Data Processing Addendum (DPA)

Version Date: August 27, 2021

The terms of this Data Processing Addendum (DPA) will apply in addition to the general terms set out in the Event Store Cloud Services Subscription Agreement where:

A. an Event Store customer uploads personal data to the Cloud Provider Platform; and
B. the Event Store customer is located in Europe or the personal data the customer uploads relates to individuals located in Europe or in the United Kingdom.

All defined terms in this DPA have the same meaning as in the Event Store Cloud Subscription Agreement.

This DPA is an agreement between the entity named on the Order Form (**Customer**, **you** or **your**) and Event Store Limited, a company incorporated in England and Wales (company number 11389094) with its registered office at 3 Corsham Science Park, Park Lane, Corsham, England, SN13 9FU (**Event Store**).

1. Roles of the parties

1.1. You are the controller and Event Store is the **processor** for any personal data you upload to the Cloud Provider Platform. It is your responsibility to determine the purposes and means of the processing of personal data, and ensure you meet the conditions of your chosen lawful basis. If you store special category data (such as health data) it is your responsibility to meet the additional requirements to process such data.

1.2. You specify the location of the server to which you upload personal data to on the Order Form when you register to use our services. It is your responsibility to ensure that you comply with applicable data protection law (which may apply either because of your location or because of the location of the data subjects whose personal data you upload to the Cloud Provider Platform).

1.3. Event Store is the **controller** in relation to limited categories of personal data for your staff (to the extent their details are required to register and gain access to Event Store Platform). For more information about how Event Store uses personal data as a controller, please read our Privacy Policy.

2. Details of processing

2.1. Except where otherwise stated during the subscription process, Event Store processes personal data:

a. to fulfil our obligations to you under the Event Store Cloud Subscription Agreement. Namely, providing access to third party cloud storage and ancillary technical support (**subject matter**);
b. for the period beginning when you first upload personal data to the Cloud Provider Platform and ending when our contractual relationship terminates, when Event Store deletes or returns any personal data to you (**duration**);
c. by facilitating the transfer to a Cloud Provider Platform on a server in a territory selected by you (**nature**);
d. of any type which you upload to the Cloud Provider Platform, which can be any information which can or can be used to identify a living person (**type of personal data**); and
e. about any person who can be identified by the information you upload to Cloud Provider Platform (**categories of data subjects**).

2.2. You may amend or supplement the details of processing set out at Clause 2.1 by sending an email to security@eventstore.com, which will form part of the contract, at the time of the subscription.

3. Obligations of Event Store

3.1. Where we process any personal data for which you are the controller, we shall:

a. only process personal data on your written instructions, unless Event Store is required by law to process or transfer that personal data, in which case we will inform you in advance (except where it would be illegal for us to do so);
b. ensure that any person who accesses the personal data is subject to confidentiality obligations, whether contractual or statutory;
c. implement the technical and organisational security measures as set out in the Event Store Security Policy at Schedule 1 to mitigate the risk of a personal data breach;
d. only appoint third parties (who we instruct to help us deliver our service) after we have notified you in writing and you have not objected within 30 calendar days;
e. promptly inform you if a data subject has made a request under an applicable data protection law and assist you to respond to the data subject;
f. promptly inform you if there has been a personal data breach and, at your cost, assist you respond to any such security incident;
g. at the end of our contractual relationship, or any earlier written request from you, delete the personal data. If you wish to retain a copy of the information, you must download a copy before the contract end date; and
h. provide the information you reasonably require to demonstrate that Event Store complies with our data protection obligations.

4. Security measures

4.1. You acknowledge that it is your responsibility as the controller to assess whether the security measures set out in the Event Store Security Policy are sufficient for the categories and types of personal data you upload to the Cloud Provider Platform, and when you use the Event Store Platform you are deemed to accept our security measures as appropriate. You acknowledge that there is a higher risk associated with certain categories of personal data (such as special category data or financial data).

4.2. We may amend the Event Store Security Policy from time to time and we recommend you routinely review it for updates to ensure it continues to meet your requirements. We will notify you in advance if there are any material changes to our Event Store Security Policy.

5. Sub-processors

5.1. When you register to use our services, you are deemed to authorise the third parties engaged by Event Store at the date of registration. Event Store lists the third parties we use to help us provide our service to customers (sub-processors) at Schedule 2, these include the Cloud Platform Provider you choose to store your information and other organisations within our supply chain that help us deliver our services.

5.2. Event Store will only appoint new sub-processors after we have notified you in writing and you have not objected within 30 calendar days.

5.3. Where you object to a proposed sub-processor, Event Store will contact you to identify your concerns and discuss options to help resolve the objection. However, where the parties are unable to resolve the objection, you may elect to either (i) cease to use Event Store for storage of personal data or (ii) exercise your right to terminate the contractual relationship under the Event Store Cloud Subscription Agreement terms with no penalty.

5.4. We always enter into contracts with our sub-processors which contain equivalent data protection obligations as this DPA, in particular which require our sub-processors to provide sufficient guarantees as to their technical and organisational measures. Where our sub-processor fails to fulfil its data protection obligation, we remain fully liable to you for the performance of their obligations.

6. International transfers

6.1. Event Store Limited is a part of a group of companies. We use approved standard contractual clauses to ensure our internal transfers are subject to appropriate safeguards and ensure enforceable data subject rights and effective legal remedies for data subjects. The Event Store group is formed of:

- Event Store Limited: United Kingdom
- Event Store Netherlands BV: Netherlands
- Event Store (Mauritius) Ltd: Mauritius
- Event Store USA Inc: United States of America

6.2. We only transfer your information to the server you have selected on your Order Form. As the controller, it is your responsibility to conduct any required risk assessments. At your request and for the Assistance Fee, Event Store can assist you conduct such risk assessments.

6.3. We only transfer personal data to a territory outside the United Kingdom with your prior authorisation. We always have in place a legal mechanism to ensure any such transfer is lawful (for example, by ensuring the recipient is located in a country recognised as providing adequate data protection safeguards or because such safeguards have been contractually guaranteed by model clauses approved by the Secretary of State).

6.4. We include the standard contractual clauses (set out in Schedule 3, the UK SCCs) and where these apply, nothing in this DPA varies or modifies the UK SCCs.

7. Liability

7.1. You indemnify and defend at your own expense Event Store against all costs, claims, damages and expenses incurred by Event Store or for which Event Store may become liable due to your (or your employees' or agents') failure to comply with applicable data protection law or the terms of this DPA.

7.2. Event Store's liability shall not exceed either the amount paid by you in the 12 months immediately preceding any breach of this DPA or £100,000 (one hundred thousand pounds), whichever amount is lower (except where such limitation or exclusion of liability is prohibited by law).

8. Costs

8.1. Event Store is entitled to a separate fee (**Assistance Fee**) for assistance to the data controller under these Clauses, which is not directly related to the Event Store's provision of the Event Store Cloud, including, but not limited to, the Event Store's assistance to the Customer and Event Store's incurred costs as a result of an audit. The fee shall be calculated on basis of the Event Store's applicable hourly rate of £250. The fee will be applied for unreasonable or excessive requests for assistance at Event Store discretion. Event Store shall on request from the Customer document the time spent by Event Store on assistance to the Customer or for the time during the audit or inspection.

Schedule 1: Event Store Security Policy

Description of the technical and organisational security measures implemented by Event Store:

- Information Security Policies
  - Management has defined and approved the company-wide policies.
  - Policies are reviewed annually or sooner if required.
- Organization of Information Security
  - The company has a Chief Information Security Officer and a Data Privacy Officer.
  - There is segregation of duties between security, development and operations.
  - Event Store employees are members of special interest groups on cybersecurity.
  - Information security is considered in every stage of the development process.
  - There is a teleworking policy for employees.
- Human Resource Security
  - There are background checks on employees prior to employment.

    - Employees receive training on information security.
    - There is a procedure for removing access to systems and tools on termination of employment or change of duties.
- Asset Management
    - There is an asset inventory with defined employee ownership.
    - There is an information classification procedure.
    - There is a procedure for the safe disposal of assets.
- Access Control
    - There is an access control policy on applications, networks and services based on the need to know.
    - There is a user access provisioning procedure.
    - Privileged access is restricted and usage is recorded.
    - Access rights are reviewed on an annual basis.
    - Passwords must meet the complexity criteria.
    - Two-factor authentication is applied on all systems with such feature.
    - Access to source code changes is restricted and monitored.
- Cryptography
    - There is a policy for encryption keys handling.
    - Data is encrypted at rest.
- Physical and Environmental Security
    - All production systems are hosted in cloud services. Those suppliers are required to comply with ISO 27001.
- Operations Security
    - There is a policy for change management.
    - There are monitoring solutions for capacity management.
    - Development, testing and operational environments are separated.
    - There is a backup procedure in place.
    - All the systems and applications have logging enabled and are reviewed regularly.
    - Aligned with the segregation of duties and change management, the installation of software on operational systems is restricted and planned.
    - New operating system packages are installed automatically to avoid known technical vulnerabilities.
- Communications Security
    - There are firewalls in place to restrict access.
    - Networks are segregated. Each customer environment uses an independent network.
    - All network communications are encrypted (for example using HTTPS), which guarantees the authenticity of the service provider.
    - There is a confidentiality policy for employees and suppliers.
- System Acquisition, Development and Maintenance
    - There is an information security requirement specification regarding availability, confidentiality and integrity for new information systems.
    - A secure version control system is used for software development.
    - The change management policy includes updating the business continuity plan.
    - The same security requirements for the operational environment are applied to the development environment.
    - The software development includes the testing of security functionality.
    - No personal or confidential data is used during tests.
- Supplier Relationships
    - All production systems are hosted in cloud services. Those suppliers are required to comply with ISO 27001.
    - There is a policy for monitoring supplier services and changes.
- Information Security Incident Management
    - There is a procedure for security incident response planning, preparation, monitoring, detecting, analysing and reporting.
    - There is a policy on reporting information security incidents and their response.
- Information Security Aspects of Business Continuity Management
    - The business continuity plan covers information security.
    - The cloud services include redundancy of systems to avoid or minimise disruptions.
- Compliance
    - Applicable laws and regulations to the services provided have been identified.
    - There is a policy for the usage of licensed software.
    - There is a policy for the protection of records.
    - Personally identifiable information is managed under UK Data Protection Act 2018.
    - The information security and technical compliance are reviewed by an independent internal team.

Schedule 2: List of Sub-Processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

Infrastructure Providers

Event Store may engage the following entities to process personal data that you include in your use of Event Store Cloud or any other Event Store cloud services:

Third-Party Entity	Description of Processing	Location of Processing
Amazon Web Services, Inc.	Cloud Infrastructure Provider	Chosen by You
Google Inc.	Cloud Infrastructure Provider	Chosen by You
Microsoft Corp.	Cloud Infrastructure Provider	Chosen by You

Other Third-Party Subprocessors

To provide support and perform other service functions, we may also engage the following entities to process personal data on your behalf:

Third-Party Entity	Description of Processing	Location of Processing
Arlo Software Limited	Training Portal	Ireland
Auth0, Inc.	Authentication Services	United States of America
Freshworks, Inc.	Support Portal	United States of America
GitHub Inc.	Development Portal	United States of America
Google Inc.	Email Support	Europe
Hubspot Inc.	Sales Support	United States of America
Stripe Inc.	Payment Processor	United States of America

Schedule 3: UK SCCs: Controller-Processor

BACKGROUND

These clauses apply where there is a controller-processor relationship between the parties and personal data is being transferred from a party located in the UK to a party located in a territory deemed to be a "third country" for the purposes of UK data protection law. Where another safeguard or derogation under Chapter 5 of the UK GDPR does not apply, the parties can incorporate an unamended version of the following clauses into their agreement to legitimise the international transfer of personal data.

1. Definitions

For the purposes of the Clauses:

a. '**personal data**', '**special categories of data**', '**process/processing**', '**controller**', '**processor**', '**data subject**' and '**Commissioner**' shall have the same meaning as in the UK GDPR;
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 covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;
d. '**the sub-processor**' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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 UK;
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.

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.

3. Third-party beneficiary clause

3.1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) 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.

3.2. The data subject can enforce against the data importer this Clause, Clause 5(a) 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.

3.3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) 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 sub-processor shall be limited to its own processing operations under the Clauses.

3.4. 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.

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 Commissioner) and does not violate the applicable data protection law;
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 covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;
g. to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner 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 sub-processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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;
j. that it will ensure compliance with Clause 4(a) to (i).

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 Commissioner 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 Commissioner;
g. to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;
i. that the processing services by the sub-processor will be carried out in accordance with Clause 11;
j. to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6. Liability

6.1. 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 sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

6.2. 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 sub-processor 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 of 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 sub-processor of its obligations in order to avoid its own liabilities.

6.3. 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

7.1. 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 Commissioner;
b. to refer the dispute to the UK courts.

7.2. 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.

8. Co-operation with supervisory authorities

8.1. The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law.

8.2. The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any sub-processor, 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.

8.3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

9. Governing Law

9.1. The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established, namely England and Wales.

10. Variation

10.1. The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause.

11. Sub-processing

11.1. 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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor 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 sub-processor's obligations under such agreement.

11.2. The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

11.3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK where the exporter is established.

11.4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Commissioner.

12. Obligation after termination

12.1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor 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.

12.2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.