Subject	Customers' clients or users. Employees of the Customer.

4. Customer's Responsibilities as the Controller

4.1. Without prejudice to clause 2, the Customer will ensure that it has all necessary and appropriate consents and notices in place to enable lawful transfer of the personal data to Element for the duration and purposes of this Agreement.

5. Element's Responsibilities as the data Processor

Without prejudice to clause 2, Element shall, in relation to any personal data processed by Element under this Agreement:

5.1. process that personal data within the scope of the Main Contract and exclusively on behalf of and in accordance with the instructions of the Customer within the meaning of Article 28 of the EU GDPR (commissioned processing); unless Element is required by law to

otherwise process that personal data. Where Element is relying on legal obligations as the basis for processing personal data, Element shall promptly notify the Customer of this before performing the processing required by law unless the law in question prohibits Element from so notifying the Customer;

5.2. ensure, in accordance with Article 32 of the GDPR, that it has in place and maintains appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting personal data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to personal data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it), whereas such technical and organisational measures comprise in particular those as listed in Annex 1;

5.3. ensure that all personnel who have access to and/or process personal data are obliged to keep the personal data confidential (even beyond the term of the Main Contract) and to allow Customer to verify compliance with this clause; and

5.4. assist the Customer as far as possible with suitable organisational measures in fulfilling the Customers obligations pursuant to Articles 12 to 22 and 32 to 36 of the GDPR.

5.5. where possible in responding to a request from a data subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

5.6. notify the Customer without undue delay if a data subject asserts rights, such as the right to information, correction or deletion with regard to their data, directly against Element. Element shall immediately forward this request to the Customer and await the Customer's instructions. Element shall not contact the data subject without corresponding instruction by the Customer.

5.7. notify the Customer without undue delay on becoming aware of a personal data breach;

5.8. notify the Customer without undue delay if Element is of the opinion that an instruction by the Customer violates Data Protection Legislation. Element shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Customer.

5.9. at the written direction of the Customer, delete, destroy or return personal data and copies thereof to the Customer on termination of this Agreement unless required by law to store the personal data, and to confirm deletion, destruction or return to the Customer upon request; this does not apply to such data that serves to document accurate processing in accordance with the Main Contract, such data may be retained by Element for one (1) year after the end of this Agreement and has to be provided to the Customer upon its request; and

5.10. maintain complete and accurate records and information to demonstrate its compliance with this clause and allow for audits by the Customer or the Customer's designated auditor, only so far as is necessary in order to demonstrate compliance, provided that the

Customer: provides Element with no less than thirty (30) days' notice of such audit or inspection; and the parties agree the scope, duration, and purpose of such audit or inspection. If the Customer becomes privy to any confidential information of Element as a result of this clause; and

5.11. the Customer shall hold such confidential information in confidence and, unless required by law, not make the confidential information available to any third party, or use it for any other purpose. The Customer acknowledges that Element shall only be required to use reasonable endeavours to assist the Customer in procuring access to any third-party assets, records or information as part of any audit.

6. Customer's instruction rights

6.1. Instructions shall be issued by the Customer in writing as a matter of principle; instructions issued verbally shall be confirmed in writing by Element. The persons authorised to issue and receive instructions are set out in Annex 2. In the event of a change or long-term prevention of the persons named in Annex 2, the successor or representative shall be named to the other party in text form without delay. The Customer shall notify Element of a change in the person authorised to issue instructions in good time. Until receipt of such notification by the Customer, the designated persons shall continue to be deemed authorised to issue instructions.

7. Third Party Processors

7.1. The Customer gives its consent to the appointment by Element of a third party data processors (Sub-processors), provided that the same data protection obligations as set out in clauses 2, 6 and 7 have been and remain imposed upon such third party data processors. In particular, the Customer consents to and approves of the Sub-processors (and, where applicable, to the Sub-processors of such Sub-processors) listed in Annex 3.

7.2. Element confirms that:

7.2.1. it shall impose on all Sub-processors the same data protection obligations as set out in this Agreement; and

7.2.2. it shall remain fully liable for the actions of its Sub-processors at all times.

7.3. Element shall give the Customer prior notice of the appointment of any new Sub-processors and provide the Customer with full details of the processing to be undertaken by the Sub-processor, thereby giving the Customer the opportunity to object to such appointment. If Element so notifies the Customer of any changes to Sub-processors and the Customer objects to such changes, the Customer will be entitled to terminate this Agreement (without liability for either party, and such termination will be deemed to be a no-fault termination) if the Customer has reasonable grounds for objecting to such changes by reason of the changes causing or being likely to cause the Customer to be in breach of the Data Protection Legislation. The Customer must give Element at least thirty (30) days' written notice of such termination.

7.4. A third-party data processing within the meaning of this Agreement shall not exist if Element commissions third parties with services which are to be regarded as purely ancillary services. These include, for example, postal, transport and shipping services, cleaning services, security services, telecommunications services without any specific reference to services provided by Element to the Customer as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software

of data processing systems. Element's obligation to ensure compliance with data protection and data security in these cases shall remain unaffected.

8. Data transfers

8.1. By default, transfers of data will occur within the EU/UK and countries which have received an adequacy decision/regulation in relation to the GDPR.

8.2. In the case of a transfer of Customer Personal Data to a country not providing an adequate level of protection pursuant to the applicable Data Protection Laws ("Non-Adequate Country"), the parties shall cooperate to ensure compliance with the applicable Data Protection Laws. If the Customer believes the measures set out below are not sufficient to satisfy the applicable legal requirements, the Customer shall notify Element and the parties shall work together to find an alternative safeguard mechanism.

8.3. The parties acknowledge that the applicable module of the Standard Contractual Clauses will be determined as the Customer acting as a Controller and Element acting as a Processor. Module 2 of the Standard Contractual Clauses will apply to the Personal Data transferred to any Non-Adequate Country outlined in the Standard Contractual Clauses annex, available here on the Element website and added to this Agreement as per the Customer's requirements.

9. Liability

9.1. The parties' liability is determined by Article 82 of the GDPR.

9.2. A party shall fully release, indemnify and hold harmless the respective other party from liability if a party proves that it is not responsible in any respect for the circumstance as a result of which the damage occurred to an affected party. This shall apply *mutatis mutandis* in case a fine or administrative penalty is imposed on a party, with the release being to the extent that the releasing party bears a share of the responsibility for the violation sanctioned by the fine.

10. Term and termination

10.1. The term of this Agreement corresponds to the term of the Main Contract. If the Main Contract can be terminated for convenience, those provisions shall also apply to this Agreement. In case of doubt, a termination of the Main Contract shall also be deemed a termination of this Agreement and a termination of this Agreement shall be deemed a termination of the Main Contract.

10.2. The Customer is entitled to extraordinary termination of this Agreement for good cause at any time. Good cause shall be deemed to exist if Element fails to fulfill its obligations under this Agreement, violates provisions of the GDPR intentionally or with gross negligence, or is unable or unwilling to carry out an instruction of the Customer. In the case of simple violations (neither intentional nor grossly negligent), the Customer shall first set Element a reasonable deadline within which Element can remedy the violation. If this period

expires without a conclusion, the Customer shall then be entitled to extraordinary termination. Clause 7.3 of this Agreement remains unaffected.

11. General

11.1. In case of doubt, the provisions of this Agreement shall take precedence over the provisions of the Main Contract. Should individual provisions of this Agreement prove to be invalid or unenforceable in whole or in part, or become invalid or unenforceable as a result of changes in legislation after conclusion of the Agreement, this shall not affect the validity of the remaining provisions. The invalid or unenforceable provision shall be replaced by the valid and enforceable provision that comes as close as possible to the meaning and purpose of the invalid provision.

11.2. Amendments and supplements to this Agreement must be made in writing. This shall also apply to the waiver of this formal requirement.

11.3. This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of England and Wales or in accordance with the laws of the Element's contracting entity in the Main Contract.

Annex 1: Technical Organisational Measures (TOMs)

Access controls

Element follows a managed, strict least privilege access policy and admin account separation. Additionally technical controls are in place securing access to systems. Physical access controls are in place for the company offices.

Encrypted transfer of data & data at rest

Matrix is encrypted in transit and most content is additionally encrypted end-to-end between conversation participants. Backups are also encrypted.

Backups of personal data

For Element's hosted customers there are backups saved on a regular basis. All production infrastructure is reproducible from source code allowing business recovery.

Passwords

Multi factor authentication is the default. Employees must use a password manager. Employees are educated about passwords and there are technical controls ensuring appropriate entropy and complexity of passwords.

Employee training

All employees undergo security and data protection training as part of onboarding. This training is updated annually for all employees.

Third party management

All third party vendors are vetted and assessed as part of Element's supplier management processes which includes assigning a vendor risk rating.

Vulnerability management

Element ensures production and non-production systems are patched. Element conducts vulnerability scans and remediates any discovered security issues.

Firewalls and hardening

Element runs firewalls in front of the services offered to mitigate against denial-of-service attacks. Audits of service ports and firewall rules are performed regularly.

Personal Data and Data Retention

Element has a comprehensive privacy policy which gives users clear guidance on how personal data is processed, duration of processing and storage locations.

Incident response management

Element has an incident management process and policies in place.

Certifications

Element holds a Cyber Essentials Plus Certification, a technical certification that confirms boundary firewalls, secure configurations, access control, malware protection and patch management are in place across all systems.

Annex 2: Processor Key Contact

Element

Full Name: Denise Almeida

Job Title: Head of Policy and Compliance (DPO)

Contact details including email: dpo@element.io

element

Annex 3: Element Sub-processors

Name of Sub-processor	Sub-processor services	Location of Sub-processor	Website & address
Amazon Web Services (AWS)	Infrastructure services: Cloud services and data centre services	Dependent on customer (Ohio, US; Amsterdam, Frankfurt, EU; London, England)	https://aws.amazon.com/ Amazon Web Services EMEA SARL, UK BRANCH 1 Principal Place, Worship Street, London, EC2A 2FA, UNITED KINGDOM
Hubspot. Inc.	Web analytics & marketing automation	United States	https://www.hubspot.com/ HubSpot, Inc. 2 Canal Park Cambridge, MA 02141 United States
Posthog	Web analytics	United States or Germany	https://posthog.com/ 2261 Market St #4008, San Francisco, United States
Stripe	Payments Processor	UK	https://stripe.com/gb Stripe payments Europe Ltd.
Twillio	SMS Multi Factor Authentication	United States	https://www.twilio.com/ 375 Beale St #300, San Francisco, United States
Zammad	Customer service communication	Germany	https://zammad.com/en Zammad GmbH Marienstrasse 18 10117 Berlin Germany

12. Document History

- 2023, November 24: updates to definitions
- 2023, October 31: updates to definitions
- 2023, August 17: Updates to applicable Data Protection Legislation
- 2023, June 23: Format changes.
- 2022, December 20: current version derived from previous Data Processing Agreement.